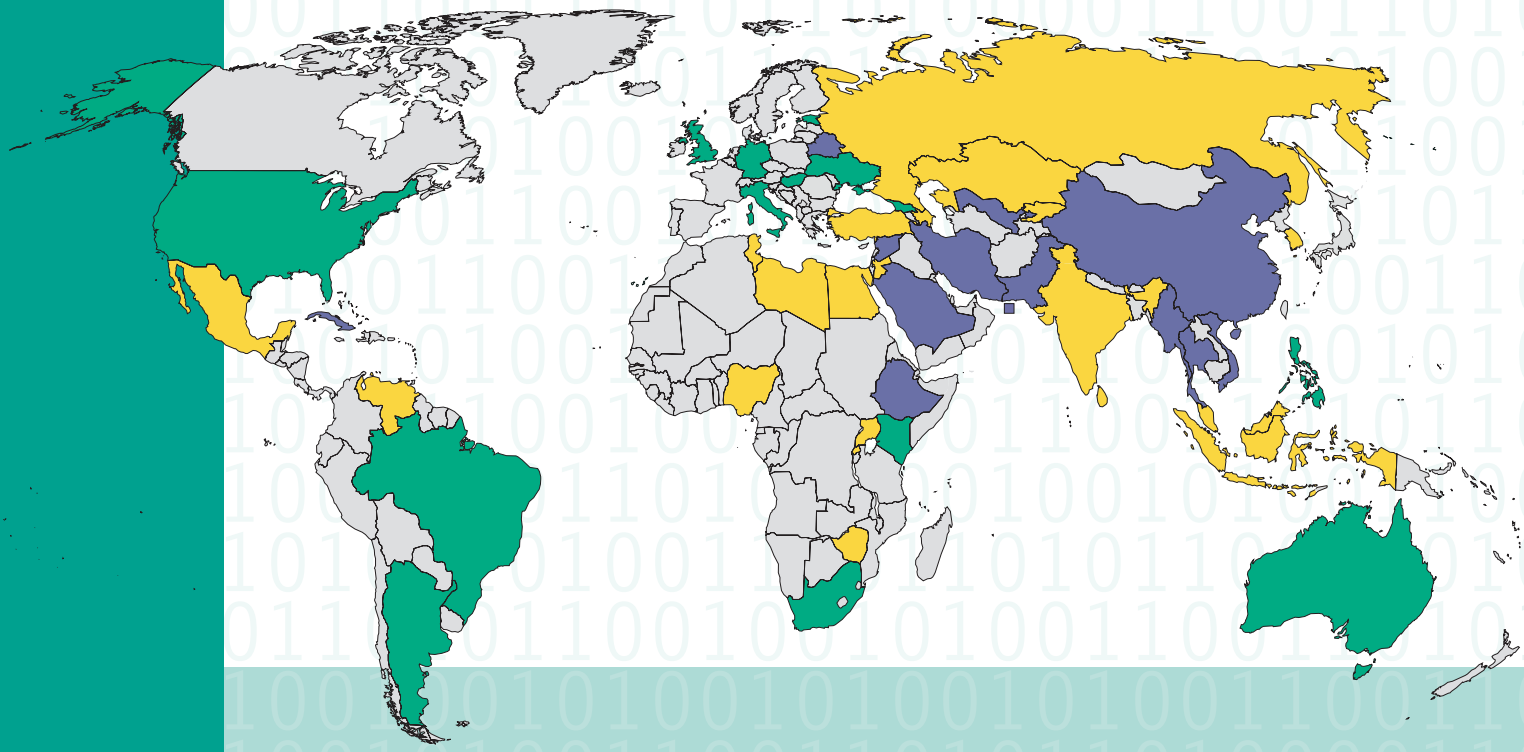
FREEDOM HOUSE

FREEDOM ON THE NET 2012

A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA



SUMMARY OF FINDINGS

www.freedomhouse.org

FREEDOM ON THE NET 2012

A Global Assessment of Internet and Digital Media

Sanja Kelly
Sarah Cook
Mai Truong
EDITORS

September 24, 2012

TABLE OF CONTENTS

	Page
Acknowledgments	i
Overview:	**1**
Evolving Tactics of Internet Control and the Push for Greater Freedom	
Sanja Kelly and Sarah Cook	
Charts and Graphs of Key Findings	**18**
Main Score Table	18
Global Graphs	21
Score Changes	22
Internet Freedom vs. Press Freedom	25
Internet Freedom vs. Internet Penetration	26
Regional Graphs	27
Freedom on the Net 2012 Map	30
Country Reports	**31**
Argentina	32
Australia	43
Azerbaijan	53
Bahrain	65
Belarus	84
Brazil	100
Burma	112
China	126
Cuba	152
Egypt	164
Estonia	177
Ethiopia	184
Georgia	197
Germany	205
Hungary	220
India	231
Indonesia	248
Iran	262

Italy 279
Jordan 294
Kazakhstan 305
Kenya 319
Kyrgyzstan 327
Libya 338
Malaysia 350
Mexico 364
Nigeria 375
Pakistan 386
Philippines 400
Russia 408
Rwanda 422
Saudi Arabia 433
South Africa 445
South Korea 456
Sri Lanka 472
Syria 484
Thailand 497
Tunisia 514
Turkey 525
Uganda 536
Ukraine 546
United Kingdom 557
United States 569
Uzbekistan 582
Venezuela 602
Vietnam 616
Zimbabwe 628

Methodology and Checklist of Questions 640

Contributors 649

Glossary 651

Freedom House Board of Trustees 656

About Freedom House 657

ACKNOWLEDGMENTS

Completion of the *Freedom on the Net* publication would not have been possible without the tireless efforts of the following individuals.

As project director, Sanja Kelly oversaw the research, editorial, and administrative operations, supported by senior research analyst Sarah Cook and staff editor Mai Truong. Together, they provided essential research and analysis, edited the country reports, conducted field visits in Turkey, Malaysia, and South Africa, and led capacity building workshops abroad. Over 50 external consultants served as report authors and advisors, and made an outstanding contribution by producing informed analyses of a highly diverse group of countries and complex set of issues.

Helpful contributions and insights were also made by Daniel Calingaert, executive vice president; Arch Puddington, vice president for research; Danilo Bakovic, internet freedom director; as well as other Freedom House staff in the United States and abroad. Intern Ezgi Ozturk provided indispensable research, editorial, and administrative assistance.

This publication was made possible by the generous financial contributions of the U.S. State Department's Bureau of Democracy, Human Rights, and Labor (DRL), the U.S. Agency for International Development (USAID), Google, and Yahoo. Freedom House is also grateful to the Dutch Ministry of Foreign Affairs for their grant to support future editions of *Freedom on the Net*. The content of the publication is the sole responsibility of Freedom House and does not necessarily reflect the views of DRL, USAID, Google, Yahoo, the Dutch Ministry, or any other funder.

EVOLVING TACTICS OF INTERNET CONTROL AND THE PUSH FOR GREATER FREEDOM

By Sanja Kelly and Sarah Cook

As of 2012, nearly a third of the world's population has used the internet, and an even greater portion possesses a mobile phone. The internet has transformed the way in which people obtain news, conduct business, communicate with one another, socialize, and interact with public officials. Concerned with the power of new technologies to catalyze political change, many authoritarian states have taken various measures to filter, monitor, or otherwise obstruct free speech online. These tactics were particularly evident over the past year in countries such as Saudi Arabia, Ethiopia, Uzbekistan, and China, where the authorities imposed further restrictions following the political uprisings in Egypt and Tunisia, in which social media played a key role.

To illuminate the nature of these evolving threats and identify areas of growing opportunity, Freedom House has conducted a comprehensive study of internet freedom in 47 countries around the globe. This report is the third in its series and focuses on developments that occurred between January 2011 and May 2012. The previous edition, covering 37 countries, was published in April 2011. *Freedom on the Net 2012* assesses a greater variety of political systems than its predecessors, while tracing improvements and declines in the countries examined in the previous two editions. Over 50 researchers, nearly all based in the countries they analyzed, contributed to the project by researching laws and practices relevant to the internet, testing the accessibility of select websites, and interviewing a wide range of sources.

This year's findings indicate that restrictions on internet freedom in many countries have continued to grow, though the methods of control are slowly evolving and becoming less visible. Of the 47 countries examined, 20 have experienced a negative trajectory since January 2011, with Bahrain, Pakistan, and Ethiopia registering the greatest declines. In Bahrain, Egypt, and Jordan, the downgrades reflected intensified censorship, arrests, and violence against bloggers as the authorities sought to quell public calls for political and economic reform. Declines in Mexico occurred in the context of increasing threats of violence from organized crime, which began to directly influence free speech online. Ethiopia presented an unusual dynamic of growing restrictions in a country with a tiny population of users, possibly reflecting a government effort to establish more sophisticated controls before allowing access to expand. And Pakistan's downgrade reflected extreme punishments meted out for dissemination of allegedly blasphemous messages and the increasingly aggressive efforts of the telecom regulator to censor content transmitted via information and communications technologies (ICTs).

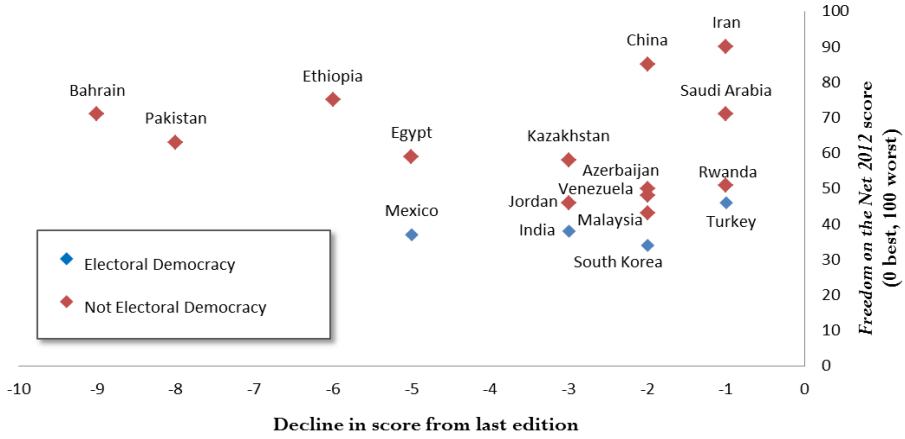
Sanja Kelly is the project director for *Freedom on the Net* at Freedom House. **Sarah Cook** is a senior research analyst at Freedom House.

At the same time, 14 countries registered a positive trajectory. In some countries—such as Tunisia, Libya, and Burma—this was the result of a dramatic regime change or political opening. Elsewhere—as in Georgia, Kenya, and Indonesia—the improvements reflected a growing diversity of content and fewer cases of arrest or censorship than in previous years. The remaining gains occurred almost exclusively in established democracies, highlighting the crucial importance of broader institutions of democratic governance—such as elected representatives, free civil society, and independent courts—in upholding internet freedom. While proposals that could negatively affect internet freedom did emerge in democratic states, civil society, the media, and the private sector were more likely to organize successful campaigns to prevent such proposals from being formally adopted, and the courts were more likely to reverse them. Only 4 of the 20 countries that recently experienced declines are considered electoral democracies (see figure below).

Despite the noted improvements, restrictions on internet freedom continue to expand across a wide range of countries. Over the past decade, governments have developed a number of effective tools to control the internet. These include limiting connectivity and infrastructure, blocking and filtering content that is critical of the regime, and arresting users who post information that is deemed undesirable. In 2011 and 2012, certain methods that were previously employed only in the most oppressive environments became more widely utilized.

To counter the growing influence of independent voices online, an increasing number of states are turning to proactive manipulation of web content, rendering it more challenging for regular users to distinguish between credible information and government propaganda. Regimes are covertly hiring armies of pro-government bloggers to tout the official point of view, discredit opposition activists, or disseminate false information about unfolding events. This practice was in the past largely limited to China and Russia, but over the last year, it has been adopted in more than a quarter of the countries examined. The Bahraini authorities, for example, have employed hundreds of "trolls" whose responsibility is to scout popular domestic and international websites, and while posing as ordinary users, attack the credibility of those who post information that reflects poorly on the government.

INTERNET FREEDOM AND DEMOCRACY



Of the 17 countries that experienced numerical declines since the 2011 edition of *Freedom on the Net,* only four are designated as electoral democracies by Freedom House's flagship publication *Freedom in the World.* Another three countries included for the first time in *Freedom on the Net 2012* showed a negative trajectory since January 2011: Sri Lanka, Syria, and Uzbekistan. None of the three are electoral democracies.

Both physical and technical attacks against online journalists, bloggers, and certain internet users have also been on the rise in 2011 and 2012, demonstrating that the tactics previously used against opposition journalists are now being applied to those writing in the online sphere as well. Moreover, the attacks have become more violent. In Azerbaijan, for example, a prominent journalist and contributor to several online news sites died of stab wounds after being attacked by unknown assailants. In Mexico, for the first time, individuals who had circulated information online about organized crime and corruption were brutally murdered, with the killers often leaving notes that cited the victim's online activities.

As another method of controlling speech and activism online, governments have imposed temporary shutdowns of the internet or mobile phone networks during mass protests, political events, or other sensitive times. While the most widely reported example occurred in Egypt in January 2011, this report's findings reveal that both nationwide and localized shutdowns are becoming more common. Prior to its downfall, the Qadhafi regime in Libya shut off the internet nationwide in March 2011, and large swaths of the country remained disconnected until August 2011. Select regions in Syria have experienced repeated internet shutdowns during 2011 and 2012, as the regime has tried to prevent citizens from spreading information and videos about the government's attacks on civilians. Localized internet shutdowns also occurred in China and Bahrain during antigovernment protests, and localized mobile phone shutdowns occurred in India and Pakistan due to security concerns.

Based on the types of controls implemented, many of the countries examined in this edition of *Freedom on the Net* can be divided into three categories:

1. **Blockers:** In this set of countries, the government has decided to block a large number of politically relevant websites, often imposing complete blocks on certain social-media platforms. The state has also invested significant resources in technical capacity and manpower to identify content for blocking. Among the countries that fall into this category are Bahrain, China, Ethiopia, Iran, Saudi Arabia, Vietnam, Syria, Thailand, and Uzbekistan. Although most of these governments employ a range of other tactics to curb internet freedom—including imposing pressure on bloggers and internet service providers, hiring pro-government commentators, and arresting users who post comments that are critical of the authorities—they use blocking and filtering as a key tool for limiting free expression. Over the past year, governments in this group have continued to refine their censorship apparatus and devoted greater energy to frustrating user attempts to circumvent the official blocking.

2. **Nonblockers:** In this category, the government has not yet started to systematically block politically relevant websites, though the authorities may have demonstrated interest in restricting online content, particularly after witnessing the role online tools can play in upending the political status quo. Most often, these governments seek the appearance that their country has a free internet, and prefer to employ less visible or less traceable censorship tactics, such as behind-the-scenes pressure from government agents to delete content, or anonymous cyberattacks against influential news sites at politically opportune times. These states also tend

to have a harsh legal framework surrounding free speech, and in recent years have arrested individuals who posted online information that is critical of the government. Among the countries that fall into this category are Azerbaijan, Egypt, Jordan, Malaysia, Venezuela, and Zimbabwe.

3. **Nascent blockers:** These countries—including Belarus, Sri Lanka, Pakistan, and Russia—appear to be at a crossroads. They have started imposing politically motivated blocks, but the system has not yet been institutionalized, and it is often sporadic. For example, in Russia, the government officially blocks material deemed to promote "extremism," but due to the vague definition of extremism, political websites are occasionally blocked as well. In addition, regional courts in Russia have at times ordered the blocking of websites that unveil local corruption or challenge local authorities. Other countries in this group, such as Pakistan, have seriously considered instituting nationwide filtering, but have not yet implemented it, thus not fully crossing into the first category.

Despite the growing threats, the study's findings reveal a significant uptick in citizen activism related to internet freedom, which has produced several notable mobilization efforts and legislative victories. In several European countries, fierce public opposition to the Anti-Counterfeiting Trade Agreement (ACTA) has prompted governments to step away from ratification of the treaty. In Pakistan, nongovernmental organizations (NGOs) and activists played a key role in exposing and resisting the government's plan to impose systematic, nationwide filtering. In Turkey, demonstrations against a proposal to implement mandatory filtering of content deemed "harmful" to children and other citizens drew as many as 50,000 people, prompting the government to back down and render the system voluntary. In the United States, campaigns by civil society and technology companies helped to halt passage of the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA), which were criticized for their potentially negative effects on free speech. The simultaneous blacking out of popular websites by their administrators as a form of protest helped increase public awareness of the two bills, and the tactic has since been repeated in countries like Jordan and Italy in the face of potentially restrictive legislation.

In largely democratic settings, the courts have started to play an instrumental role in defending internet freedom and overturning laws that may infringe on it. In Hungary, the Constitutional Court decided in December 2011 that the country's restrictive new media regulations would not be applicable to online news sources and portals. In South Korea in August 2012, the Constitutional Court issued its third decision favorable to internet freedom in two years, ruling against the real-name registration system. In countries where the judiciary is not independent, public and international pressure ultimately yielded executive branch decisions that nullified negative court rulings. In Azerbaijan, Bahrain, China, Egypt, Syria, Russia, and Saudi Arabia, at least one jailed blogger or internet activist was pardoned or released from extralegal detention following a high-profile campaign on his or her behalf. And in a dramatic reversal from previous practice, dozens of activists were released from prison in Burma, though the restrictive laws under which they had been jailed remained in place.

Since 2011, China has exerted a greater influence in the online world, emerging as an incubator for sophisticated new types of internet restrictions. The Chinese method for controlling social-media content—restricting access to international networks while coercing their domestic alternatives to robustly censor and monitor user communications according to Communist Party directives—has become a particularly potent model for other authoritarian countries. Belarus's autocratic president has praised China's internet controls, and Uzbekistan has introduced several social-media platforms on which users must register with their real names and administrators have preemptively deleted politically sensitive posts. In Iran, a prominent internet specialist likened the intended outcome of the country's proposed National Internet scheme to the Chinese censorship model, with users enjoying "expansive local connections," but having their foreign communications filtered through a "controllable channel." Meanwhile, reports have emerged of Chinese experts, telecommunications companies, or hackers assisting the governments of Ethiopia, Libya, Sri Lanka, Iran, and Zimbabwe with attempts to enhance their technical capacity to censor, monitor, or carry out cyberattacks against regime opponents.

Alongside China, authoritarian countries such as Russia, Tajikistan, and Uzbekistan have recently increased efforts on the international stage to institutionalize some of the restrictions they already implement within their own borders. For example, this coalition of states in 2011 submitted to the United Nations General Assembly a proposal for an internet "code of conduct," which would, among other things, legitimize censoring of any website that "undermines political and social order." Moreover, some of these countries have been at the forefront of an effort to expand the mandate of the International Telecommunication Union—a UN agency—to include certain internet-related matters, which could negatively impact free expression, user privacy, and access to information.

KEY TRENDS

Freedom on the Net 2012 identifies a shifting set of tactics used by various governments to control the free flow of information online. While blocking and filtering remain the preferred methods of restriction in many of the states examined, a growing set of countries have chosen other tools to limit political and social speech that they view as undesirable. These alternative tactics include (1) introduction of vague laws that prohibit certain types of content, (2) proactive manipulation, (3) physical attacks against bloggers and other internet users, and (4) politically motivated surveillance.

New Laws Restrict Free Speech and Prompt Arrests of Internet Users

Responding to the rise of user-generated content, governments around the world are introducing new laws that regulate online speech and prescribe penalties for those found to be in violation of the established rules. The threat in many countries comes from laws that are ostensibly designed to protect national security or citizens from cybercrime, but which are so broadly worded that they can easily be turned on political opponents. In Ethiopia, for example, a prominent dissident blogger

was recently sentenced under an antiterrorism law to 18 years in prison for publishing an online article that called for greater political freedom. In Egypt, after the fall of President Hosni Mubarak in early 2011, several bloggers were detained and sentenced to prison for posts that were critical of the military or called for protests against military rule.

Countries that passed a new law in 2011-2012 that negatively impacts internet freedom: *Argentina, Bahrain, Belarus, Burma, China, India, Indonesia, Iran, Kazakhstan, Kyrgyzstan, Malaysia, Mexico, Pakistan, Russia, Saudi Arabia, Sri Lanka, Syria, Thailand, Vietnam*

Of the 47 countries analyzed in this edition, 19 have passed new laws or other directives since January 2011 that could negatively affect free speech online, violate users' privacy, or punish individuals who post certain types of content. In Saudi Arabia, a new law for online media, which took effect in February 2011, requires all news websites and websites that host video or audio content to register with the government. Similarly, the government of Sri Lanka issued a directive that requires websites "carrying any content relating to Sri Lanka" to register for accreditation with the Ministry of Mass Media and Information, whether they are based inside or outside the country. While the authorities often claim that such regulations will "protect" online journalists or users, in effect they make it easier to block and fine websites containing content that is politically or socially unacceptable to the government.

An increasing number of countries are passing laws or interpreting current legislation so as to make internet intermediaries legally liable for the content posted through their services. For instance, in April 2012, Malaysia's parliament passed an amendment to the 1950 Evidence Act that holds the hosts of online forums, news outlets, blogging services, and businesses providing WiFi responsible for any seditious content posted by anonymous users. In Thailand, pressure on intermediaries intensified in May 2012 after a forum moderator for the popular online news outlet *Prachatai* received a suspended eight-month jail sentence and a fine for not deleting quickly enough an anonymous reader's criticism of the royal family.

As a consequence, intermediaries in some countries are voluntarily taking down or deleting potentially offending websites or posts on social networks to avoid legal liability. In the most extreme example, intermediary liability in China has resulted in private companies maintaining whole divisions responsible for monitoring the content of blogs, microblogs, search engines, and online forums, deleting tens of millions of messages or search results a year based on administrators' interpretation of both long-standing taboos and daily Communist Party directives. Reports have emerged of similar preemptive deletion by moderators in other countries, such as Kazakhstan, Vietnam, and Saudi Arabia.

In India, amid several court cases regarding intermediaries' responsibility for hosting illegal content and new guidelines requiring intermediaries to remove objectionable content within 36 hours of notice, much evidence has surfaced that intermediaries are taking down content without fully evaluating or challenging the legality of the request. For example, in December 2011, the website "Cartoons against Corruption" was suspended by its hosting company after a complaint filed with

the Mumbai police alleged that the site's cartoons ridiculed India's parliament and national emblems. As a result of such dynamics, large swaths of online content are disappearing, and the losses are far more difficult to reverse than the mere blocking of a website.

Laws that restrict free speech are also forcing a growing number of internet users and content providers into court, or putting them behind bars. Two Tunisians were given seven-year prison sentences in March 2012 for publishing online content that was perceived as offensive to Islam and "liable to cause harm to public order or public morals," an offense found in the largely unreformed penal code from the era of autocratic former president Zine el-Abidine Ben Ali. In some countries, harsh penalties are also applicable to content transmitted through other ICTs as evidenced in the case of a Pakistani man who was sentenced to death in 2011 for sending an allegedly blasphemous text message via his mobile phone. In Thailand, a 61-year-old man was sentenced to 20 years in prison after he allegedly sent four mobile phone text messages that were deemed to have insulted the monarchy; several months into his sentence he died in prison due to illness.

In 26 of the 47 countries assessed, a blogger or other ICT user was arrested for content posted online or sent via mobile phone text message.

Paid Commentators, Hijacking Attacks Spread Misinformation

In addition to taking steps to remove unfavorable content from the internet, a growing number of governments are investing significant resources and using deceptive tactics to manipulate online discussions. Already evident in a small sets of countries assessed in previous editions of *Freedom on the Net*, the phenomenon of paid pro-government commentators has spread over the past two years, appearing in 14 of the 47 countries examined in this study. Even where such dynamics had previously emerged, their prevalence has evolved and expanded, as governments seek to undermine public trust in independent sources of information and counter the influence of particular websites and activists.

Countries where pro-government commentators were used to manipulate internet discussions in 2011-2012: *Bahrain, Belarus, China, Cuba, Egypt, Ethiopia, Iran, Malaysia, Russia, Saudi Arabia, Syria, Thailand, Ukraine, Venezuela*

Paid commentators rarely reveal their official links when posting online, nor do governments inform taxpayers that state funds are being spent on such projects. Moreover, some of the tactics used to manipulate online discussions—including spreading false statements or hacking into citizens' accounts—are illegal in many of the countries where they occur. In Cuba, an estimated 1,000 bloggers recruited by the government have disseminated damaging rumors about the personal lives of the island's influential independent bloggers.

In some countries, such as Bahrain and Malaysia, the government or ruling party is reported to have hired international public relations firms to engage in such activities on its behalf. In Russia, media reports indicated that the ruling party planned to invest nearly $320,000 to discredit prominent

blogger Aleksey Navalny, including through a possible scheme to disseminate compromising videos using a Navalny look-alike. China's paid pro-government commentators, known informally as the "50 Cent Party," are estimated to number in the hundreds of thousands, while an Iranian official claimed in mid-2011 that 40 companies had received over $56 million to produce pro-government digital content.

Rather than creating their own websites or social-media accounts to influence online discussion, some governments or their supporters have hijacked the online presence of their critics and altered the content posted in an effort to deceive the growing audience of citizens who are shifting from state-controlled media to alternative sources of news. In Jordan, the popular *Amman News* website was hacked, and a sensitive statement by tribal leaders calling for reforms was forcibly deleted. In Burma, prior to the government's shift to a more tolerant attitude toward dissent, the website of the exile news outlet *Irrawaddy* was hacked, and fake news items that could discredit the outlet or sow discord among the opposition were posted. In Egypt, in the run-up to elections in late 2011 and early 2012, a Facebook account used for reporting electoral violations was hacked, and pro-military messages were disseminated.

***Countries where government critics faced politically motivated cyberattacks in 2011-2012**: Bahrain, Belarus, Burma, China, Egypt, Iran, Jordan, Kazakhstan, Libya, Malaysia, Mexico, Russia, Saudi Arabia, Syria, Thailand, Uzbekistan, Venezuela, Vietnam, Zimbabwe*

Some hijackings or impersonations have targeted influential individuals rather than news websites. In early 2012, a fake Twitter account was created using the name of a British-Syrian activist whose reports on a massacre by Syrian government forces had drawn international attention. The fake account's postings combined plausible criticism of the regime with comments that seemed to incite sectarian hatred. In one of the most notable examples of this dynamic, since August 2011, the blogs and Twitter accounts of at least two dozen government critics and prominent figures in Venezuela—including journalists, economists, artists, and writers—have been hacked and hijacked. The messages disseminated in their names have ranged from support for the government's economic policy and criticism of the opposition presidential candidate to threatening comments directed at other users.

Physical Attacks against Government Critics Intensify

Governments and other powerful actors are increasingly resorting to physical violence to punish those who post critical content online, with sometimes fatal consequences. In 19 of the 47 countries assessed, a blogger or internet user was tortured, disappeared, beaten, or brutally assaulted. In five countries, an activist or citizen journalist was killed in retribution for information posted online that exposed human rights abuses.

This rise in violence has taken different forms in different countries. In some repressive states—like China, Iran, Saudi Arabia, Syria, and Vietnam—reports abound of individuals being tortured in

custody after being detained for online activities. In Bahrain, the moderator of an online forum was killed in police custody in April 2011, within one week of his arrest. His body showed clear signs of abuse, and a commission of inquiry subsequently confirmed his death under torture. In other countries, such as Cuba, the authorities have shifted tactics, replacing long-term imprisonment with extralegal detentions, intimidation, and occasional beatings. In Sri Lanka and Uzbekistan, online critics of the government have disappeared under mysterious circumstances, with previous official harassment fueling suspicions that they are being illegally detained.

In China, following online calls for a Tunisian-style Jasmine Revolution in February 2011, dozens of bloggers, lawyers, and activists who had large followings on social-media sites were abducted in one of the worst crackdowns on free expression in recent memory. Several of those detained were sentenced to long prison terms, but most were released after weeks of incommunicado detention, with no legal record or justification for their arrest. Many reported being beaten, deprived of sleep, or otherwise abused, with at least one lawyer contracting tuberculosis within only 21 days in custody.

Countries where a blogger or ICT user was physically attacked or killed in 2011-2012: *Azerbaijan, Bahrain, Burma, China, Cuba, Egypt, Indonesia, Iran, Jordan, Kazakhstan, Libya, Mexico, Pakistan, Saudi Arabia, Sri Lanka, Syria, Thailand, Uzbekistan, Vietnam*

In a newly emerging phenomenon, bloggers and citizen journalists in a number of countries were specifically targeted by security forces while reporting from the field during periods of unrest or armed conflict. In Kazakhstan, a blogger was reportedly assaulted by police who held a pistol to his head after he uploaded video footage to YouTube that showed local residents protesting a government crackdown. In Egypt, several well-known online activists were badly injured during police and military assaults on protesters, causing one blogger to lose his right eye and another to suffer 117 birdshot wounds. The circumstances surrounding the attacks raised suspicions that the individuals had been singled out by members of the security forces, who either responded to their filming of events or recognized them as influential online opinion leaders. In both Libya and Syria, citizen journalists who had gained international prominence for their live online video broadcasts were killed in targeted attacks by government forces.

Bloggers and citizen journalists are also facing violence by nonstate actors or unidentified attackers. But even in these cases, impunity for the perpetrators or possible pro-government motives have given the assaults an appearance of at least tacit official approval. In Indonesia, Islamists beat a man who had started a Facebook group promoting atheism, then reported him to the authorities. Police arrived and arrested the user, who was subsequently prosecuted, while the attackers went unpunished. In Thailand, a professor leading a petition campaign to amend restrictive lèse-majesté legislation was assaulted by two unidentified people in an incident that rights groups believed was connected to his advocacy. In some countries, attacks by nonstate actors have proved fatal, as with the killings in Mexico mentioned above. In Pakistan, a series of bombing attacks against cybercafes by Islamist militants have led to several deaths and dozens of injuries.

Some of these attacks against online writers are especially cruel. In Jordan, a female blogger was stabbed in the stomach. In Kazakhstan, reporters from an online television station were beaten with baseball bats. In Egypt, an online columnist suffered broken wrists after being beaten and sexually assaulted. In Syria, the body of a freelance photographer killed by security forces was mutilated. And in China and Uzbekistan, detained activists and journalists were forcibly medicated with psychiatric drugs.

However, extralegal harassment of online activists and bloggers is not always so extreme. In a wide range of countries, intimidation takes more mundane but also more pervasive forms. In Bahrain, Belarus, Cuba, Turkey, Thailand, and Vietnam, individuals have been fired from their jobs, barred from universities, or banned from traveling abroad after posting comments that criticize the government or otherwise cross "red lines." In Russia and Azerbaijan, the harassment has expanded to activists' families, with parents receiving calls from security personnel who press them to stop their adult children's activism.

In addition to individual users, the offices of news websites or free expression groups have been subject to arbitrary attacks. In Belarus, Jordan, and Thailand, security forces or unidentified armed men raided the editorial offices of popular online news and information sites, confiscating or destroying equipment. In Venezuela, the offices of a civil society group that is active in defending online freedom of expression were burglarized on two occasions. And in Sri Lanka, an arson attack destroyed the offices of a popular online news site that had supported the president's competitor in the 2010 election.

Surveillance Increases, with Few Checks on Abuse

Many governments are seeking less visible means to infringe upon internet freedom, often by increasing their technical capacity or administrative authority to access private correspondence via ICTs. Governments across the full spectrum of democratic performance—including South Korea, Kenya, Thailand, Egypt, and Syria—have enhanced their surveillance abilities in recent years or announced that they intend to do so. Of the 19 countries that passed new regulations negatively affecting internet freedom in 2011 and early 2012, 12 disproportionately enhanced surveillance or restricted user anonymity. Although some interception of communications may be necessary for fighting crime or preventing terrorist attacks, surveillance powers are abused for political ends in many countries. Even in democratic settings, proper procedures are not always followed, resulting in violations of user privacy.

In the more repressive and technically sophisticated environments, authorities engage in bulk monitoring of information flows, often through a centralized point. Intelligence agencies then gain direct access to users' communications across a range of platforms—mobile phone conversations, text messages, e-mail, browsing history, Voice over IP discussions, instant messaging, and others. The most advanced systems scan the traffic in real time, with preset keywords, e-mail addresses, and phone numbers used to detect communications of interest to the authorities. Voice-recognition

software is being applied in a growing number of countries to scan spoken conversations for either sensitive keywords or particular individuals' voices. Even in less technologically advanced settings, the government has little trouble accessing user communications once an offender has been identified, as service providers can be required to retain data and content and submit them to the authorities upon request. In most authoritarian countries, security services can intercept communications or obtain user data from service providers without a judicial warrant. Some democratic governments also have highly advanced monitoring equipment, but court approval is needed to access user information, and what is retained usually involves the time and recipients of communications rather than their actual content.

Surveillance in nondemocratic countries is often political in nature, aimed at identifying and suppressing government critics and human rights activists. Such monitoring can have dire repercussions for the targeted individuals, including imprisonment, torture, and even death. In Belarus, Bahrain, Ethiopia, and elsewhere, activists found that their e-mails, text messages, or Skype communications were presented to them during interrogations or used as evidence in politicized trials. In Libya, following Mu'ammar al-Qadhafi's ouster, journalists discovered a sophisticated monitoring center and a storage room filled with dossiers of the online activities of both Libyans and foreigners. Such revelations have raised serious ethical questions and public relations problems for Chinese companies and some firms based in developed democracies that have been known to supply surveillance tools to repressive regimes.

Even governments with sophisticated technological capabilities are finding that it is not always possible to trace a particular message to its author. Several countries have therefore passed regulations requiring real-name user registration, whether at the point of access, via a service provider, or directly with the government. In Iran, new regulations require cybercafe customers to submit personal information before using a computer. In China, major microblogging services were given a March 2012 deadline to implement real-name registration for their users. Kazakhstan, Syria, and Saudi Arabia also passed regulations enhancing restrictions on user anonymity.

A large number of middle-performing countries—some of them democracies—are also expanding their surveillance abilities. While there are fewer fears in these settings that the government will engage in pervasive, politically motivated monitoring, rights safeguards and oversight procedures are lagging far behind the authorities' technical capacities and legal powers. For example, in a number of democratic or semidemocratic states—such as Thailand, Indonesia, Malaysia, India, and Mexico—regulations passed over the last year and a half have expanded the authority of security and intelligence services to intercept communications, sometimes without requiring a court order. Even when a judge's permission is required by law, approval is sometimes granted almost automatically due to inadequate judicial independence. In a classic example of the legal ambiguities surrounding surveillance in some countries, Indonesia has nine different laws authorizing surveillance, the most recent of which was passed in October 2011. Each law sets different standards of accountability, with only some requiring judicial approval.

The proliferation of surveillance without appropriate safeguards almost inevitably leads to abuse or inadvertent violations of user privacy. A range of countries have experienced scandals in recent years involving individual politicians or law enforcement agents who misused their powers to spy on opponents or engage in extortion. In 2011, India's federal authorities had to rein in the availability of certain interception equipment acquired after the 2008 terrorist attacks in Mumbai, as it had been improperly employed by state governments. In April 2012, Mexico's new Geolocation Law came into effect, allowing law enforcement agencies, including certain low-level public servants, to gain access to the location data of mobile phone users, without a warrant and in real time. Although such tools are intended to facilitate the apprehension of drug traffickers and violent criminals, there are credible fears that user data will fall into the wrong hands, as organized crime groups have infiltrated Mexico's law enforcement agencies. Indeed, previously collected data on mobile phone purchasers were found to have already been posted for sale online.

Even in more developed democracies, where surveillance generally requires judicial approval and oversight mechanisms are fairly robust, concerns have increased that the government is becoming too intrusive. In 2012, the British government announced a proposal to expand the existing surveillance measures and require ISPs to keep certain details of their customers' social networking activity, e-mail, internet calls, and gaming for a period of 12 months. In the United States, controversial provisions of the PATRIOT Act were renewed in May 2011, and legal ambiguities regarding data stored in the "cloud" have prompted concerns among experts. Pending legislation in Australia and South Africa has come under criticism for broadening service providers' surveillance obligations and legalizing the mass monitoring of transnational communications, respectively.

COUNTRIES AT RISK

After reviewing the findings for the 47 countries covered in this edition of *Freedom on the Net*, Freedom House has identified seven that are at particular risk of suffering setbacks related to internet freedom in late 2012 and in 2013. A number of other countries showed deterioration over the past two years and may continue to decline, but the internet controls in those states—which include Bahrain, China, Iran, Syria, and Ethiopia—are already well developed. By contrast, in most of the countries listed below, the internet remains a relatively unconstrained space for free expression, even if there has been some obstruction of internet freedom to date. These countries also typically feature a repressive environment for traditional media and have recently considered or introduced legislation that would negatively affect internet freedom.

Malaysia

Although the Malaysian government places significant restrictions on traditional media, it has actively encouraged internet and mobile phone access, resulting in an internet penetration rate of over 60 percent and a vibrant blogosphere. No politically sensitive websites are blocked, and a

notorious security law was repealed in early 2012, but other infringements on internet freedom have emerged in the last year. Prominent online news outlets and opposition-related websites have suffered cyberattacks at politically critical moments. Bloggers have faced arrest or disproportionate defamation suits for criticizing government officials or royalty. And legal amendments rendering intermediaries liable for seditious comments were passed in April 2012, as were changes to the penal code that criminalized "any activity detrimental to parliamentary democracy." In the watershed general elections of March 2008, the ruling coalition lost its two-thirds parliamentary majority for the first time since 1969, and the use of the internet for political mobilization was widely perceived as contributing to the opposition's electoral gains. As Malaysia prepares for another set of highly contentious elections scheduled to take place by April 2013, greater efforts by the government and ruling party to increase their influence over the internet are anticipated.

Russia

Given the elimination of independent television channels and the tightening of press restrictions since 2000, the internet has become Russia's last relatively uncensored platform for public debate and the expression of political opinions. However, even as access conditions have improved, internet freedom has eroded. Since January 2011, the obstacles to freedom of expression online have evolved, with massive distributed denial-of-service (DDoS) attacks, smear campaigns to discredit online activists, and extralegal intimidation of average users intensifying. Nevertheless, online tools—such as social-media networks and video-sharing platforms—played a critical role in galvanizing massive public protests that began in December 2011. The government, under the renewed leadership of President Vladimir Putin, subsequently signaled its intention to tighten control over internet communications. Since May 2012, the parliament has passed legislation that recriminalized defamation and expanded the blacklisting of websites, while prominent bloggers face detention and questionable criminal prosecutions. As the Kremlin's contentious relationship with civil society and internet activists worsens and the country prepares for regional elections in October, such controls appear likely to increase.

Sri Lanka

Although internet penetration remains at around 15 percent of the population, since 2007 there has been an incremental growth in the influence and use of online news sites and social-media tools for civic and political mobilization. The government has responded with arbitrary blocks on news websites and occasional attacks against their staff, a dynamic that has intensified since January 2011. In November, the government suddenly announced a policy requiring websites that carry "any content related to Sri Lanka" to register with the authorities, and a prominent online journalist and cartoonist remains "disappeared," apparently in police custody. The country's judicial system has proven a poor safeguard against these infringements, with the Supreme Court recently refusing to even open proceedings on a petition that challenged the arbitrary blocking of five prominent websites focused on human rights and governance. In June 2012, police raided two news websites'

offices, and in July the government announced new registration fees for such sites, illustrating the potential for further assaults on internet freedom in the coming year.

Libya

The political unrest and armed conflict in Libya, which in 2011 led to a dramatic regime change, was also reflected in the country's internet freedom landscape. The online environment was notably more open after the rebel victory in October 2011 than during the Qadhafi era or the period of civil conflict, when the internet was shut off in large areas of the country. A frenzy of self-expression has since erupted online, as Libyans seek to make up for lost time. Nevertheless, periodic electricity outages, residual self-censorship, and weak legal protections pose ongoing challenges to internet freedom. Meanwhile, the passage and subsequent overturning in mid-2012 of restrictive legislation under the guise of preventing the glorification of the Qadhafi regime highlighted the ongoing threats to online expression as different actors seek to assert their authority. Such dynamics, alongside factional fighting and recent violence in response to a YouTube video that insulted Islam, illustrate the potential pitfalls for internet freedom in Libya as the country embarks on a transition to democracy under the leadership of a new legislative body elected in July.

Azerbaijan

As the host of two high-profile international events in 2012—the Eurovision Song Contest in May and the Internet Governance Forum (IGF) in November—the government of Azerbaijan has been eager to promote itself as a leader of ICT innovation in the region. Indeed, with few websites blocked, the internet remains much less restricted than print and broadcast media, the main sources of information for most citizens. Nevertheless, as internet usage has increased dramatically over the past two years, online tools have begun to be used for political mobilization, including a series of Arab Spring–inspired prodemocracy protests in early 2011. The authorities have responded with increased efforts to clamp down on internet activities and stifle opposition viewpoints. Rather than significantly censoring online content, the government has employed tactics such as raiding cybercafes to gather information on user identities, arresting politically active netizens on trumped-up charges, and harassing activists and their family members. In a worrisome development, the authorities ramped up their surveillance capabilities in early 2012, installing "black boxes" on a mobile phone network that reportedly enable security agencies to monitor all communications in real time. While international attention on Azerbaijan's human rights record has led to some positive developments, including the recent release of imprisoned bloggers and website editors, there is concern that after the global spotlight fades, a crackdown will ensue. Furthermore, with a presidential election expected in 2013—and online tools potentially serving as an avenue for exposing electoral fraud—the risk of additional restrictions being imposed on internet freedom in Azerbaijan over the coming year remain high.

Pakistan

Mobile phones and other ICTs have proliferated in Pakistan in recent years, spurring dynamic growth in citizen journalism and activism. The government, and particularly the Pakistan Telecommunications Authority (PTA), has responded with increasingly aggressive efforts to control the new technologies. These efforts were especially pronounced between January 2011 and mid-2012, resulting in an alarming deterioration in internet freedom from the previous year. Disconcerting developments included a ban on encryption and virtual private networks (VPNs), a death sentence imposed for transmitting allegedly blasphemous content via text message, and a one-day block on all mobile phone networks in Balochistan Province in March 2012. Several other initiatives to increase censorship—including a plan to extensively filter text messages by keyword and a proposal to develop a nationwide internet firewall—were shelved after facing resistance in the form of civil society advocacy campaigns. Despite these victories, additional restrictions on internet freedom have emerged since May 2012: a brief block on Twitter, a second freeze on mobile phone networks in Balochistan, and a new PTA directive to block 15 websites featuring content about "influential persons." Evidence has also surfaced that the government is in the process of installing sophisticated internet surveillance technologies. Together, these developments signal the government's continued commitment to controlling the internet and new media. As access expands and general elections approach in April 2013, such efforts are likely to increase.

Rwanda

The government of Rwanda under President Paul Kagame has been applauded for its commitment to economic development and reconstruction since the country's devastating genocide in 1994. Investment in ICTs over the past two decades has led to the expansion of internet and mobile phone usage. Nevertheless, internet penetration remains low at only 7 percent, and widespread poverty continues to impede access to ICTs. Moreover, alongside its generally strict control over civic and political life, the government has begun exerting greater control over digital media. In the lead-up to the presidential election in 2010, the authorities blocked the online version of an independent newspaper for six months. Other online outlets have reported government requests to delete content related to political affairs or ethnic relations. Furthermore, violence against online journalists, though sporadic, appears to be on the rise, and one editor living in exile was sentenced in absentia to two and a half years in prison in June 2011. These worrying incidents have fueled concerns that the government's firm restrictions on print and broadcast media—particularly regarding content on the ruling party or the 1994 genocide—are crossing over into the internet sphere. In one ominous sign, in August 2012 the government approved legislation that, if passed by the Senate, would enable security and intelligence services to conduct widespread surveillance of e-mail and telephone communications.

KEY INTERNET CONTROLS BY COUNTRY (JANUARY 2011 – MAY 2012)

Country (by *Freedom on the Net 2012* ranking)	Web 2.0 blocked	Notable political blocking	Localized or nationwide ICT shut down	Progov't commentators manipulate online discussions	New law /regulation increasing censorship or punishment passed	New law /regulation increasing surveillance or restricting anonymity	Blogger/ICT user arrested for political or social writings	Blogger/ICT user physically attacked or killed (incl. in custody)	Technical attacks against government critics
Estonia									
USA			X						
Germany									
Australia									
Hungary									
Italy									
Philippines									
United Kingdom									
Argentina	X				X				
South Africa									
Brazil									
Ukraine				X					
Kenya									
Georgia									
Nigeria									
South Korea		X					X		
Uganda									
Kyrgyzstan					X				
Mexico						X		X	X
India	X		X		X	X	X		
Indonesia					X	X	X	X	
Libya	X		X				X	X	X
Malaysia				X	X	X	X		X
Jordan							X	X	X

	Web 2.0 blocked	Notable political blocking	Localized or nationwide ICT shut down	Progov't commentators manipulate online discussions	New law /regulation increasing censorship or punishment passed	New law /regulation increasing surveillance or restricting anonymity	Blogger/ICT user arrested for political or social writings	Blogger/ICT user physically attacked or killed (incl. in custody)	Technical attacks against government critics
Tunisia							X		
Turkey	X	X							
Venezuela	X			X					X
Azerbaijan							X	X	
Rwanda									
Russia				X	X		X		X
Zimbabwe							X		X
Sri Lanka		X			X		X	X	
Kazakhstan	X	X	X		X	X	X	X	X
Egypt	X		X	X			X	X	X
Thailand		X		X		X	X	X	X
Pakistan		X	X			X	X	X	
Belarus		X		X	X	X	X		X
Bahrain	X	X	X	X	X		X	X	X
Saudi Arabia		X		X	X	X	X	X	X
Vietnam		X			X		X	X	X
Burma	X	X			X		X	X	X
Ethiopia	X	X		X			X		
Uzbekistan	X	X	X				X	X	X
Syria	X	X	X	X	X	X	X	X	X
China	X	X	X	X	X	X	X	X	X
Cuba	X	X		X			X	X	
Iran	X	X		X		X	X	X	X
Total # of countries	**15**	**17**	**10**	**14**	**15**	**12**	**26**	**19**	**19**

FREEDOM ON THE NET 2012: GLOBAL SCORES

Freedom on the Net aims to measure each country's level of internet and digital media freedom. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of Free (0-30 points), Partly Free (31-60 points), or Not Free (61-100 points).

Ratings are determined through an examination of three broad categories: Obstacles to Access, Limits on Content, and Violation of User Rights.

A. **Obstacles to Access:** assesses infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; and legal, regulatory and ownership control over internet and mobile phone access providers.
B. **Limits on Content:** examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
C. **Violations of User Rights:** measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

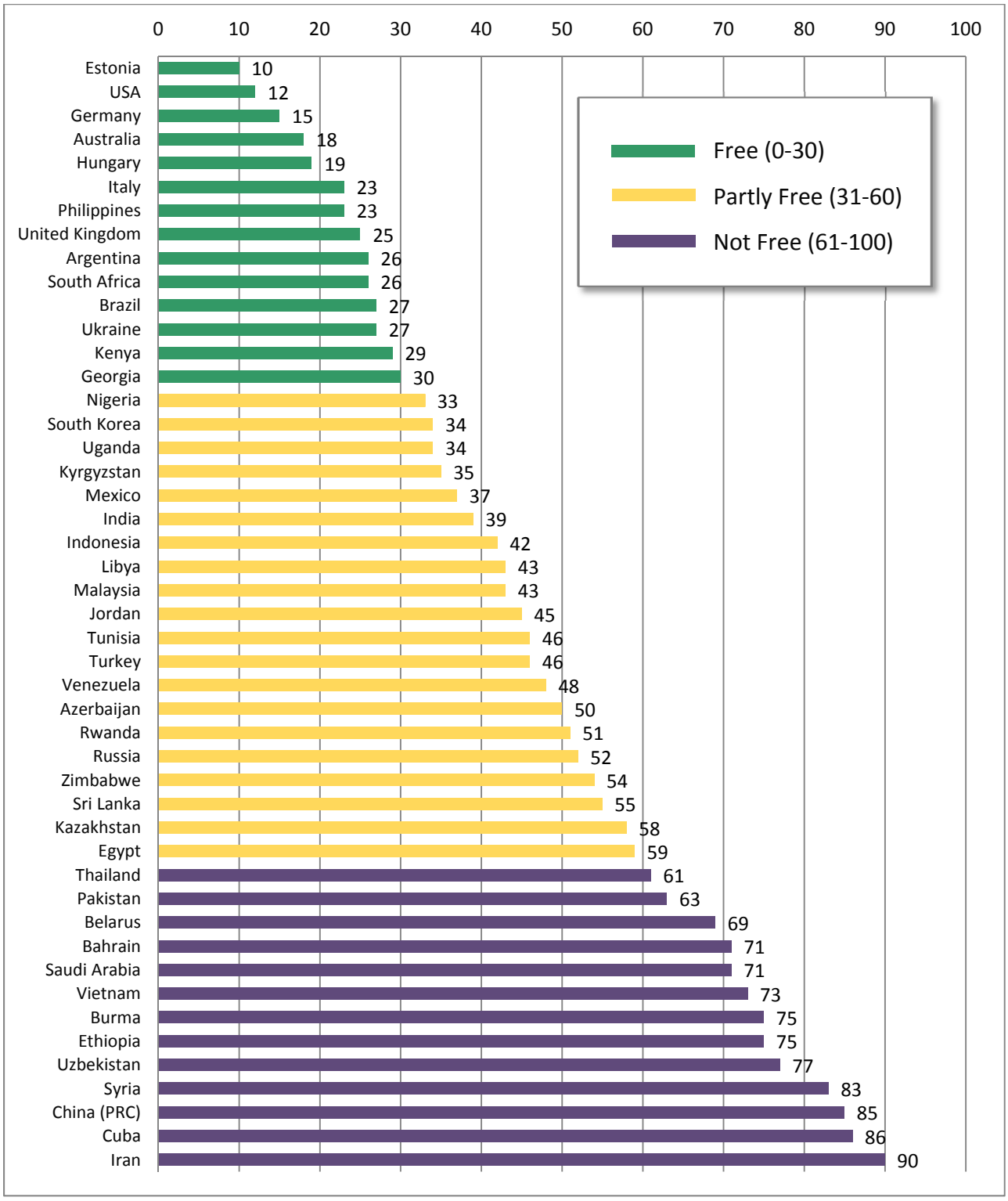
COUNTRY	*FREEDOM ON THE NET* STATUS 2012	*FREEDOM ON THE NET* TOTAL *0-100 Points*	A. SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B. SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C. SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
Estonia	**Free**	**10**	2	3	5
USA	**Free**	**12**	4	1	7
Germany	**Free**	**15**	4	3	8
Australia	**Free**	**18**	2	6	10
Hungary	**Free**	**19**	5	6	8
Italy	**Free**	**23**	4	7	12
Philippines	**Free**	**23**	10	5	8

COUNTRY	*FREEDOM ON THE NET* STATUS	*FREEDOM ON THE NET* TOTAL *0-100 Points*	A SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
United Kingdom	**Free**	**25**	1	8	16
Argentina	**Free**	**26**	9	9	8
South Africa	**Free**	**26**	8	8	10
Brazil	**Free**	**27**	7	6	14
Ukraine	**Free**	**27**	7	8	12
Kenya	**Free**	**29**	10	7	12
Georgia	**Free**	**30**	9	10	11
Nigeria	**Partly Free**	**33**	12	9	12
South Korea	**Partly Free**	**34**	3	12	19
Uganda	**Partly Free**	**34**	11	8	15
Kyrgyzstan	**Partly Free**	**35**	13	10	12
Mexico	**Partly Free**	**37**	11	11	15
India	**Partly Free**	**39**	13	9	17
Indonesia	**Partly Free**	**42**	11	11	20
Libya	**Partly Free**	**43**	18	9	16
Malaysia	**Partly Free**	**43**	10	14	19
Jordan	**Partly Free**	**45**	13	12	20
Tunisia	**Partly Free**	**46**	14	12	20
Turkey	**Partly Free**	**46**	12	17	17
Venezuela	**Partly Free**	**48**	15	14	19

COUNTRY	*FREEDOM ON THE NET* STATUS	*FREEDOM ON THE NET* TOTAL *0-100 Points*	A. SUBTOTAL: OBSTACLES TO ACCESS *0-25 Points*	B. SUBTOTAL: LIMITS ON CONTENT *0-35 Points*	C. SUBTOTAL: VIOLATIONS OF USER RIGHTS *0-40 Points*
Azerbaijan	**Partly Free**	**50**	13	16	21
Rwanda	**Partly Free**	**51**	13	19	19
Russia	**Partly Free**	**52**	11	18	23
Zimbabwe	**Partly Free**	**54**	17	14	23
Sri Lanka	**Partly Free**	**55**	16	18	21
Kazakhstan	**Partly Free**	**58**	15	23	20
Egypt	**Partly Free**	**59**	14	12	33
Thailand	**Not Free**	**61**	11	21	29
Pakistan	**Not Free**	**63**	19	18	26
Belarus	**Not Free**	**69**	16	23	30
Bahrain	**Not Free**	**71**	12	25	34
Saudi Arabia	**Not Free**	**71**	14	26	31
Vietnam	**Not Free**	**73**	16	26	31
Burma	**Not Free**	**75**	22	23	30
Ethiopia	**Not Free**	**75**	22	27	26
Uzbekistan	**Not Free**	**77**	19	28	30
Syria	**Not Free**	**83**	23	25	35
China	**Not Free**	**85**	18	29	38
Cuba	**Not Free**	**86**	24	29	33
Iran	**Not Free**	**90**	21	32	37

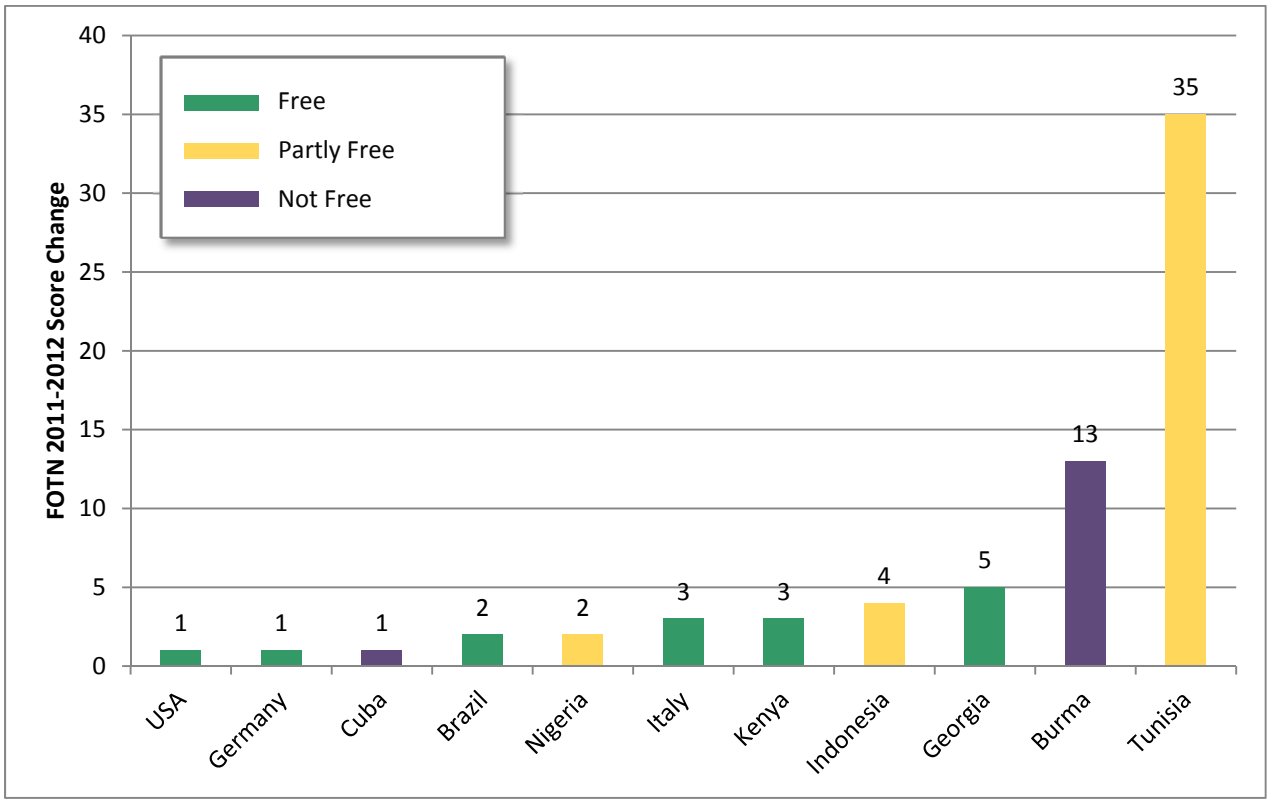
FREEDOM ON THE NET 2012: GLOBAL GRAPHS

47 COUNTRY SCORE COMPARISON (0 = Most Free, 100 = Least Free)



SCORE CHANGES: *FREEDOM ON THE NET 2011 VS. 2012*

SCORE IMPROVEMENTS

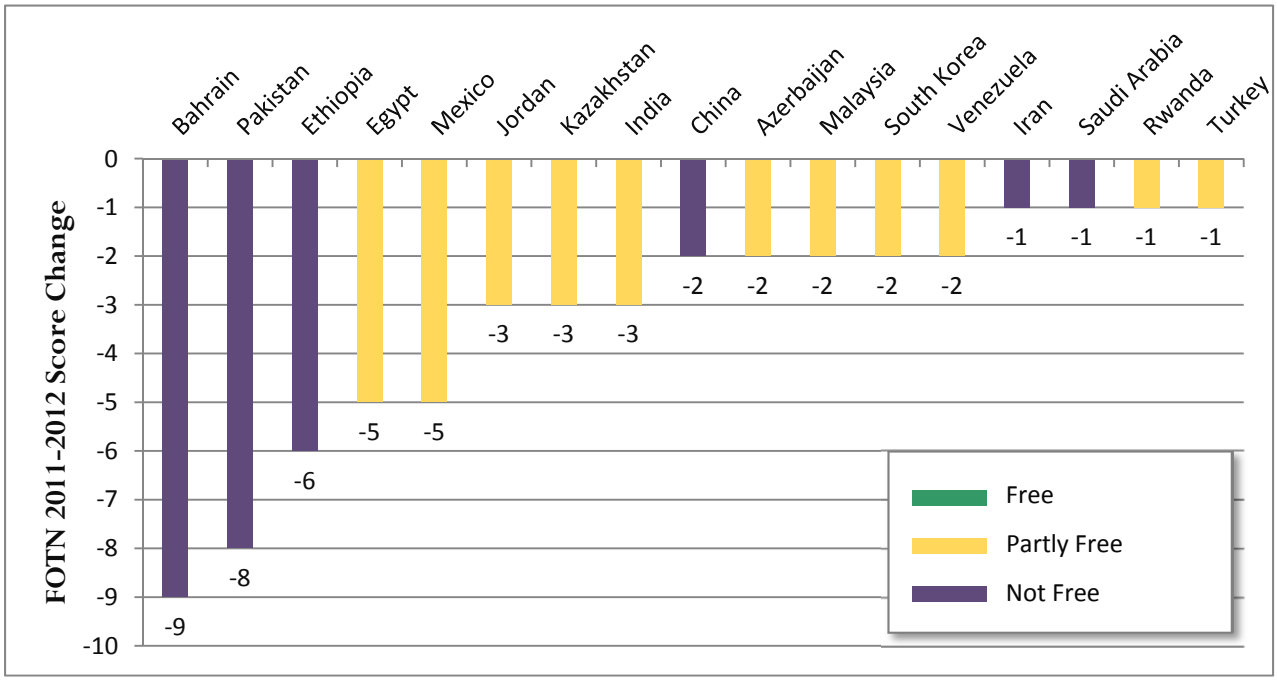


COUNTRY	FOTN 2011	FOTN 2012	TRAJECTORY
USA	13	12	Slight ↑
Germany	16	15	Slight ↑
Cuba	87	86	Slight ↑
Brazil	29	27	Slight ↑
Nigeria	35	33	Slight ↑
Italy	26	23	Notable ↑

COUNTRY	FOTN 2011	FOTN 2012	TRAJECTORY
Kenya	32	29	Notable ↑
Indonesia	46	42	Notable ↑
Georgia	35	30	Significant ↑
Burma	88	75	Significant ↑
Tunisia	81	46	Significant ↑

*A *Freedom on the Net* score decline represents a positive trajectory (↑) for internet freedom.

SCORE DECLINES



COUNTRY	FOTN 2011	FOTN 2012	TRAJECTORY
Bahrain	62	71	Significant ↓
Pakistan	55	63	Significant ↓
Ethiopia	69	75	Significant ↓
Egypt	54	59	Significant ↓
Mexico	32	37	Significant ↓
Jordan	42	45	Notable ↓
Kazakhstan	55	58	Notable ↓
India	36	39	Notable ↓
China	83	85	Slight ↓

COUNTRY	FOTN 2011	FOTN 2012	TRAJECTORY
Azerbaijan	48	50	Slight ↓
Malaysia	41	43	Slight ↓
South Korea	32	34	Slight ↓
Venezuela	46	48	Slight ↓
Iran	89	90	Slight ↓
Saudi Arabia	70	71	Slight ↓
Rwanda	50	51	Slight ↓
Turkey	45	46	Slight ↓

*A *Freedom on the Net* score increase represents a negative trajectory (↓) for internet freedom.

NO OVERALL SCORE CHANGE: CATEGORY TRAJECTORIES

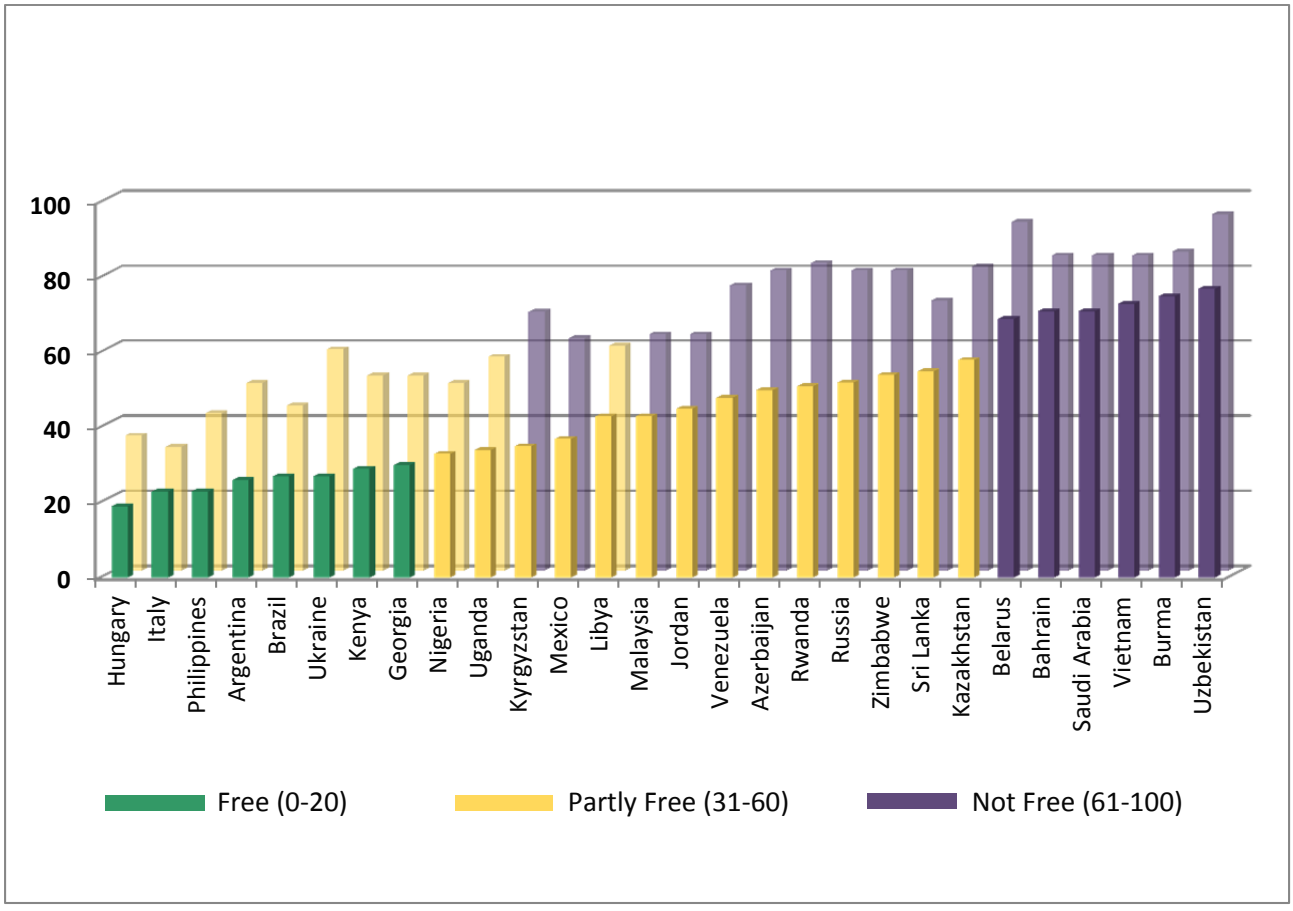
Eight countries assessed in *Freedom on the Net 2012* registered no overall score change from the previous edition. However, a closer look at the score changes within the survey's three broad categories reveals how internet freedom restrictions have evolved in nuanced and dynamic ways. Notably, the gains many of the countries listed below made in the "Obstacles to Access" category—which reflect the rise of internet and mobile phone penetration or decreased regulatory obstacles—were offset by increases in limits placed on content or violations of user rights.

COUNTRY	FOTN 2011	FOTN 2012	A. OBSTACLES TO ACCESS TRAJECTORY	B. LIMITS ON CONTENT TRAJECTORY	C. VIOLATIONS OF USER RIGHTS TRAJECTORY
Australia	18	18	Slight ↑	No change	Slight ↓
Belarus	69	69	Notable ↑	No change	Notable ↓
Estonia	10	10	No change	Slight ↓	Slight ↑
Russia	52	52	Slight ↑	Slight ↓	No change
South Africa	26	26	Slight ↓	Slight ↑	No change
Thailand	61	61	Slight ↑	Slight ↑	Notable ↓
Vietnam	73	73	No change	Slight ↓	Slight ↑
Zimbabwe	54	54	Slight ↓	Slight ↑	No change

COUNTRIES AT RISK: INTERNET FREEDOM VS. PRESS FREEDOM

Among the 47 countries covered in this study, one notable contingent of states were those where the internet remains a relatively unobstructed domain of free expression when compared to a more repressive or dangerous environment for traditional media. This difference is evident from the comparison between a country's score on Freedom House's *Freedom on the Net 2012* assessment and its score on the *Freedom of the Press 2012* study.

The figure below is a graphical representation of this phenomenon, focusing on the 28 countries in this edition where the gap between their performance on the two surveys is 10 points or greater. This difference reflects the potential pressures in both the short and long term on the space for online expression. Among the 28 are six of the seven states identified as "countries at risk": Malaysia, Russia, Sri Lanka, Libya, Azerbaijan, and Rwanda.

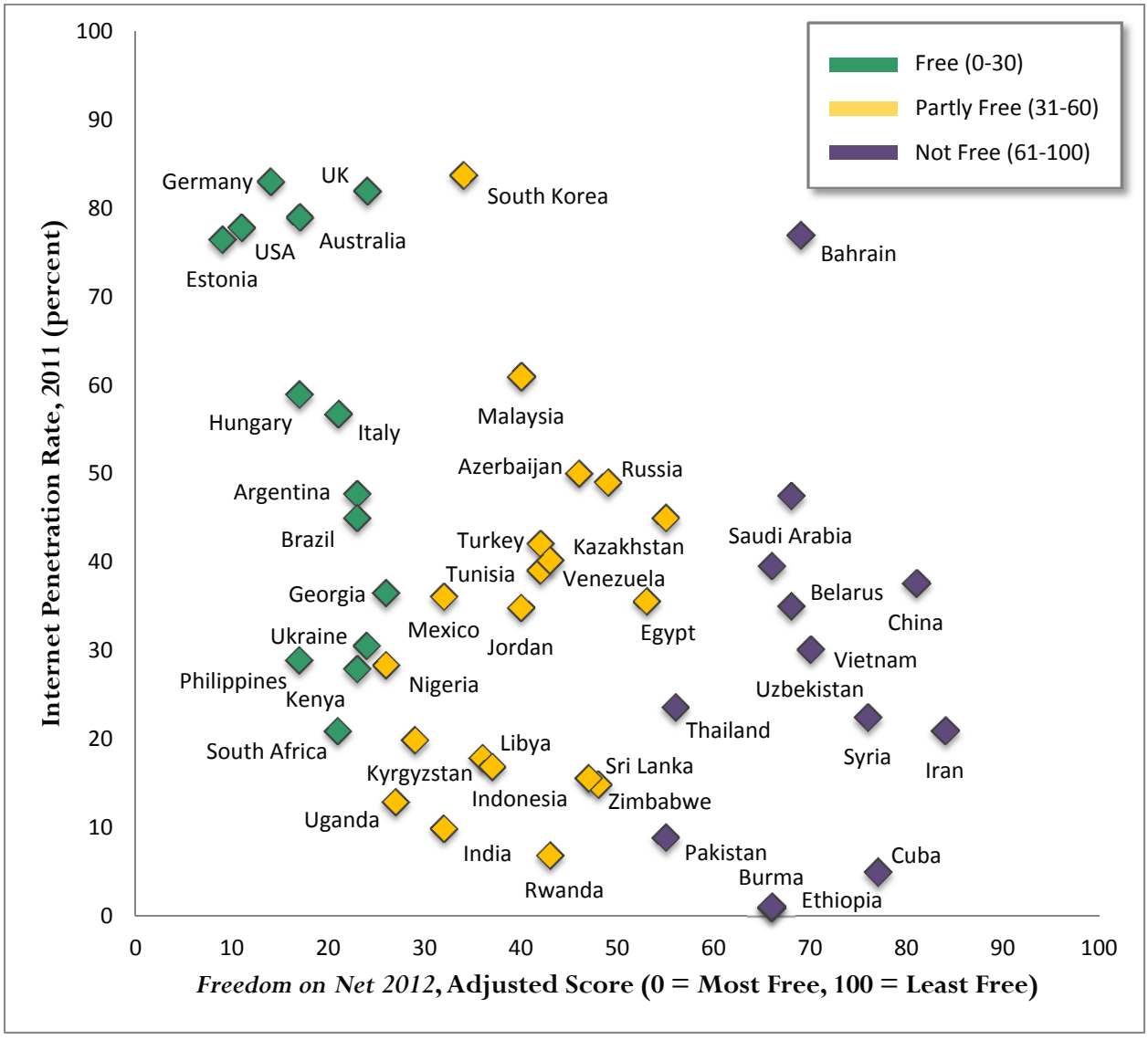


* The front-row bar reflects a country's *Freedom on the Net 2012* score; the back-row bar reflects the country's score on Freedom House's *Freedom of the Press 2012* index, which primarily assesses television, radio, and print media.

INTERNET FREEDOM VS. INTERNET PENETRATION

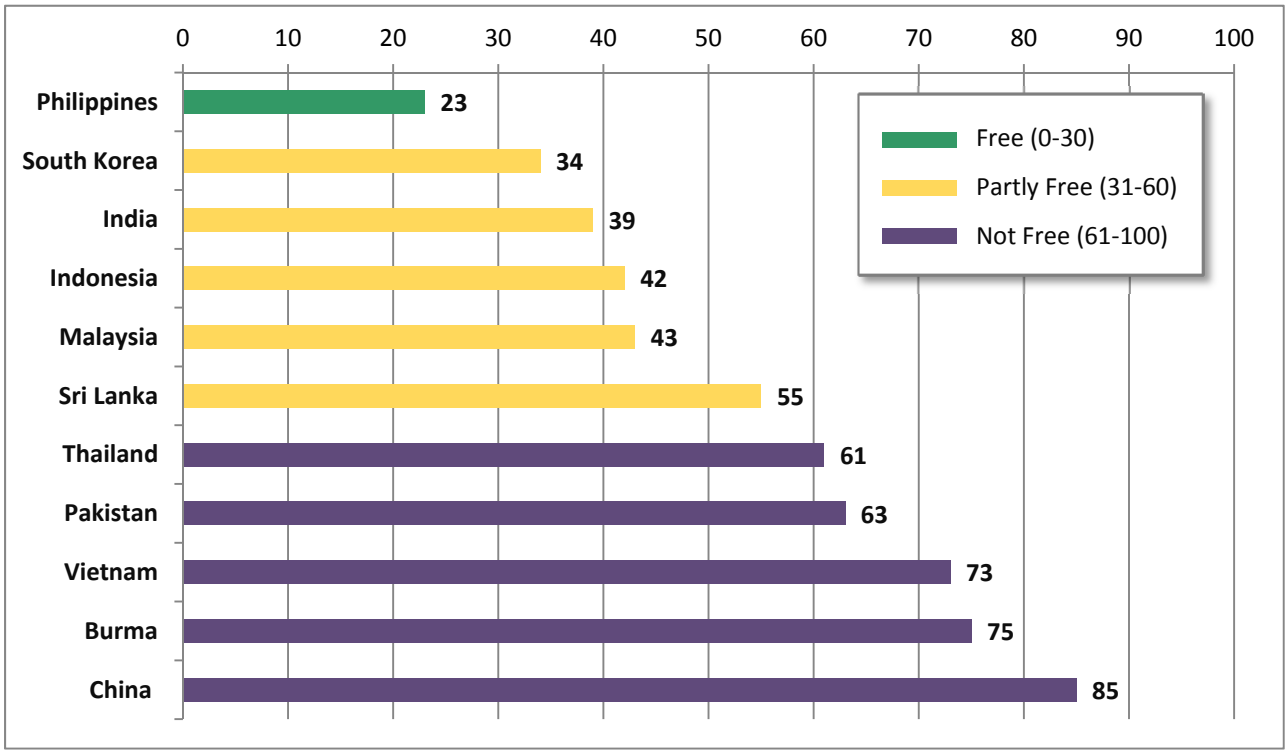
The figure below depicts the relationship between internet penetration rates and the level of digital media freedom as assessed by the *Freedom on the Net 2012* study. Each point is plotted to reflect its level of internet penetration as noted in the report, as well as its performance in the survey. To minimize possible overlap among variables, the scores have been adjusted to exclude performance on the first two questions of the *Freedom on the Net* methodology, which assess the degree of internet access in a given society.

Of note is a potential trajectory for the Partly Free countries in the middle, which may move towards greater repression (the high-tech, Not Free countries on the middle right) or better protection of free expression (the mid-penetration, Free countries on the left) as digital media access rates increase.

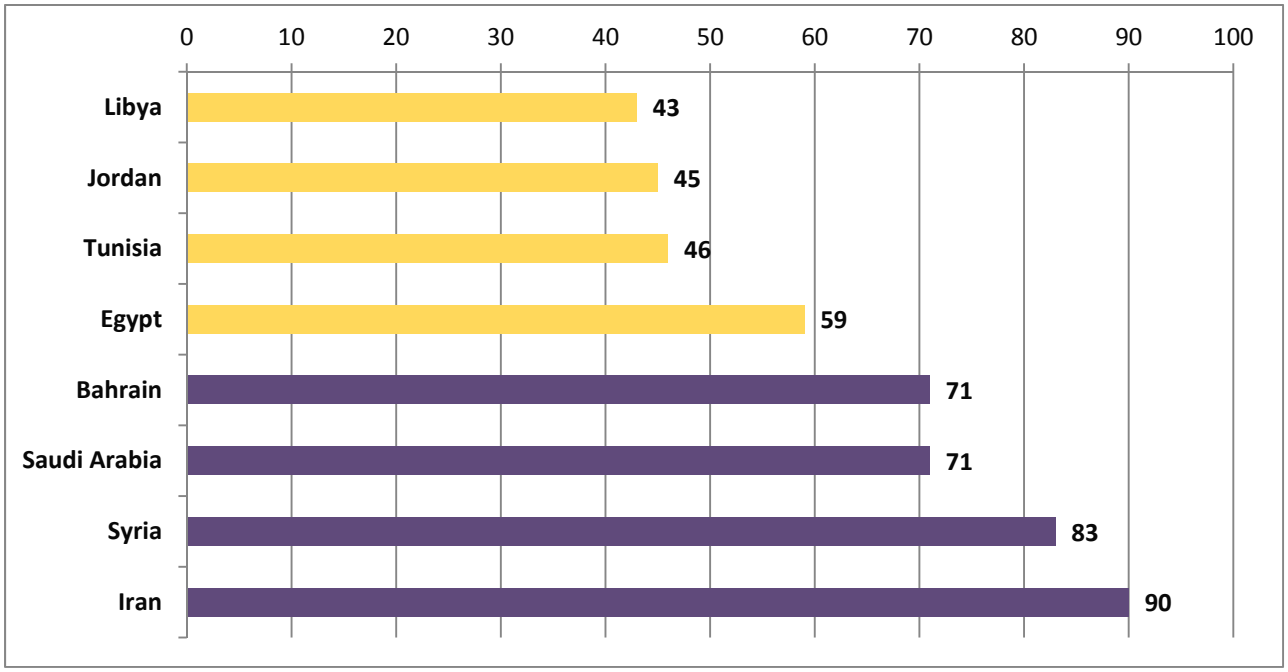


REGIONAL GRAPHS

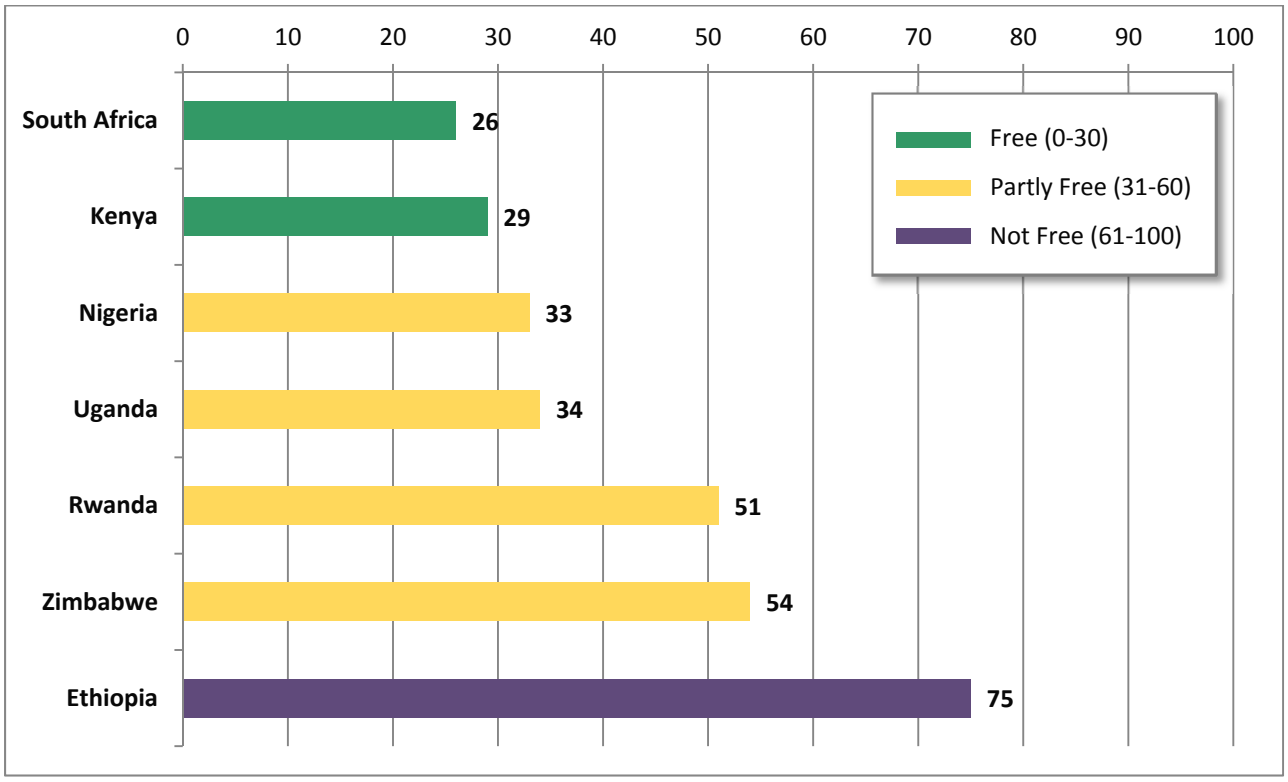
ASIA (0 = Most Free, 100 = Least Free)



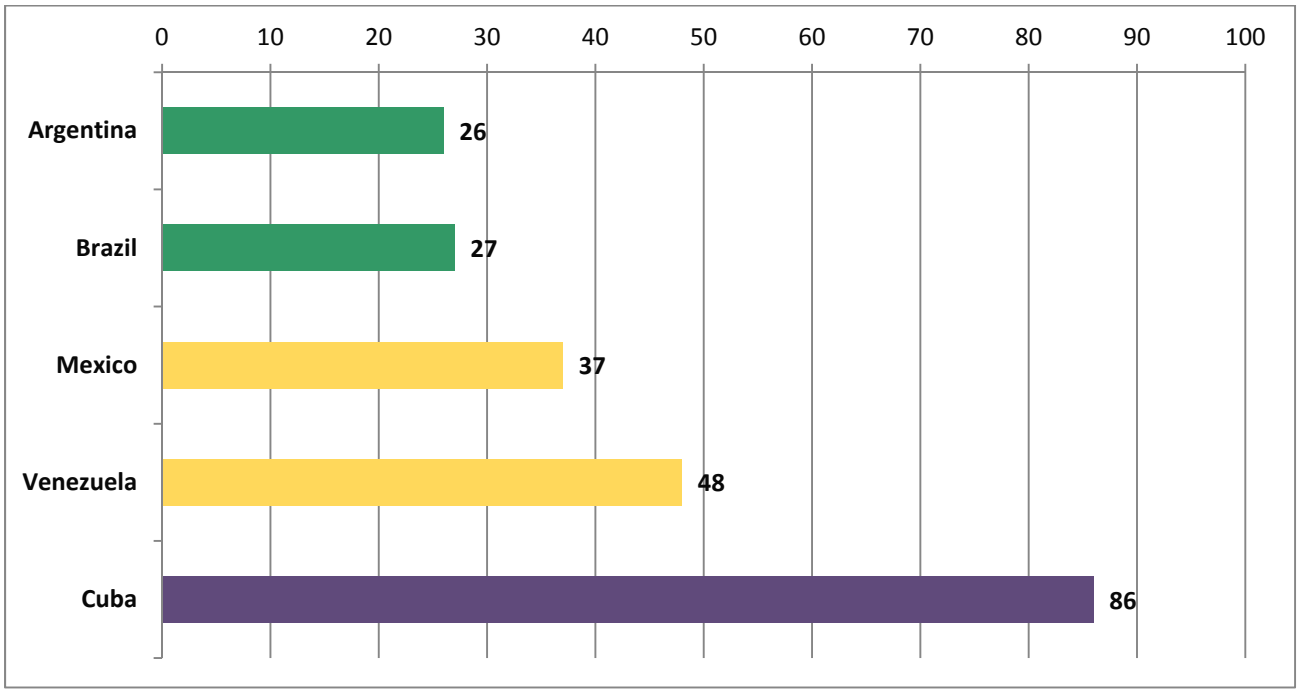
MIDDLE EAST & NORTH AFRICA (0 = Most Free, 100 = Least Free)



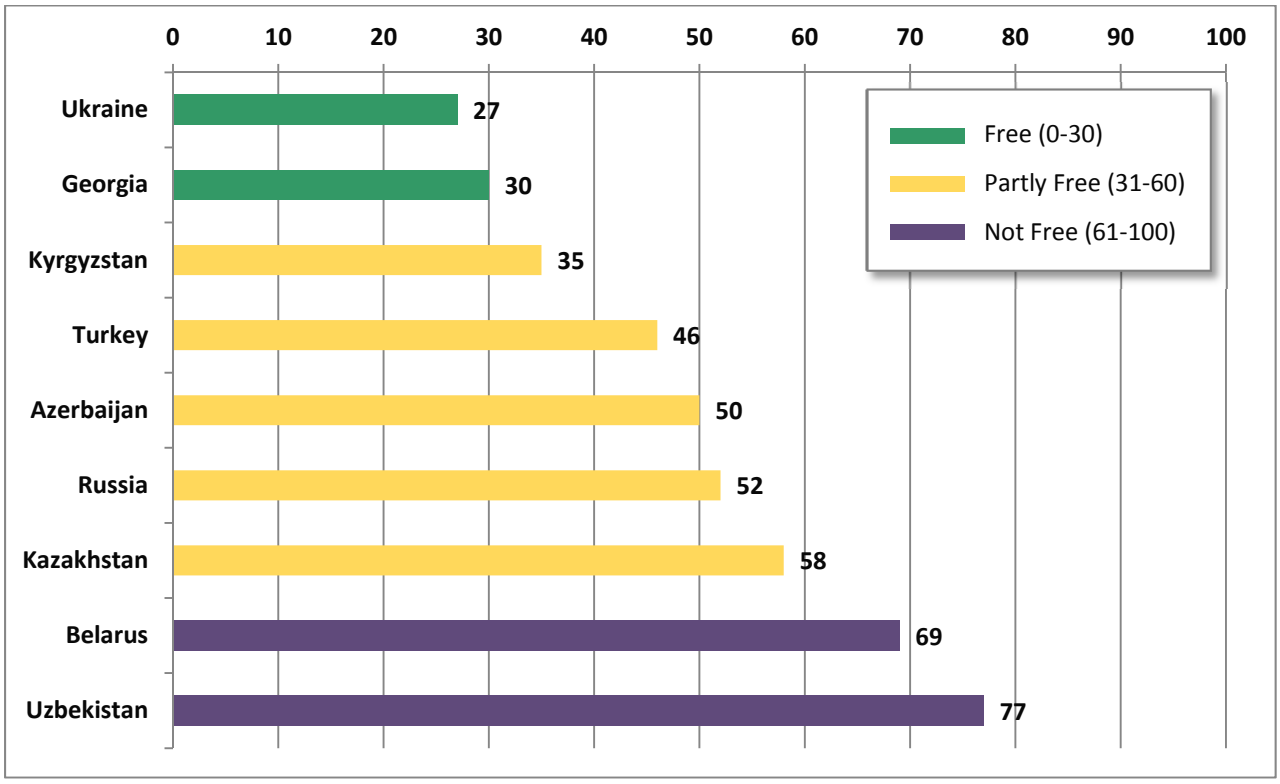
SUB-SAHARAN AFRICA (0 = Most Free, 100 = Least Free)



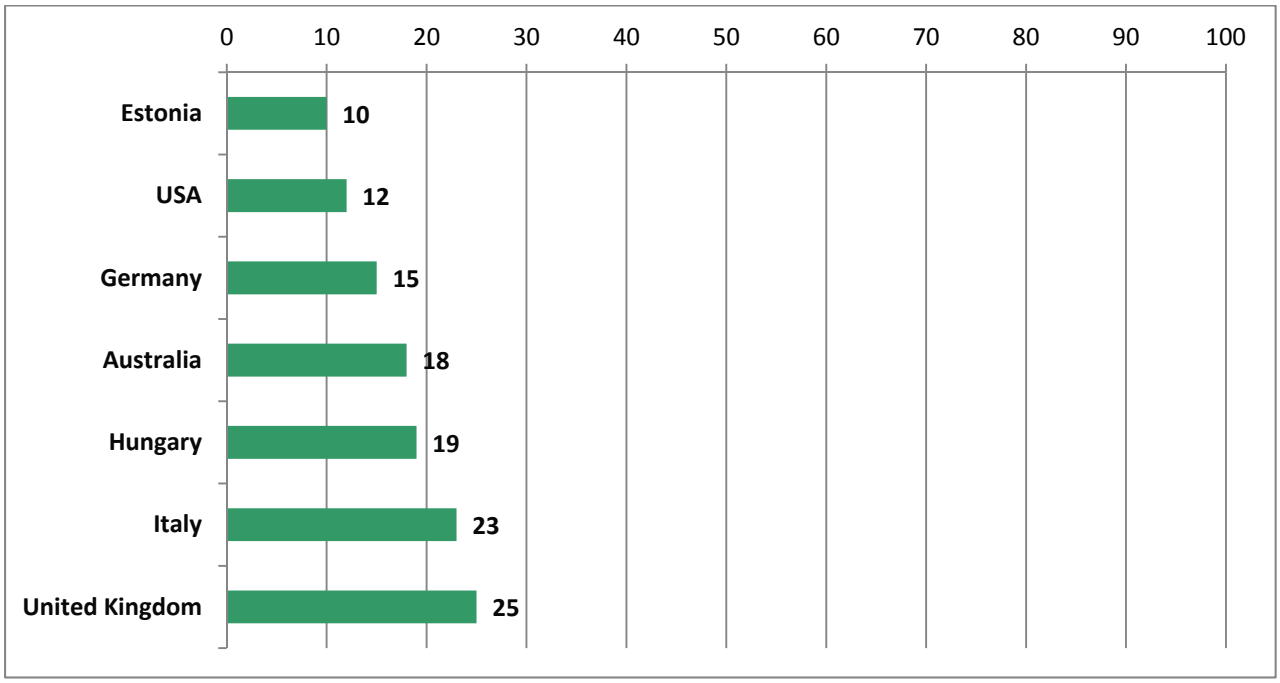
LATIN AMERICA (0 = Most Free, 100 = Least Free)



EURASIA (0 = Most Free, 100 = Least Free)

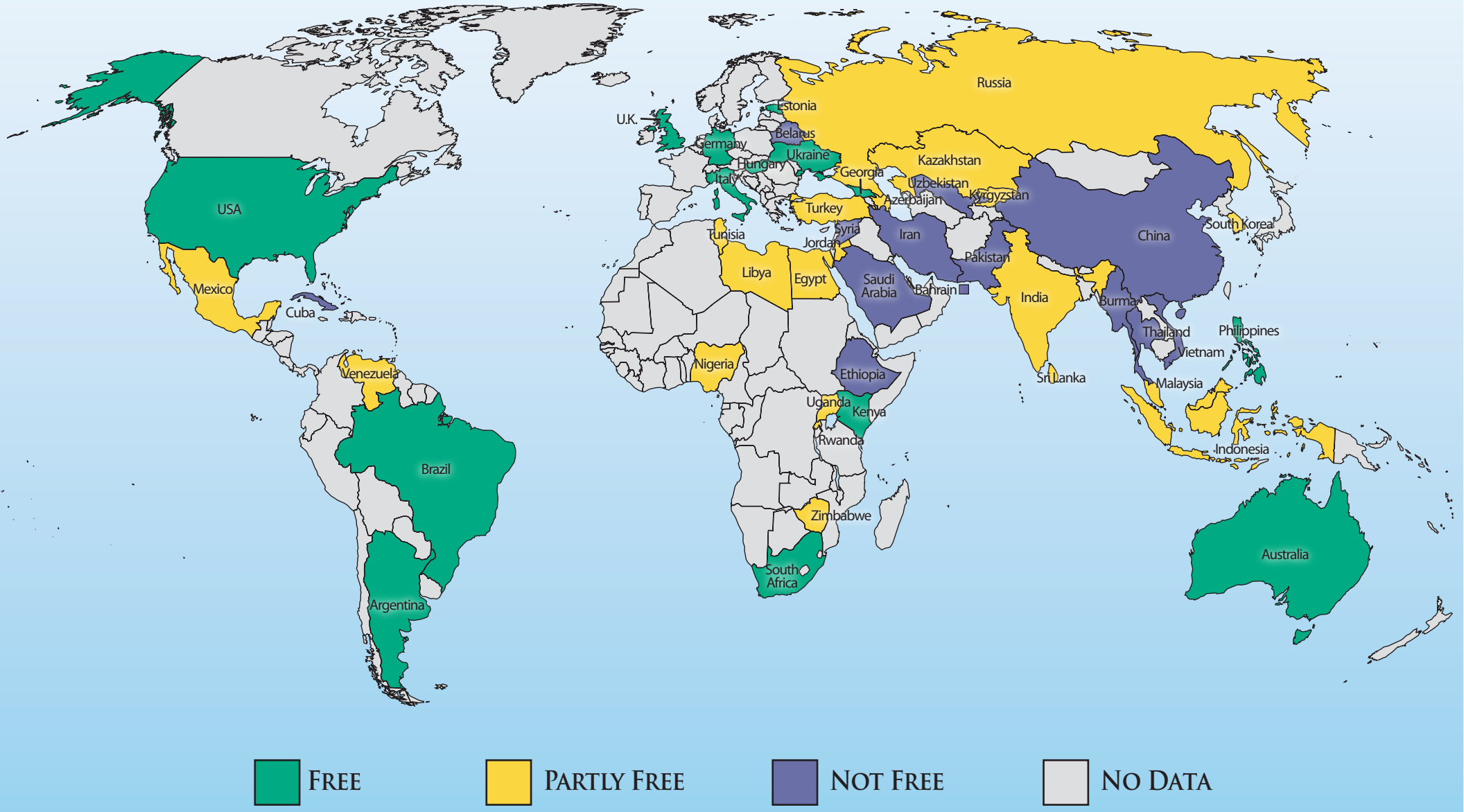


EUROPE & OTHERS (0 = Most Free, 100 = Least Free)



Freedom on the Net 2012

A Global Assessment of Internet and Digital Media



COUNTRY REPORTS

ARGENTINA

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Free**
Obstacles to Access (0-25)	n/a	9
Limits on Content (0-35)	n/a	9
Violations of User Rights (0-40)	n/a	8
Total (0-100)	**n/a**	**26**

* 0=most free, 100=least free

POPULATION: 41 million
INTERNET PENETRATION 2011: 48 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

The internet first began being used for commercial purposes in Argentina in 1991, though it had been a focus of academic study from the 1980s.[1] Internet penetration has since steadily increased and Argentina is now home to one of the largest contingents of internet users in South America. Since 2009, access has grown especially quickly, partly the result of successful government policies to improve services and expand broadband connections throughout the country.

The country's legal framework and independent courts generally protect online freedom of expression, both in law and in practice, and Argentineans have free access to a wide array of information sources over the internet. Nevertheless, several court decisions in 2010 and 2011 restricted access to websites on claims of defamation or intellectual property rights violations, and one led to the accidental blocking of an entire blog-hosting platform. More seriously, a series of injunctions imposed intermediary liability on search engines to delete links from the results they present users. The rulings drew criticism from freedom of expression advocates and international firms like Google, and some were subsequently overturned by higher courts.

[1] Jorge Amodio, "History and Evolution of the Internet in Argentina" [in Spanish], Internet Argentina, Historia y Evolucion (blog), May 16, 2010, http://blog.internet-argentina.net/p/indice.html.

OBSTACLES TO ACCESS

Internet penetration has consistently increased over the past decade, from about 21 percent of the population in 2006 to nearly 48 percent in 2011, according to the International Telecommunications Union (ITU), an increase of over 10 percent from the previous year.[2] Some sources suggest that by the end of 2011, overall internet penetration had risen even higher, to 75 percent of the population.[3] This dramatic expansion in usage has been facilitated by increased government investment in telecommunications infrastructure and equipment over the past two years. As a result, a growing number of people are connecting to the internet from their homes and via mobile devices. By December 2011, the number of internet subscriptions reached 8.2 million for residential connections and another 1.2 million at organizations or businesses, according to government figures, an increase of over 50 percent in each sector compared to 2010.[4] Mobile web connectivity increased by around 160 percent over the same period.[5] The proportion of broadband connections compared to dial-up has also increased, and by early 2012, broadband accounted for 99 percent of the internet market[6] at an average speed of 3 Mbps.[7] Mobile phone penetration is significantly higher than internet usage, with 58 million lines active as of late 2011 (a penetration rate of about 142 percent).[8]

Although access is growing across the country, according to the National Statistics Institute (Instituto Nacional de Estadísticas y Censos, INDEC), there remains a stark gap between large urban areas like Buenos Aires, Cordoba, and Santa Fe versus other provinces; the former account for over 75 percent of home internet connections.[9] Besides socioeconomic disparities and price differences, the lack of access to National Access Points in geographically remote areas, such as Patagonia or the northwest, contributes to this urban-rural divide.[10] In general, expense has not been a primary obstacle to access for most people. The average

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[3] "75% of the population has internet access in Argentina" [in Spanish], Prince & Cooke, January 3, 2012, http://economia.terra.com.ar/noticias/noticia.aspx?idNoticia=201201031637_TEL_4213101.

[4] National Institute of Statistics and Censuses (INDEC), "Press Reports on Access to Internet, Fourth Quarter of 2011" [in Spanish], Ministry of Economics and Public Finances, Institute of Statistics and Censuses, accessed April 6, 2012, http://www.indec.gob.ar/nuevaweb/cuadros/14/internet_03_12.pdf.

[5] Ibid.

[6] Ibid.

[7] "Argentina out of the podium of Internet Speed in Latin America" [in Spanish], Yahoo News Online, May 30, 2012, http://ar.noticias.yahoo.com/argentina-podio-velocidad-internet-am%C3%A9rica-latina-181000405.html.

[8] National Institute of Statistics and Censuses (INDEC), "Historic Series of Communications: Active Cellphones" [in Spanish], National Communications Commission, accessed June 5, 2012, http://www.indec.gob.ar/nuevaweb/cuadros/14/sh_comunicac2.xls.

[9] INDEC, "Press Reports on Access to Internet, Fourth Quarter of 2011."

[10] Interview with employee of the Library of the National Communications Commission (Comisión Nacional de Comunicaciones), February 18, 2012.

broadband plan cost 100 pesos (US$22) per month and the average monthly wage is 2,300 pesos (US$500).

In recent years, the Argentine government has accelerated its efforts to promote internet access and as noted above, these appeared to bear fruit in 2011. Policies that contributed to these successes included the Digital Agenda, the Argentina Connected Plan, the Equal Connection Plan, and the Universal Service Trust Fund. The Digital Agenda, approved in 2009, established a national plan for strategically using information and communication technologies (ICTs) to connect government institutions and citizens to create a knowledge society. The Argentina Connected Plan was approved in 2010 as a five-year strategic initiative to expand infrastructure and telecommunications services to the entire country. It seeks to reduce the cost of broadband connections and make them available on equal terms for all inhabitants. The Equal Connection Plan, also approved in 2010, led to the provision of internet connections at all public secondary schools and laptop computers for students throughout the country. Lastly, although universal service obligations have been in place since 2001, initiatives to seriously enforce these commitments only began in November 2010. That month, the government established the Universal Service Trust Fund, which receives one per cent of the profits from telecommunications companies and uses it to reinvest in expanding broadband access to narrow the gap across provinces.[11]

When the telecommunications industry was privatized in the 1980s, the former state-owned operator was split into two companies: Telecom Argentina to cover the north of the country and Telefonica de Argentina to cover the south. As of the end of 2010, these two incumbents owned around 90 percent of the fixed-line infrastructure in the country and both provided internet services.[12] Meanwhile, some 300 other companies have been granted licenses to operate as internet service providers (ISPs).[13] Many of these are regional providers, serving as provincial subsidiaries of the above two companies or other large firms like Fibertel of Grupo Clarín that also has a notable share of the broadband market.[14] The mobile phone market is dominated by three providers: Telefonica's Movistar, Telecom's Personal, and Claro, owned by Mexican billionaire Carlos Slim. Each of the three covers about one third of the market

[11] "The Digital Agenda" [in Spanish], Cabinent of Ministers of the President, accessed March 20, 2012 http://www.agendadigital.ar/; "The National Telecommunications Argentina Connected Plan" [in Spanish], Ministry of Federal Planning, Public Investment and Services, accessed March 20, 2012, http://www.argentinaconectada.gob.ar; "The Equal Connection Plan" [in Spanish], Cabinent of Ministers of the President, accessed March 20, 2012, http://www.conectarigualdad.gob.ar/; "Universal service obligations and the Universal Service Trust Fund" [in Spanish], National Communications Commission, accessed March 20, 2012, http://www.cnc.gov.ar/infotecnica/facturacion/servuniversal.asp.

[12] "Argentina Broadband Overview," Point-Topic, July 12, 2011, http://point-topic.com/content/operatorSource/profiles2/argentina-broadband-overview.htm.

[13] "Business Information" [in Spanish], National Communications Commission, accessed March 20, 2012, http://www.cnc.gob.ar/ciudadanos/internet/empresas.asp?offset=0.

[14] "Argentina Broadband Overview," Point-Topic.

and all offer 3G services.[15] To date, the state has not interfered with international internet connectivity. However, as part of the Argentina Connected Plan, the government is working to construct an internal state-sponsored fiber-optic cable backbone that would be managed by a government-owned firm.[16] The project is scheduled for completion in 2015 and is currently in the procurement phase.

Private companies wishing to operate as ISPs must first obtain a license from the National Communications Commission (Comisión Nacional de Comunicaciones, CNC).[17] The CNC functions under the Secretariat of Communications (Secretaría de Comunicaciones) as a decentralized entity. Both operate under the authority of the Ministry of Federal Planning, Public Investment and Services.[18] Upon receipt of an application, the CNC refers the submission to the Secretariat of Communications, which makes the final decision to grant a license. The applicant is required to pay a relatively modest sum of 5,000 Argentine pesos (US$1,100) at the time of submission.[19] The licensing process for mobile phone providers is similar. Once the license is approved, there are no additional fees, but new providers are required to pay special taxes, like the Universal Service Trust Fund mentioned above. Cybercafe licenses are processed like those of any other small business, without additional conditions or approvals required.

Although the statutory composition of the CNC offers some degree of independence, it has been taken over by the executive since 2002 per Presidential decree 521 in order to increase its efficiency.[20] The decree provides for an ad hoc administrator (*interventor*) appointed by the president, who will fulfill the functions of the CNC President and Board of Directors, as well as appoint other commission members at his or her discretion. This arrangement has detracted from the independence of the institution. In practice, there have been few complaints about corruption or unfairness in the CNC's operations. Since 2010, however, controversy and accusations of political bias have emerged surrounding Fibertel's ISP license, indicating some public mistrust of the regulator.[21] The relevant judicial case was pending before a federal court as of May 2012.

---

[15] Ibid.

[16] The government-owned corporation AR-SAT would manage the network. AR-SAT began operating in July 2006 and its stated purpose is to promote the Argentine space industry and increase satellite services to different parts of the country. AR-SAT Company website, http://www.arsat.com.ar.

[17] "Decree 764/2000 Annex 1" [in Spanish], National Communications Commission, accessed March 20, 2012, http://www.cnc.gov.ar/normativa/Dec764_00-AnexoI.pdf.

[18] "Organization Chart" [in Spanish], Ministry of Federal Planning, Public Investment and Services, accessed June 6, 2012, http://institucional.minplan.gov.ar/html/organigrama/.

[19] "Guide for license applications," National Communications Commission, accessed March 20, 2012, http://www.cnc.gob.ar/infotecnica/archivos/Guide_Licence%20Application[eng].pdf.

[20] National Communications Commission (Comisión Nacional de Comunicaciones), *Presidential Decree N° 521/2002* [in Spanish], March 20, 2002, http://www.cnc.gov.ar/institucional/biblioteca/buscador/Normativa/pdf/Decreto-521_02.pdf.

[21] "Argentina's media Pressed," The Economist, August 25, 2010, http://www.economist.com/blogs/americasview/2010/08/argentinas_media; "Federal judge freezes order to cancel Fibertel's

LIMITS ON CONTENT

Argentinean internet users have access to a wide array of online content, including international and local news outlets, political parties' websites, and civil society initiatives. The government does not impose any automated filtering or restrictions on politically oriented information. However, some websites related to child pornography are blocked. In recent years, controversy has emerged over the blocking of allegedly defamatory or copyright protected content, as well as injunctions that invoke intermediary liability.

Web 2.0 tools such as the social networking site Facebook, the video-sharing platform YouTube, or the microblogging service Twitter are freely available. Nevertheless, in one notable exception, Google's blog-hosting platform Blogger was blocked for approximately one week in August 2011. Following a court decision, the CNC ordered local ISPs to restrict access to two URLs: www.leakymails.com and Leakymails.blogspot.com.[22] The websites, local spinoffs of the anti-secrecy site Wikileaks, had published the email correspondence of government officials, politicians, journalists and other public figures. Much of the content appeared to be personal and irrelevant to public policy, rather than exposing malfeasance or corruption, prompting the complaints that led to the court order.[23] ISPs complied and blocked access to the IP addresses of the two pages, but this also restricted access to the Blogspot.com domain, effectively blocking the entire Blogger platform, including over one million other blogs not listed in the judicial order. After criticism from the public and Google,[24] the sweeping block was lifted a week later, though the specific Leakymails blog remained inaccessible, as ISPs shifted to a more precise filtering technique.

Another case drawing public attention involves judicial action taken against Cuevana, a website dedicated to cataloguing and linking to sites that enable the free streaming of movie and television programs. Launched in 2009, Cuevana quickly became one of the most visited websites in Argentina and the largest of its kind in Latin America. Since late 2011, various international content producers have filed lawsuits against the site (including HBO, Turner Argentina, Twentieth Century Fox, and Disney Enterprises) alleging infringement of

license, govt to appeal," Business News Americas, September 27, 2010, http://www.bnamericas.com/news/telecommunications/Federal_judge_freezes_order_to_cancel_Fibertel*s_license,_govt_to_appeal.

[22] "A todos los Licenciatarios de Telecomunicaciones que brindan Servicios de Acceso a Internet" [All Telecom licensees providing Internet Access services] National Communications Commission, accessed March 20, 2012, http://www.cnc.gov.ar/noticia_detalle.asp?idnoticia=106.

[23] "Justice blocked the argentine 'Wikileaks'," [in Spanish] TN Cable Online, August 11, 2011, http://tn.com.ar/politica/00062732/juez-pidio-bloquear-al-%E2%80%9Cwikileaks%E2%80%9D-argentino; "A todos los Licenciatarios de Telecomunicaciones que brindan Servicios de Acceso a Internet" [All Telecom licenses providing Internet Access services], National Communications Commission, accessed March 20, 2012, http://www.cnc.gov.ar/noticia_detalle.asp?idnoticia=106.

[24] "Google reports blockage of blogs in Argentina" [in Spanish], TN Cable Online, August 19, 2012, http://tn.com.ar/tecnologia/00064541/google-denuncia-un-bloqueo-masivo-de-sus-blogs-en-la-argentina.

intellectual property rights.[25] As a result, in November 2011, the National Court of First Instance ordered the blocking of certain programs from Cuevana's website, though ISPs only partially implemented the directive.[26] In March 2012, the prosecutor opened a criminal case against the site's administrator for allegedly profiting from copyrighted materials via donations to the site; the administrator denied the charges, claiming that any profits have been reinvested and that most of those involved are volunteers.[27] If found guilty, he could face between one month and six years in prison.

Regarding intermediary liability, several private individuals have sued search engines like Google and Yahoo, requesting that some results be removed from searches for their names. Most such complaints specifically ask for removal of links to content on third-party websites that the individual finds objectionable or damaging to his or her reputation.[28] Between 2006 and 2010, over 130 such cases were reportedly filed, often by prominent entertainers. In several instances, intermediaries have had to pay monetary compensation to the plaintiffs.[29] In one high profile case, a judge ruled in July 2009 that Google and Yahoo should remove all results linking to sites containing sexual images related to pop star Virginia Da Cunha. Google responded that it could not comply with such a sweeping injunction, while Yahoo held that the only way to comply would be to block all search results for her name. The firm temporarily took this unusual action for both her and other plaintiffs such as swimsuit model Yesica Toscanini.[30] In August 2010, the decision was overturned on appeal. The court ruled that the search engines could be held liable only if they were informed of defamatory content and negligently failed to remove it; they were not required to systematically identify and preemptively remove such material on their own. In two other cases that did not

[25] "Cuevana gets in more problems" [in Spanish], Clarin, March 7, 2012, http://www.clarin.com/internet/mundo_web/titulo_0_659334165.html; "Cuevana: Open criminal case against the owners of the site in Argentina" [in Spanish], La Tercera online, March 16, 2012, http://www.latercera.com/noticia/tendencias/2012/03/659-438170-9-cuevana-abren-causa-penal-contra-los-duenos-del-sitio-en-argentina.shtml.

[26] Juan Pablo De Santis, "Justice blocks access to TV shows in Cuevana" [in Spanish], La Nacion online, November 30, 2011, http://www.lanacion.com.ar/1428736-la-justicia-pidio-bloquear-el-acceso-a-series-en-cuevana.

[27] Gonzalo Larrea, "Argentina Opens Criminal Case Against Cuevana," Ttvmedianews.com, http://www.ttvmedianews.com/scripts/templates/estilo_nota.asp?nota=eng%2FTech%2FInternet%2F2012%2F03_Marzo%2F16_justicia_vs_cuevana; Pablo Sirven, "Inician causa penal contra Cuevana" [Initiate crimanl proceedings against Cuevana], La Nacion online, March 16, 2012, http://www.lanacion.com.ar/1456828-inician-causa-penal-contra-cuevana; "Cueva the End?" Rapid TV News, http://www.rapidtvnews.com/index.php/2011113017494/cuevana-the-end.html#ixzz1vUbANxZl (site discontinued).

[28] Eduardo Bertoni and Elizabeth Compa, "Emerging Patterns in Internet Freedom of Expression: Comparative Research Findings in Argentina and Abroad," Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (Presented at the Latin American Regional Meeting on Freedom of Expression and the Internet), 2010: 25-38, http://www.palermo.edu/cele/libertad-de-expresion-en-Internet.pdf. Such cases include, inter alia, Da Cunha Virginia c/ Yahoo de Argentina SRL y otro s/ Daños y perjuicios; Zámolo, Sofía K. c/ Yahoo de Argentina SRL y otro; Sosa, María Agustina c/ Yahoo de Argentina SRL y otros s/ Medidas precautorias; etc.

[29] Google was ordered to pay 10,000 Argentine pesos (US$ 2,300) plus court costs for facilitating the damage suffered by the claimant. BLUVOL, Esteban Carlos c/ GOOGLE INC: y otros s/ Daños y Perjuicios.

[30] The following message appeared to users seeking to search for information about these individuals: "Due to a court order requested by private parties, we have been forced to temporarily suppress all or some of the results related to this search."

involve sexual content, one filed by Judge María Romilda Servini de Cubría and the other by soccer player Diego Maradona, the courts ruled in the search engine's favor on the grounds that government officials, and in some cases prominent figures, can be subject to a higher level of public scrutiny than ordinary citizens. As of May 2012, the Cunha case was pending before the Supreme Court.

In a slightly different case, a judge granted an injunction in May 2011 ordering Google to remove 76 websites deemed anti-Semitic and "highly discriminatory" from its search results.[31] The court also ruled that a set of 13 terms whose results led to those websites should be removed from the "suggested search" function on Google, a feature that offers optional terms similar to the one the user enters into the query field. Freedom of expression advocates criticized the decision, arguing that if applied more broadly, it could lead to significant intermediary liability and censorship. Instead, they recommended a similar approach to the United States, where an ad linking to information from the Anti-Defamation League was posted alongside anti-Semitic search results to educate users.

Despite the controversy surrounding the above decisions, it is notable that all blocks and removals have been based on court rulings. The websites and intermediaries involved have had access to an independent judicial process to challenge the decisions and have sometimes succeeded in overturning earlier rulings on appeal. According to Google's Transparency Report, from January to June 2011, the Argentine government submitted 21 content removal requests, covering 56 items, and the firm complied at least partially with all of them.[32] Except for one request, all were made based on a court order. Google's breakdown of the requests indicates that nearly all related to claims of defamation or violations of privacy and none concerned government criticism.

Self-censorship among bloggers or online users is not widespread, and Argentinians express a wide diversity of views online. Nevertheless, in the interior parts of the country, where the rule of law is weaker than in the capital, some online journalists and bloggers use care when writing about powerful local officials or mining companies. In Argentina's polarized political environment, others may adjust their reporting based on the partisan affiliation of their publication.

The Argentine federal and local governments are known to allocate official advertising in a discriminatory manner, excluding news outlets whose reporting has been critical of the

[31] "Argentine court blocks Google 'suggested' searches," CNN online, May 19, 2011, http://edition.cnn.com/2011/TECH/web/05/18/argentina.google/.
[32] "Google Transparency Report, Argentina," last updated for July to December 2011, accessed on March 20, 2012, http://www.google.com/transparencyreport/governmentrequests/AR/.

government and rewarding supportive ones.[33] This phenomenon has had a negative impact on freedom of expression, particularly in the print and broadcast media sectors, and could affect online communications.[34] To date, however, there have been no documented cases of similar pressures being applied to online news outlets. In a positive development, in March 2011, the Supreme Court ruled unanimously that the government should apply a reasonable degree of balance in the distribution of state advertising.[35]

There are no restrictions on access to national or foreign news sources and Argentineans are able to express themselves freely online. According to some observers, the dynamism of the pro-government blogosphere has increased since 2009, though other political parties have also started to gain ground.[36] A wide range of topics and views are shared online, including potentially sensitive ones like dissection of President Cristina Kirchner's speech to Congress following her reelection in October 2011 or scrutiny of her health when she underwent surgery in January 2012.[37] Nevertheless, journalists have complained about a lack of access to government representatives and a dearth of official press conferences. In 2009**,** an online portal called "Better Democracy" (*Mejor Democracia)* that provided the public with government-related information was closed. When it later reopened, it offered notably less information than previously, reducing transparency.[38] Most civic groups have a website, although user engagement in sociopolitical movements is low. Mobile phones are increasingly being used for activism, and such devices will likely play a decisive role in the future.[39] In addition, the popularity of social media tools has grown. By April 2012, the country had over 18 million Facebook registered users, almost 45 percent of the population. As of April 2011, there were about 850,000 Twitter users in Argentina.[40]

[33] "The Dimension of Oficial Publicity in Argentina" [in Spanish], Poder Ciudadano, accessed March 20, 2012, http://poderciudadano.org/wp/wp-content/uploads/2011/12/Informaci%C3%B3n-preliminar-PO-Poder-Ciudadano.pdf; Asociacion por los Derechos Civiles and Open Society Justice Initiative, "Buying the News: A report on financial and indirect censorship in Argentina," Open Society Institute (2005), http://www.censuraindirecta.org.ar/advf/documentos/48ee57ee263549.92961213.pdf

[34] "The Dimension of Oficial Publicity in Argentina" [in Spanish], Poder Ciudadano.

[35] IFEX, "Supreme Court urges government to avoid bias in allocating state advertising," news release, March 8, 2011, http://www.ifex.org/argentina/2011/03/08/omit_discriminatory_criteria/; "Supreme Court tells Argentina to avoid bias in allocating ads," Committee to Protect Journalists, March 4, 2011, http://cpj.org/2011/03/supreme-court-urges-argentina-to-avoid-bias-in-all.php.

[36] Jorge Gobbi, "Argentina: Presidential Elections, a Review of Blogs," Global Voices (blog), October 26, 2011, http://globalvoicesonline.org/2011/10/26/argentina-presidential-elections-a-review-of-blogs/.

[37] Natan Calzolari, "Argentina: President Cristina Fernandez' Controversial Cancer Diagnosis," Global Voices (blog), January 16, 2012, http://globalvoicesonline.org/2012/01/16/argentina-president-cristina-fernandez-controversial-cancer-diagnosis/; Natan Calzolari, "Argentina: President Fernandez's Speech Under Netizens' Scrutiny," Global Voices (blog), March 6, 2012, http://globalvoicesonline.org/2012/03/06/argentina-president-fernandezs-speech-under-netizens-scrutiny/ .

[38] "Califican de "retroceso" el bloqueo de la Web oficial" [in Spanish], Asociacion por los Derechos Civiles (ADC), October 8, 2009, http://www.adc.org.ar/sw_contenido.php?id=643.

[39] Lourdes Cajrdenas, "NGOs mobilize citizenship by cellphone" [in Spanish], CNN Expansion, January 15, 2010, http://www.cnnexpansion.com/expansion/2009/12/11/Mensajes-sin-excusas.

[40] "Datos Twitter Latinoamerica 2011 (infografía)" [Latin American Twitter Data 2011 (infographic)], Ecualinkblog.com, http://www.ecualinkblog.com/2011/04/datos-twitter-latinoamerica-2011.html.

VIOLATIONS OF USER RIGHTS

The Argentine Constitution and human rights treaties incorporated into the Constitution in 1994 guarantee freedom of expression.[41] Other laws also ensure that citizens can express their views without fear of censorship or reprisal. In 2005, Law No. 26032 was adopted explicitly extending constitutional protections to "the search, reception and dissemination of ideas and information of all kinds via internet services."[42]

The judiciary is generally independent, particularly at its higher echelons, such as the Supreme Court of Justice (SCJ). The SCJ has issued several rulings supportive of freedom of expression in recent years. These include the above-mentioned 2011 decision on discriminatory allocation of government advertising and a 2009 ruling that led to the suspension of requirements for service providers to retain user data for ten years.[43] The government has also been responsive to decisions of the Inter-American Court of Human Rights and the recommendations of the Inter-American Commission on Human Rights. These procedures have helped accelerate reform of the Criminal Code's provisions on insult (*desacato*) and defamation. In November 2009, the legislature decriminalized defamatory statements referring to matters of public interest.

No specific laws criminalize online expression on political or social issues. Law No. 26388, known as the Law on Cybercrime, was adopted in 2008. It amended the Argentine Criminal Code to cover offenses such as hacking, dissemination of child pornography, and other online crimes.[44] Some of the amendments have been criticized as overly vague and imprecise in their wording, using terms like "other similar communications," which could open the door to abusive or unpredictable interpretations. In December 2011, the parliament passed an amendment to the country's antiterrorism law. Lawyers and human rights groups

[41] Particularly article 14. See Text of the Argentine Constitution in English, "Argentine Constitution," Senate of the Argentine Nation, accessed March 20, 2012, http://www.senado.gov.ar/web/interes/constitucion/english.php. The Argentine Constitution was amended in 1994, and article 75 (22) now accords the following international human rights treaties with constitutional status and precedence over national laws: the American Declaration of the Rights and Duties of Man; the Universal Declaration of Human Rights; the American Convention on Human Rights; the International Covenant on Economic, Social and Cultural Rights; the International Covenant on Civil and Political Rights and its Optional Protocol; the Convention on the Prevention and Punishment of the Crime of Genocide; the International Convention on the Elimination of all Forms of Racial Discrimination; the Convention on the Elimination of all Forms of Discrimination against Woman; the Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment; the Convention on the Rights of the Child.

[42] Law No. 26032 [in Spanish] (2005), Documentation and Information Center, accessed March 20, 2012, http://www.infoleg.gov.ar/infolegInternet/anexos/105000-109999/107145/norma.htm.

[43] Lorenzo Villegas Carrasquilla, "Personal data protection in Latin America: retention and processing of personal data in the Internet sphere," Center for Studies in Freedom of Expression and Access to Information, http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/05-Personal_data_protection_Latin_America_Villegas_Carrasquilla.pdf; Judgment of Halabi v. P.E.N. Argentine Supreme Court, June 26, 2007.

[44] Law No. 26.388 [in Spanish] (2008), Documentation and Information Center, accessed March 20, 2012, http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

expressed concerns that the definition of terrorism provided was overly broad and could therefore be employed to punish legitimate political dissent, social protests, or economic analysis.[45] So far, neither of these laws has been used in practice to punish online expression.

As of April 2012, no bloggers, online journalists, or ordinary users were imprisoned for the peaceful expression of their views online or via private communications. One website administrator was facing criminal charges and a possible jail term over allegations of profiting from copyrighted material (see "Limits on Content"). Local press freedom watchdogs recorded about 18 cases of physical and verbal attacks against journalists during the first half of 2011. Most attacks were by non-state actors, in inland regions, and against those working for traditional media outlets.[46] However, in some cases, the journalists targeted also maintained websites or contributed to online news outlets. For example, in July 2011, Carlos Walker, a website editor and reporter for the local FM Ciudad radio station in Mar del Plata, was beaten, shot in the leg, and robbed of his journalistic equipment within minutes of taking pictures of political posters; the circumstances raised suspicions that he was targeted for his reporting rather than as a random victim of robbery.[47] Impunity for such assaults appears to be less in Argentina compared to other countries in the region, partly due to the well-functioning court system in Buenos Aires, where most major media outlets are based. Violence against bloggers or online journalists by law enforcement agents or government officials is rare. However, in April 2012, a city council president in Candelaria punched a TV journalist and news website editor who was arguing against being denied access to cover a city council session;[48] the council president was subsequently charged for injuring the reporter.

There are no restrictions on anonymity for internet users, and neither bloggers nor website owners are required to register with the government. Users are able to freely post anonymous comments in a variety of online forums and there are no restrictions on the use of encryption. However, users must provide identifying information when purchasing a mobile phone line or prepaid SIM card.[49]

---

[45] Lillie Langtry, "Argentina: Concerns over new terrorism law," Memory in Latin America (blog), December 30, 2011, http://memoryinlatinamerica.blogspot.com/2011/12/argentina-concerns-over-new-terrorism.html; "Argentina: Fears Over Terror Law," New York Times, December 28, 2011, http://www.nytimes.com/2011/12/29/world/americas/argentina-fears-over-terror-law.html?_r=1&partner=rss&emc=rss.

[46] "Argentina," Committee to Protect Journalists, accessed July 31, 2012,http://cpj.org/2012/02/attacks-on-the-press-in-2011-argentina.php.

[47] IFEX, "FOPEA condemns attack on journalist in Mar del Plata," news release, August 2, 2011, http://www.ifex.org/argentina/2011/08/02/walker_shot/.

[48] Liliana Honorato, "Argentine city council president punches journalist in the face," Journalism in the Americas (blog), April 19, 2012, http://knightcenter.utexas.edu/blog/00-9784-argentine-city-council-president-punches-journalist-face.

[49] Law No. 19.798, Resolution No. 490/97 [in Spanish] (1997), "Text of the General Terms for Users of Mobile Communication Services," National Communications Commission, accessed March 20, 2012, http://www.cnc.gob.ar/normativa/sc0490_97.pdf.

A court order is required to intercept private communications,[50] including in cases related to national security.[51] These procedures are generally followed in practice, although the government did not publish figures on how many such interceptions are implemented annually. According to Google's Transparency Report, between January and June 2011, the Argentine authorities made 134 requests for user data covering 188 accounts and Google complied with approximately one third of them.[52] Over the past decade, there have been several scandals involving officials on both sides of the political spectrum engaging in illegal surveillance of opponents' telephone communications. In one high-profile scandal, evidence surfaced of navy personnel monitoring former President Nestor Kirchner for decades.[53] In another incident, the mayor of Buenos Aires, an opposition politician, and the city's police chief are alleged to have illegally wiretapped civic leaders, politicians, and trade union activists.[54] Most such incidents occurred in 2007 or earlier and there is no clear evidence that such violations of privacy continue. Meanwhile, related prosecutions continue to make their way through the courts.

Widespread technical violence is not a problem and there have been no reports of websites belonging to government opponents or civil society groups being the victims of denial-of-service (DoS) attacks. Should such incidents occur, those responsible would be liable for prosecution under the Criminal Code, as amended by Law No. 26388, mentioned above.

[50] Law No. 19.798, Articles *45 bis, 45 ter and 45 quáter* [in Spanish] (1972), "Law of National Telecommunications," Documentation and Information Center, accessed March 20, 2012, http://infoleg.mecon.gov.ar/infolegInternet/anexos/30000-34999/31922/texact.htm.
[51] Law No. 25.520 [in Spanish] (2001), "Law of National Intelligence," Documentation and Information Center, http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70496/norma.htm.
[52] "Google Transparency Report, Argentina."
[53] "Fernandez shakes up Argentine military," UPI.com, January 6, 2012, http://www.upi.com/Top_News/Special/2012/01/06/Fernandez-shakes-up-Argentine-military/UPI-92341325853530/.
[54] Nic Pollock, "Wiretapping Case Continues as Judge Oyarbide Closes Investigation Stage," The Argentina Independent, May 16, 2012, http://www.argentinaindependent.com/currentaffairs/wiretapping-case-continues-as-judge-oyarbide-closes-investigation-stage/; Maria Magro, "Two Clarin journalists testify in Buenos Aires wiretapping scandal," Journalism in the Americas (blog), November 18, 2010, http://knightcenter.utexas.edu/blog/two-clarin-journalists-testify-buenos-aires-wiretapping-scandal.

AUSTRALIA

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	3	2
Limits on Content (0-35)	6	6
Violations of User Rights (0-40)	9	10
Total (0-100)	**18**	**18**

* 0=most free, 100=least free

POPULATION: 22 million
INTERNET PENETRATION 2011: 79 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Australia enjoys affordable, high-quality access to the internet and other digital media. This quality of access improved in 2011 with the rollout of the National Broadband Network (NBN), a new communications network that aims to significantly improve broadband capacity and speed. Once fully implemented, the NBN will eliminate the need for any remaining dial-up connections and make high-speed broadband available in remote and rural areas.[1]

Access to online content is far-reaching, and Australians are able to explore all facets of political and societal discourse, including information about human rights violations. Nonetheless, privacy and freedom of expression concerns remain, particularly in the context of Australia's pending accession to the Convention on Cybercrime and the proposed Cybercrime Legislation Amendment Bill.[2] Unlike many other countries that have already ratified the convention, Australia is expected to go beyond the treaty's terms in calling for greater monitoring of all internet communications by internet service providers (ISPs).

[1] Australian Government National Broadband Network, "What is the NBN," accessed April 11, 2012, http://www.nbn.gov.au/about-the-nbn/what-is-the-nbn/.
[2] Cybercrime Legislation Amendment Bill 2011, Bills Digest no.31, 2011-12, accessed April 11, 2012, http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1112a/12bd031.

OBSTACLES TO ACCESS

Access to the internet and other digital media is widespread, almost ubiquitous. Australians have a number of internet connection options, including ADSL, wireless, cable, satellite, and dial-up.[3] Wireless systems have the capacity to reach 99 percent of the population, while satellite capabilities are able to reach 100 percent. Dial-up has been phasing out, with nearly 90 percent of internet connections now provided through other means.

In 2011, the National Broadband Network (NBN) was launched to further expand high-speed internet access across the country. The NBN includes laying high-speed fiber-optic cable to connect homes and businesses in Australia and incorporate 93 percent of the country's population, with prioritization of the rollout to remote communities with either no broadband capacity or limited connection. The other 7 percent would connect to the internet by new satellite and fixed wireless technologies.[4] With the development of the high-speed National Broadband Network (NBN),[5] all Australians, including those in more remote areas, will soon enjoy peak connection at a minimum of 12 Mbps using a "nationwide network of fibre, fixed wireless and satellite technologies."[6]

In 2011, Australia had an internet penetration rate of 79 percent,[7] and between 2010 and 2011, additional one million households gained access to broadband internet, with 73 percent of households equipped with a broadband connection by December 2011.[8] These figures are expected to steadily increase with the implementation of the NBN. Although internet access is widely available in locations such as libraries, educational institutions, and internet cafes, Australians predominantly access the internet from home, work, and increasingly through mobile telephones.

People of all ages are using the internet, but the elderly population lags behind.[9] In fact, age is a significant indicator of internet use, with 69 percent of Australians between 18 and 24

[3] Australian Communications and Media Authority (ACMA), *Communications Report, 2010-2011* (Canberra: ACMA, 2011), accessed March 2012, http://www.acma.gov.au/webwr/_assets/main/lib410148/communications_report_2010-11.pdf.
[4] Nick Galvin, "A Nation on The Broadband Wagon," in the special report, *Update on the NBN*, The Sydney Morning Herald, April 23, 2012, http://www.thenewspaperworks.com.au/files/dmfile/optus-nbn.pdf.
[5] Australian Government, Department of Broadband, Communications and the Digital Economy, "National Broadband Network," accessed March 2012, http://www.dbcde.gov.au/broadband/national_broadband_network.
[6] National Broadband Network Corporation, "Broadbanding Australia," accessed March 2012, www.nbnco.com.au/assets/brochures/nbn-co-corporate-brochure.pdf.
[7] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[8] Australian Bureau of Statistics, "Nearly three-quarters of Australian households now have broadband," media release, December 15, 2011, http://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/8146.0Media%20Release12010-11?opendocument&tabname=Summary&prodno=8146.0&issue=2010-11&num=&view=, accessed March 1 2012.
[9] Australian Bureau of Statistics, "Household Use of Information Technology, Australia, 2010-11," December 2011.

years accessing the internet at home on a daily basis, and 75 percent of people 15 years or over reporting having used the internet in the past 12 months.[10] By contrast, only 31 percent of those 65 and over had used the internet during the same time period.[11] Approximately 50 percent of Aboriginal and Torres Strait Islanders living in discrete indigenous communities (not major cities) have access to the internet, with 36 percent having internet access in the home.[12]

Australia had a mobile phone penetration rate of 108 percent in 2011 with some consumers using more than one phone or SIM card.[13] Third-generation (3G) mobile services are the driving force behind the recent growth in usage.[14] The overall mobile phone penetration rate in Aboriginal communities is unknown, however, and not all indigenous communities have mobile phone coverage.

Australia, like most other industrialized nations, hosts a competitive market for internet access, with 97 medium to very large ISPs in June 2011,[15] as well as hundreds of small ISPs. Many of the latter are "virtual" ISPs, maintaining only a retail presence and offering end users access through the network facilities of other companies.[16] ISPs are considered carriage service providers (CSPs) under Australian law. As such, they are required to obtain a license from the Australian Communications and Media Authority (ACMA) and to be members of the Telecommunications Industry Ombudsman (TIO), an independent dispute resolution service. Australian ISPs are co-regulated under Schedule 7 of the 1992 Broadcasting Services Act (BSA), meaning there is a combination of regulation by the ACMA and self-regulation by the telecommunications industry.[17] The industry's involvement consists of the development of industry standards and codes of practice.

The government has adopted a strong policy of technical neutrality. There are no limits to the amount of bandwidth that ISPs can supply, and ISPs are free to adopt internal market practices on traffic-shaping. Some Australian ISPs practice traffic-shaping under what are

[10] Australian Bureau of Statistics, "ONLINE @ HOME," June 2011, accessed March 2012, http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4102.0Main+Features50Jun+2011.
[11] Ibid.
[12] Australian Bureau of Statistics, "Internet Access at Home," 2008, accessed October 2010, http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4102.0Chapter10002008. For a comprehensive report on indigenous Internet use and access, see: ACMA, *Telecommunications in Remote Indigenous Communities* (Canberra: ACMA, 2008), p 48, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311397.
[13] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[14] Ibid.
[15] Australian Bureau of Statistics, "Internet Activity, Australia, June 2011."
[16] Australian Bureau of Statistics, "Internet Activity, Australia, Dec 2009."
[17] "Australian Communications and Media Authority Act 2005," accessed June 2010, http://www.austlii.edu.au/au/legis/cth/consol_act/acamaa2005453/; "Broadcasting Services Act 1992," accessed June 2010, http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/; ACMA, "Service Provider Responsibilities," http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_90157.

known as fair-use policies. If a customer is a heavy peer-to-peer user, for example, internet connectivity for those activities are slowed down to free bandwidth for other applications.[18] Advanced web applications such as the social-networking sites Facebook and MySpace, the Skype voice-communications system, and the video-sharing site YouTube are neither restricted nor blocked in Australia.

LIMITS ON CONTENT

Australian law does not provide for mandatory blocking or filtering of websites, blogs, chat rooms, or platforms for peer-to-peer file sharing. Users are able to access a wide range of information, and their ability to openly express dissatisfaction with politicians and criticize government policies is not hindered by the authorities.[19]

However, there are two systems in place that regulate internet content and place some restrictions on what can be viewed online. First, material deemed by the ACMA to be "prohibited content" is subject to take down notices. The ACMA notifies the relevant ISP that it is hosting illicit content and is then required to take down the offending material.[20] Under the BSA, the following categories of online content are prohibited:

- Any online content that is classified Refused Classification (RC) by the Classification Board, including real depictions of actual sexual activity; child pornography; depictions of bestiality; material containing excessive violence or sexual violence; detailed instruction in crime, violence, or drug use; and material that advocates the commission of a terrorist act.
- Content that is classified R 18+ and not subject to a restricted access system that prevents access by children, including depictions of simulated sexual activity; material containing strong, realistic violence; and other material dealing with intense adult themes.
- Content that is classified MA 15+, provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and that is not subject to a restricted access system, including material containing strong

[18] "Bad ISPs," VuzeWiki, accessed June 2010, http://wiki.vuze.com/w/Bad_ISPs#Australia.
[19] Chris Nash, "Freedom of the Press in Australia," Democratic Audit of Australia, November 19, 2003, http://apo.org.au/research/freedom-press-australia.
[20] "Who Is an Internet Content Host or an Internet Service Provider (and How Is the ABA Going to Notify Them?" Internet Society of Australia, accessed June 2010, http://www.isoc-au.org.au/Regulation/WhoisISP.html; Stuart Corner, "EFA Fights ACMA Over 'Take-Down' Notice," iTWire, April 20, 2010, http://www.itwire.com/it-policy-news/regulation/38423-efa-fights-acma-over-take-down-notice;"Guide for Internet Users," Internet Industry Association, March 23, 2008, http://www.iia.net.au/index.php/initiatives/guide-for-users.html.

> depictions of nudity, implied sexual activity, drug use, or violence; very frequent or very strong coarse language; and other material that is strong in impact.[21]

To date, this system for restricting access to videos, films, literature and similar material via take down notices has not emerged as problematic in terms of any overflow to information of political or social consequence. In addition, the general disposition is to allow adults unfettered access to R 18+ materials while protecting children from exposure to inappropriate content.

Under the second system, the ACMA may direct an ISP or content service provider to comply with the Code of Practice developed by the Australian Internet Industry Association (IIA). Failure to comply with such instructions may draw a maximum penalty of AUD$11,000 (US$11,400) per day. Other regulatory measures require ISPs to offer their customers a family-friendly filtering service.[22] This is known as voluntary filtering, as customers must select it as an option.

Draft legislation on mandatory filtering was proposed under the Labour government led by Kevin Rudd and then put aside during the election in August 2010. There have been no indications by the current Labour government led by Julia Gillard as to whether draft legislation on the matter will be reintroduced in the immediate future, but statements have been made that the government has no intention to abandon the plan altogether.[23] The list of sites to be blocked would initially focus on images of child abuse, particularly child pornography.

The proposed filtering system has been controversial due to concerns of over-blocking, censorship of adult materials, scope creep, and impairment of telecommunication access speeds.[24] While Prime Minister Gillard has voiced support for the filter in the media, the likelihood of any such proposal becoming law is slim due to the strong opposition to any such legislation by opposition parties.[25] In the interim, the three largest ISPs in Australia

[21] ACMA, "Prohibited Online Content," accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102.
[22] Internet Industry Association (IIA), *Internet Industry Code of Practice: Content Services Code for Industry Co-Regulation in the Area of Content Services (Pursuant to the Requirements of Schedule 7 of the Broadcasting Services Act 1992), Version 1.0*, 2008, http://www.iia.net.au/images/content_services_code_registration_version_1.0.pdf.
[23] Alana Maurushat and Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009); ACMA, "Internet Service Provider (ISP) Filtering," October 2011, http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering.
[24] See generally, Alana Maurushat and Renee Watt, "Australia's Internet filter Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009), page 18-25; and David Vaile and Renee Watt, "Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra," *University of New South Wales Law Review* Series 35 (2009).
[25] "Internet Filter is Right: Gillard," The Sydney Morning Herald, October 12, 2010, http://news.smh.com.au/breaking-news-national/internet-filter-is-right-gillard-20101012-16hiz.html.

(Telstra, Optus and Primus) voluntarily filter material listed as child abuse or child pornography.[26]

The many problems of classifying content in Australia came to light in the 2011 public inquiry and review of the current classification scheme by the Australian Law Reform Commission (ALRC). The ALRC released its final report in February 2012 entitled, "Classification-Content Regulations and Convergent Media," which recommended the creation of a new single regulator of classification and content, among other key features.[27] The new national classification scheme will also emphasise eight guiding principles.[28] While the ALRC's report announced sweeping reform to the classification and convergence of media content, it remains to be seen if the government will heed any of the recommendations.

Journalists, commentators, and ordinary users in Australia are not subject to censorship so long as their content does not amount to defamation or breach criminal laws, such as those against hate speech or racial vilification.[29] Nevertheless, the need to avoid defamation has been a significant driver of self-censorship by both the media and ordinary users (see "Violations of User Rights").

Aside from restrictions on prohibited content, incitement to violence, racial vilification, and defamation, Australians have access to a broad choice of online news sources that express diverse, uncensored political and social viewpoints. Individuals are able to use the internet and other technologies both as sources of information and as tools for mobilization.[30] Digital media such as blogs, Twitter feeds, Wikipedia pages, and Facebook groups have been harnessed for a wide variety of purposes ranging from elections to campaigns against government corporate activities, to a channel for safety-related alerts where urgent and immediate updates were required.[31] For instance, Google maps were used in a creative endeavor to map out fire dissemination in the devastating 2009 wildfires that spread across

[26] "Internet Service Provider (ISP) Filtering," accessed April 23, 2012, http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering.
[27] For some of the key features of the ALRC's new model, see: Australian Law Reform Commission, "Classification-Content Regulation and Convergent Media Final Report," February 2012, p 24, accessed April 23, 2012, http://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_118_for_web.pdf.
[28] See, Ibid, p 24-30.
[29] *Jones v. Toben* [2002] FCA 1150 (17 September 2002), http://www.austlii.edu.au/au/cases/cth/FCA/2002/1150.html.
[30] Re Lim, "Cronulla Riot: Confiscation of Mobile Phones, Invasion of Privacy and the Curbing of Free Speech," Act Now, March 15, 2006, http://www.actnow.com.au/Opinion/Cronulla_riot.aspx; Les Kennedy, "Man in Court Over Cronulla Revenge SMS," Sydney Morning Herald, December 6, 2006, http://www.smh.com.au/news/national/man-in-court-over-cronulla-revenge-sms/2006/12/06/1165081008241.html.
[31] Digital media, for example, is readily used for political campaigning and political protest in Australia. See, Terry Flew, "Not Yet the Internet Election: Online Media, Political Content and the 2007 Australian Federal Election," 2008, http://eprints.qut.edu.au/12611/1/12611.pdf.

the State of Victoria.[32] In 2011, Twitter feeds were used to assist the mobilization of people in the Occupy Sydney and Occupy Brisbane movements.[33]

VIOLATIONS OF USER RIGHTS

Australians' right to access internet content and freely engage in online discussions is based less in law than in the shared understanding of a fair and free society. Legal protection for free speech is limited to the constitutionally-implied freedom of political communication, which only extends to the limited context of political discourse during an election.[34] The full range of human rights in Australia, unlike in most other developed democracies, is not protected by a bill of rights or similar legislative instrument, and the courts have less ground to strike down legislation that infringes on civil liberties. Nonetheless, Australians benefit greatly from a culture of freedom of expression and freedom of information, further protected by an independent judiciary. The country is also a signatory to the International Covenant on Civil and Political Rights (ICCPR).

Australian defamation law has been interpreted with a wide scope[35] and is governed by legislation passed by the states as well as common-law principles. A person may bring a defamation case based on information posted by someone outside of Australia provided that the material can be accessed in the country and the defamed person enjoys a reputation in Australia. Civil actions over defamation are common and form the main impetus for self-censorship,[36] though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.[37] In one example in 2009, the operator of the Australian online discussion board ZGeek was named as a defendant in an AUD$42 million (US$43.5 million) defamation suit over comments posted on the forum,[38] but the case was later struck down by the courts.[39]

[32] John Liebhardt, "Australian wildfires and web tools," Global Voices, February 9, 2009, http://globalvoicesonline.org/2009/02/09/australian-wildfires-and-web-tools/.
[33] The Occupy Sydney Twitter page is available at http://twitter.com/occupySYDNEY. The Occupy Brisbane Twitter page is also available at http://twitter.com/OccupyBrisbane.
[34] For a full analysis of freedom of expression in Australia, see: Alana Maurushat and Sophia Christou, "Waltzing Matilda or Advance Australia Fair: Fair dealings copyright exemptions with user-generated content," *Media &Arts Law Review*, March 2009.
[35] Chris Nash, "Freedom of the Press in Australia," Democratic Audit of Australia, November 19, 2003. For more information generally on press freedom in Australia, see: Reporters Without Borders, http://en.rsf.org/australie.html.
[36] Irene Moss, "Report of the Independent Audit into the State of Free Speech in Australia," Australia's Right to Know Coaltion, October 31, 2011, http://www.alliance.org.au/documents/071031_right_to_know_report.pdf.
[37] Human Rights Constitutional Rights, "Australian Defamation Law," accessed June 2010, http://www.hrcr.org/safrica/expression/defamation.html.
[38] Asher Moses, "Online Forum Trolls Cost me Millions: Filmmaker," Sydney Morning Herald, July 9, 2009, http://www.smh.com.au/technology/technology-news/online-forum-trolls-cost-me-millions-filmmaker-20090715-dl4t.html.
[39] "ZGeek Law Suit Struck Down," Electronic Frontiers Australia, July 15, 2009, http://www.efa.org.au/2009/07/15/zgeek-defamation-lawsuit-struck-out/.

Criminal defamation charges have also been filed over online content. There have been a series of recent publicized defamation suits involving foreign companies such as Google, Yahoo, and Twitter. In October 2011 the Supreme Court of Queensland ordered Google Australia to release the details of the creators of websites that had published defamatory material about the author Jamie McIntyre.[40] In January 2012, the online music critic Joshua Meggit instigated proceedings against Twitter in Australia for failing to remove a defamatory tweet about him.[41] In another case, which is currently pending, health researcher Dr. Janice Duffy sued Google for refusing to remove defamatory links to the U.S.-based consumer complaint website, Ripoff Report, from the Google search engine.[42]

Law enforcement agencies may search and seize computers and compel an ISP to intercept and store data from those suspected of committing a crime, but such actions require a lawful warrant. The collection and monitoring of communications fall within the purview of the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records, however, are regulated by the Telecommunications Act 1997 (TA).[43] It is prohibited for ISPs and similar entities, acting on their own, to monitor and disclose the content of communications without the customer's consent.[44] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.[45] The TIAA and TA expressly authorize a range of disclosures, including to specified law enforcement and tax agencies, all of which require a warrant.

ISPs are currently able to monitor their networks without a warrant for "network protection duties," such as curtailing malicious software and spam.[46] Pending Australia's accession to the Convention on Cybercrime and adoption of the Cybercrime Legislation Amendment Bill 2011,[47] ISPs will be required to perform wider monitoring functions. Unlike many other countries that have already ratified the convention, Australia is expected to go beyond the

[40] Alison Sandy and Alex Dickinson, "Supreme Court Orders Google Australia to Release Details of Creators of Website," News Australia, October 7, 2011, http://jamiemcintyre.com/jamie-mcintyre-winning-battle-supremem-court-orders-google-australia-release-details-creators-defamatory-website/.

[41] "Australian Joshua Meggit Sues Twitter," Socialite Media, February 20, 2012, http://socialitemedia.com.au/australian-joshua-meggitt-sues-twitter/824/.

[42] Rachel Wells, "Google in the Gun as Cyber Victims Fight Back," Sydney Morning Herald, April 2, 2012, http://www.smh.com.au/technology/technology-news/google-in-the-gun-as-cyber-hate-victims-fight-back-20120401-1w6nf.html#ixzz1rmmmBLSx.

[43] Telecommunications Act 1997, Part 13, accessed June 2010, http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.

[44] Part 2-1, section 7, of the Telecommunications (Interception and Access) Act 1979 (TIAA) prohibits disclosure of an interception or communications, and Part 3-1, section 108, of the TIAA prohibits access to stored communications. See http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.

[45] Criminal offenses are outlined in Part 2-9 of the TIAA, while civil remedies are outlined in Part 2-10.

[46] Alana Maurushat, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Obfuscation Crime Tools?" *University of New South Wales Law Journal* 16, no. 1, forthcoming.

[47] Cybercrime Legislation Amendment Bill 2011, Bills Digest no.31, 2011-12, accessed April 11, 2012, http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1112a/12bd031.

treaty's terms in calling for greater monitoring of all internet communications by ISPs. Under the Convention, an ISP is only required to monitor, intercept, and retain data when presented with a warrant, and only in conjunction with an active and ongoing criminal investigation of types of crimes listed in the Convention: fraud and forgery; copyright; unauthorized access, modification and interference to data or data system (computer, network); and child pornography provisions.

Under the proposed bill, timely preservation of evidence that might otherwise be lost may be obtained without a warrant. Preservation notices are issued by the Australian Federal Police (AFP) and are available for both domestic and international investigations. Carriage service providers (CSP in the legislation but commonly interchanged with ISP) must preserve stored communications of a target(s) for up to 90 days, depending on the type of preservation notice received from the AFP. A foreign country may also send a request to the AFP, who would then make a request to the Australian CSP. It is important to note, however, that preservation notices compel a carriage service provider merely to store information and that communications may only be disclosed when a valid Australian warrant has been issued.

Public input into Australia's accession to the Convention was sought in the form of a Cybercrime Inquiry. Many submissions to the inquiry expressed concern over a lack of safeguards, the privacy invasiveness of the proposed provisions,[48] and the overly broad scope of cooperation with foreign parties extending beyond the requirements of the Convention.[49] For example, the Convention only requires mutual cooperation between countries for preservation notices and real time evidence collection in the context of four areas: fraud and forgery; child pornography; copyright infringement; and unauthorized access, modification or interference with data, data systems or a computer. The Australian proposal does not limit mutual cooperation to the crimes specified in the Convention but potentially opens the door to any type of crime.

Presently, ISPs are required by law to have real time interception capabilities,[50] generally to be used for gathering evidence in connection with serious offenses such as murder, terrorism, and child pornography.[51] Under the proposed Cybercrime Legislation Amendment Bill, such real time evidence obligations will be expanded to any crime

[48] Australian Privacy Foundation, "Cybercrime Legislation Amendment Bill 2011, Submission to the Joint Standing Committee on Cyber-Safety," August 5, 2011.
[49] Law Council of Australia, "Submission No. 5, Inquiry into Cybercrime Legislation Amendment Bill 2011," Joint Select Committee on Cyber-Security, July 14, 2011, p. 3. http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jscc/cybercrime_bill/subs.htm.
[50] Ibid.
[51] Section 5D of the *Telecommunications Act 1997*.

provided that a number of set procedural conditions are met. The data may be preserved but cannot be disclosed in the absence of a warrant.

Users do not need to register to use the internet, nor are there restrictions placed on anonymous communications. The same cannot be said of mobile phone users, as verified identification information is required to purchase any prepaid mobile service. Additional personal information is required for the service provider before a phone may be activated. All purchase information is stored while the service remains activated, and it may be accessed by law enforcement and emergency agencies with a valid warrant.[52]

There have been a number of politically-motivated cyberattacks, particularly distributed denial-of-service attacks (DDoS) that have led to websites being inaccessible or flooded with substituted content for various lengths of time. For example, offline marches and online acts of protest were staged in response to the Australian government's decision to introduce a mandatory filter in 2010. One of these protests was the online defacement and DDoS attack of the Australian Parliamentary website by the Anonymous hacktivist group, dubbed Operation Titstorm. The attack brought down the parliament's website for three days by bombarding it with pornographic images.[53] In 2011, Matthew George, an Australian member of Anonymous who participated in Operation Titstorm, was charged and convicted of incitement, and was given an AUS$550 (US$570) fine.[54] More severe cyberattacks on the nation's critical infrastructure (such as electric grids, hospitals, and banks) have occurred as well, though to date, attacks on banking institutions for financial motives have been much more frequent.[55]

[52] ACMA, "Pre-paid Mobile Services—Consumer Information Provision Fact Sheet," accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_9079.
[53] Alana Maurushat, "Ethical Hacking (2012): A Report for A Report for the National Cyber Security Division of Public Safety Canada." Publication on file with author. Report to be released to the public in 2012.
[54] Sarah Whyte, "Meet the hacktivist who tried to take down the government," Sydney Morning Herald, March 14, 2011, http://www.smh.com.au/technology/security/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html.
[55] AusCERT Conference (2009), closed session invite-only workshop on cybercrime, Chatham House Rules.

AZERBAIJAN

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	15	13
Limits on Content (0-35)	15	16
Violations of User Rights (0-40)	18	21
Total (0-100)	**48**	**50**

* 0=most free, 100=least free

POPULATION: 9.3 million
INTERNET PENETRATION 2011: 50 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

As the host of the seventh annual Internet Governance Forum (IGF) in November 2012, Azerbaijan's government has been eager to promote itself as a leader of information and communication technology (ICT) innovation in the region, with internet usage and online activism growing significantly in 2011. This growth has spurred increasing efforts by the authorities to exert greater control over the medium, though it remains much less restricted compared to print and broadcast media, the main sources of information for most citizens.

The internet was first introduced in Azerbaijan in 1994 and became available for all citizens in 1996. As a result of policies aimed at lowering prices that were enacted in 2007, the internet is now relatively accessible for businesses and individuals in urban areas; however, villages and communities outside of urban regions still have limited access.[1] Despite a notable increase in internet penetration over the past few years, the quality of connections remains very low, with paid prices not corresponding to advertised speeds and many users still relying on slow dial-up connections.

The Azerbaijani government does not generally censor online content or restrict access to ICTs, but in 2011, there were occasional blocks imposed on certain opposition news sites such as Radio Azadliq, the website of the Azerbaijan service of Radio Free Europe/Radio Liberty (RFE/RL). In addition, there were numerous arrests, prosecutions, and incidents of

[1] "Beynəlxalq Telekommunikasiya İttifaqı: Azərbaycan mobil rabitə tariflərinin azaldılması üzrə lider-ölkədir," APA Economics, February 24, 2010, http://az.apa.az/news.php?id=178885 [in Azerbaijani].

extralegal intimidation and violence against online activists for organizing demonstrations or expressing critical views of the government on social media websites, particularly following a series of pro-democracy protests inspired by the Arab Spring events in early 2011. In many cases, detained activists were given jail sentences on trumped-up charges of criminal defamation, illegal drug possession, hooliganism, or other politically motivated allegations. Fearing further Arab Spring-inspired protests, in early 2012, the Azerbaijani authorities reportedly ramped up their surveillance capabilities through the installation of "black boxes" on the Azercell mobile phone network, enabling security agencies to monitor all mobile communications in real-time.

OBSTACLES TO ACCESS

According to the International Telecommunication Union (ITU), 50 percent of the population had access to the internet in 2011, a significant increase from 2006 when the penetration rate was roughly 12 percent.[2] Fixed-broadband internet subscriptions also increased remarkably from 4,000 in 2006 to nearly one million in 2011, representing a broadband penetration rate of 10.5 percent.[3] Nonetheless, access for residents outside of the capital Baku continues to be extremely limited.

To increase accessibility, state-owned internet service providers (ISPs) dropped prices by 25 to 50 percent in October 2011.[4] At the end of 2011, ADSL connections at an average speed of 1 Mbps cost 15 AZN (US$20),[5] amounting to 4 to 5 percent of average wages in Azerbaijan. While these prices are significantly lower than several years ago, they are still out of reach for many Azerbaijanis whose average monthly salary is approximately 356 AZN (US$453).[6] Furthermore, many users still access the internet at painfully slow dial-up speeds and face problems accessing multimedia content such as audio and video material.

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[3] Ibid.

[4] "ISPs of Azerbaijan announced a price reduction," 1news.az, September 30, 2011, http://www.1news.az/economy/tech/20110930050420696.html [in Russian].

[5] "Ali Abbasov: Cost of ADSL-Internet in Azerbaijan is 4-5% of Average Wage," Contact.az, October 11, 2011, http://contact.az/docs/2011/Economics&Finance/101110442en.htm [in Russian].

[6] "Real average salary in Azerbaijan fell by 0.93% with nominal rise by 0.17%," ABC.az, December 16, 2011, http://abc.az/eng/news/60624.html.

Privately-owned but government-controlled Delta Telecom[7] (formerly AzerSat) is the country's largest satellite and fiber-optic backbone provider with approximately 40 ISPs operating in Azerbaijan on a retail basis. Delta Telecom was also the first company to implement a WiMAX technology project in the country in February 2010, laying the foundation for the use of wireless, broadband, and unlimited internet access. As the primary ISP in the country and owner of the international gateway, Delta Telecom supplies international connectivity to 90 to 95 percent of all users in Azerbaijan and sells international traffic to almost all ISPs.[8] The largest ISP operating outside of Baku is the state-owned AzTelecom, which has ownership ties to the Ministry of Communication and Information Technologies (MCIT).[9] Azertelecom, owned by Azerfon, completed its fiber-optic network in 2011 and is now competing for Delta Telecom's business.[10] Almost all ISPs supply users with bandwidth purchased from Delta Telecom and Azertelecom.

With Azertelekom's growing role in the internet business, government control over ICTs has become more apparent, particularly after it was uncovered in 2011 that Azerfon is largely owned by President Ilham Aliyev's daughters.[11] Furthermore, there is a lack of transparency over the ownership of other ICT resources. While there are no specific legal provisions or licensing requirements for ISPs in Azerbaijan, MCIT refuses to answer inquiries on the ownership of license holders.[12]

Usage of mobile phones in Azerbaijan has continued to grow steadily, with mobile phone penetration increasing from 38 percent in 2006 to over 108 percent in 2011.[13] There are three mobile service providers using the Global System for Mobile Communications (GSM) standard: Azercell, Azerfon, and Bakcell. In 2009, Azerfon, in a partnership with Britain's Vodafone, was the only company with a license for 3G service; however, in response to a number of critical media reports, Azercell and Bakcell were issued licenses in 2011, breaking Azerfon's monopoly over the 3G market. Azercell and Bakcell reduced prices to

[7] The company's ownership structure is not transparent. Many experts say that Delta Telecom is in fact owned by Baylor Ayyubov, the president's security chief, but there is no official proof of this. Requests for information on the matter were unanswered.
[8] "Azerbaijan country profile," Open Net Initiative, November 17, 2010, http://opennet.net/research/profiles/azerbaijan.
[9] Yashar Hajiyev, "Azerbaijan," European Commission, accessed August 30, 2012, http://ec.europa.eu/information_society/activities/internationalrel/docs/pi_study_rus_ukr_arm_azerb_bel_geor_kaz_mold/5_azerbaijan.pdf.
[10] "Azerbaijan Network," Azertelecom.az, accessed September 5, 2012, http://www.azertelecom.az/en/aznetwork/.
[11] Khadija Ismayilova, "Azerbaijani President's Daughter's Tied to Fast-Rising Telecoms Firm," Radio Free Europe/Radio Liberty, June 27, 2011, http://www.rferl.org/content/azerbaijan_president_aliyev_daughters_tied_to_telecoms_firm/24248340.html.
[12] Response of the Ministry of Communication to a written request for information.
[13] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

increase demand for mobile internet when they launched 3G services.[14] As a result, the number of mobile internet users on the Azercell network—the country's largest mobile communication provider with 55 percent of the market[15]—increased 300 fold in 2011, according to a company representative.[16]

Azerbaijan does not have an independent regulatory body for the telecommunications sector, and the MCIT performs the basic regulatory functions pursuant to the 2005 Law on Telecommunications. The MCIT also has a monopoly over the sale of the ".az" domain, which cannot be obtained online and requires an in-person application, subjecting the process to bureaucratic red tape and possible corruption.

LIMITS ON CONTENT

The Azerbaijani government did not engage in widespread censorship of the internet in 2011. However, domestic users regularly reported problems accessing oppositional content on websites such as Radio Azadliq, the Azerbaijan service of Radio Free Europe/Radio Liberty (RFE/RL). Official authorities have denied allegations of blocking,[17] and there is no established process through which affected entities can appeal. Sporadic filtering has also become a problem for opposition websites from the Azerbaijani diaspora such as Azdiaspora.org. Meanwhile, both the MCIT and Ministry of Education run a hotline program to uncover allegedly illegal and dangerous content.[18]

According to clause 4.2(a) of the "Rules for Using Internet Services," internet providers can unilaterally suspend services provided to subscribers in cases that violate the rules stipulated in the law "On Telecommunications." Furthermore, a provider can suspend delivery of internet services in certain circumstances including in times of war, events of natural disasters, and states of emergency, though none of these legal provisions were employed in 2011 or early 2012.

There are limited deletions of online content implemented based upon a take down notice system, primarily related to personal data. Subject to Articles 5.7 and 7.2 of the law "On

[14] "Azercell reduces prices for mobile internet services (Azerbaijan)," Wireless Federation, November 28, 2011, http://wirelessfederation.com/news/90875-azercell-reduces-prices-for-mobile-internet-services-azerbaijan/.
[15] "About us," Azercell, accessed September 5, 2012, http://company.azercell.com/en/.
[16] Nijat Mustafayev, "Number of mobile internet users of Azercell increased sharply over the past year," APA-Economics, November 18, 2011, http://en.apa.az/news.php?id=159794.
[17] "Azerbaijan's IT Ministry rejects claims of increased control over internet," News.az, July 20, 211, http://www.news.az/articles/tech/40854.
[18] Yaman Akdeniz, "Freedom of Expression on the Internet," Organization for Security and Cooperation in Europe, 2010, http://www.osce.org/fom/80723.

Personal Data," personal data published without the consent of an individual must be removed from websites following a written demand from the individual concerned, a court, or the executive branch.

Access to Web 2.0 applications such as the social-networking site Facebook and the microblogging service Twitter is unrestricted, and such sites are increasingly used to disseminate content critical of the government. Facebook, in particular, has become a key source of information on rallies, protests, and social issues such as housing demolitions.
The number of registered Facebook users grew from approximately 279,000 at the end of December 2010 to 700,000 in December 2011,[19] with the largest contingent of Facebook users being young people between the ages of 18 and 24.[20]

In addition, the incredible growth of blogging that began in 2007 continued to increase in 2011. With the introduction of Azerbaijani-language blogging platforms, active bloggers writing in the native language provide an alternative source of information on many subjects that are ignored or distorted by the traditional media. There are more than 27,000 blogs in Azerbaijan, most of which are written in the Azerbaijani language, and only about 1,000 blogs are written in English, Russian, and other languages. Many bloggers, such as Ali Novruzov, Arzu Geybullayeva, Nigar Fatali and Zaur Gurbanly, are well known for their independent views, and an estimated 50,000 to 70,000 users read blogs online. Beyond blogging, according to the head of the Press Council in Azerbaijan, more than ten internet radio stations and TV channels operate in the country's virtual space, and over 100,000 users watch television online. Additionally, there are more than 40 online news websites.[21]

As journalists, activists, and those critical of the government have increasingly turned to the internet to express their views, the Azerbaijani authorities have amplified their efforts to clamp down on online activities and stifle opposition voices through tactics such as internet cafe raids, netizen arrests, and other extralegal intimidation (see "Violation on User Rights"). Some state universities warn students that they will encounter problems if they participate in online political activism. Students are instead urged to be very active in defending the government and its positions in their posts and comments on Facebook and other social media. These efforts have had a chilling effect on internet users who may be practicing self-censorship out of fear of government reprisals, although the extent of self-censorship is not as widespread as in the traditional media. Furthermore, government-

[19] "Facebook Statistics Azerbaijan," Socialbakers, accessed December 2011, http://www.socialbakers.com/facebook-statistics/azerbaijan.
[20] "Issued by the number of Facebook users in Azerbaijan," Day.az, September 20, 2011, http://news.day.az/hitech/289329.html [in Russian].
[21] "The number of Internet users in Azerbaijan is 45% of the population," Regnum News Agency, February 3, 2011. http://regnum.su/news/fd-abroad/azeri/1379705.html [in Russian].

friendly online media outlets are the main beneficiaries of the advertisement market. As is the case in the traditional media sphere, state-owned and private companies tend to refrain from advertising their products in independent or opposition online media.

In response to displays of citizen activism online in early 2011, some local state-run television stations launched campaigns criticizing social-networking sites, including broadcasting interviews with supposed internet experts who argued that online activities pose a threat to the state's security and image.[22] Similarly, in an attempt to discredit online activists and keep young people away from social media and political activism, the authorities also aired on state television interviews with psychologists who described Facebook users as "mentally ill."[23]

Despite these manipulative efforts, youth activists, organizations, and movements are widely represented in social media, providing information, organizing activities and events, and arranging flash mobs via the internet. Inspired by the Arab Spring uprisings in early 2011, young activists in Azerbaijan used social media to organize demonstrations in March and April 2011 against the government's authoritarian rule, calling for democratic reforms and an end to pervasive government corruption.[24]

VIOLATIONS OF USER RIGHTS

Article 47 of the constitution guarantees freedom of thought and speech.[25] In addition, Article 50 provides the right to distribute information, guarantees freedom of the mass media, and prohibits censorship. In practice, however, the authorities aggressively use various forms of legislation to stifle freedom in the print and broadcast media. Libel is a criminal offense,[26] and traditional media journalists who criticize the authorities are frequently prosecuted and imprisoned. Furthermore, the judiciary is largely subservient to the executive branch.[27] Under the Law on Mass Media of 1999, the internet is designated as a form of mass media, thus all rules applied to traditional media can be used to regulate the

[22] "Azerbaijani Activists Under Pressure Ahead of Protest Day," Radio Free Europe/Radio Liberty, March 7, 2011, http://www.rferl.org/content/azerbaijan_activist_prison/2330387.html.
[23] "Don't let them be silenced," Amnesty International, November 16, 2011, http://www.amnesty.org/en/appeals-for-action/freeazerbaijan.
[24] Natasha Schmidt, "Freedom of expression online," Chapter 8, *Running Scared: Azerbaijan's Silenced Voices*, Article 19: Global Campaign for Free Expression, 2012, http://www.article19.org/data/files/medialibrary/3003/12-03-26-azerbaijan.pdf.
[25] The constitution is available in English at http://en.president.az/azerbaijan/constitution.
[26] "Azerbaijan Criminal Code: Article 147. Defamation," Conseil de l'Europe, December 12, 2003, accessed August 30, 2012, http://www.coe.int/t/dghl/standardsetting/media/Doc/DH-MM(2003)006rev_fr.asp#P281_18801.
[27] Karin Karlekar, ed., "Azerbaijan," *Freedom of the Press 2011*, http://www.freedomhouse.org/report/freedom-press/2011/azerbaijan.

online sphere as well.[28] In November 2010, it was announced that the government-controlled Press Council would start monitoring online news sources for their compliance with the rules of professional journalism.[29]

While there are no laws that specifically criminalize online expression in Azerbaijan, there has been a growing trend in recent years of the authorities broadly applying existing laws to prosecute journalists and citizens for their online activities. In an effort to clamp down on free expression and silence critical voices in both the traditional media and online, the Azerbaijani authorities have increasingly detained critics on tenuous charges not directly related to their work. In many cases, arrests have been made based on politically motivated allegations of criminal defamation, fabricated accusations of illegal drug possession, or other such trumped-up charges. This trend was particularly notable following the Arab Spring-inspired events in March and April 2011 when hundreds of demonstrators took to the streets of Baku to protest against government corruption, call for fair elections, and demand respect for human rights. The demonstrations resulted in numerous arrests, with some protesters sentenced to long prison terms based on unfounded allegations and following unfair trials. According to Amnesty International, 17 people convicted around the time of the protests are to be regarded as prisoners of conscience since there was no evidence that the imprisoned opposition activists had engaged in anything more than the legitimate exercise of their right to freedom of expression and association.[30]

Among the arrested was Jabbar Savalan, a student who was accused of drug possession on February 5, 2011, a day after he posted on Facebook a call for Egypt-inspired protests against the government. With no history of drug use or possession, Savalan's supporters believed the drugs found on him were planted. He was sentenced to two and a half years in prison on the trumped-up charges but was released on a presidential pardon in late December 2011 after serving 11 months in prison. Another young man, Bakhtiyar Hajiyev, a blogger and civic activist involved in organizing a mass protest planned for March 11, 2011, was arrested on March 4 and convicted in May on charges of evading military service. Bakhtiyar had requested alternative military service as provided by the Constitution; nevertheless, he was sentenced to two years imprisonment and was reportedly beaten while in police custody.[31] Another protest organizer, Strasbourg-based blogger Enlur Majidli, was

[28] "Law of the Republic of Azerbaijan 'About Mass Media,'" Azerbaijan National Academy of Sciences, December 7, 1999, http://ict.az/en/index.php?option=com_content&task=view&id=477&Itemid=95.
[29] "Control Over Online Sources and Facebook-like sites in Azerbaijan," Today.az, November 27, 2010, http://www.today.az/view.php?id=77287.
[30] "International community must act on Azerbaijan crackdown," Amnesty International, November 16, 2011, http://www.amnesty.org/en/news/international-community-must-act-azerbaijan-crackdown-2011-11-16.
[31] "Azerbaijan: Youth Activists Targeted as Freedom of Expression Clampdown Continues," Article 19, March 10, 2011, http://www.article19.org/resources.php/resource/1732/en/azerbaijan:-youth-activists-targeted-as-freedom-of-expression-clampdown-continues.

accused of inciting hatred and calling for the violent overthrow of the government. Criminal proceedings have been initiated against Majidli in absentia, and he could face up to 12 years in prison if he returns to Azerbaijan.[32]

In another case, the editor-in-chief of the website Islamazeri.com, Ramin Bayramov, was arrested in August 2011 and sentenced in March 2012 to 18 months in prison on charges of possessing illegal arms and drugs, which Baryamov's lawyer believes were planted.[33] Similarly, blogger and human rights activist Taleh Khasmammadov was arrested in November 2011 and was still detained as of March 2012 on charges of hooliganism, although it is believed that Khasmammadov was targeted for his blogging activities, particularly for his report on the mafia and human trafficking in the country's Ujar region.[34]

Separately, on March 1, 2012, mass demonstrations took place in the remote town of Guba, prompted by the circulation of an online video. At least 17 people were subsequently arrested, including two journalists from the Khayal TV station who were accused of provoking the protests after posting the video on YouTube. The clip featured the regional governor Rauf Habibov allegedly insulting the local population. Its circulation prompted thousands of protestors to take to the streets demanding the governor's resignation.[35] In response to the unrest, the authorities searched several internet cafes in Guba to identify the individual responsible for posting the video. The authorities also tried to determine the authors of comments posted on social-networking websites that called for the demonstrations.[36]

In a positive development, journalist and editor-in-chief of the independent newspapers *Realny Azerbaijan* and *Gundalik Azarbaycan*, Eynulla Fatullayev, was given a presidential pardon and released from prison in May 2011 after a significant international campaign that led to a judgment issued by the European Court of Human Rights demanding his release. Fatullayev had been in prison since 2007 on both defamation and terrorism charges based on an online post about a massacre during the 1992 Nagorno-Karabakh conflict.[37]

[32] "Azerbaijan's Facebook Dissident," Indexoncensorship.org, April 27, 2011, http://www.indexoncensorship.org/2011/04/azerbaijans-facebook-dissident/.
[33] Rebecca Vincent, "Political use of the law to silence freedom," Chapter 4, *Running Scared: Azerbaijan's Silenced Voices*, Article 19: Global Campaign for Free Expression, 2012, http://www.article19.org/data/files/medialibrary/3003/12-03-26-azerbaijan.pdf.
[34] Ibid.
[35] Shahin Abbasov, "Report: Clashes in Azerbaijan Prompt Dismissal of Regional Government Official," Eurasianet.org, March 1, 2012, http://www.eurasianet.org/node/65068.
[36] Shahin Abbasov, "Azerbaijan: Is Guba Protest Response a Harbinger of a Political Shift in Baku?" Eurasianet.org, March 6, 2012, http://www.eurasianet.org/node/65092.
[37] "Jailed Azerbaijani journalist pardoned," Amnesty International, press release, May 26, 2011, http://www.amnestyusa.org/our-work/latest-victories/jailed-azerbaijani-journalist-pardoned.

In addition to the growing trend of politically motivated arrests of online journalists and bloggers, internet users have faced increasing levels of extralegal intimidation and physical violence for their online activities. During the March-April 2011 pro-democracy protests in Baku, for example, many journalists and bloggers were physically attacked while trying to report on the demonstrations.[38] In a tragic case, prominent Azerbaijani journalist and writer, Rafiq Tagi, died on November 23, 2011 in Baku four days after being victim to a brutal knife attack. Tagi had been receiving death threats for weeks prior to the attack, which were believed to be in response to an article he published on Radio Azadliq's website that criticized the current Iranian government and discredited Islam.[39] According to research by civil society representatives, the official investigation into Tagi's death has had serious shortcomings, and no suspects had been arrested as of mid-2012.[40]

Netizens and their family members have also been subject to instances of extralegal intimidation and harassment through surprise police visits to their homes, summons to local branches of the Ministry of National Security for questioning, and arbitrary job losses.[41] In early March 2011, for example, activist Etibar Salmanli reported being visited by the police at his home after a video was posted on YouTube showing him promoting the March 11 protests.[42] Salmanli's parents were also summoned to the police and the Surakhani district education department for questioning about their son's activities. In June 2011, Nijat Mammadbayov was fired from *Azertag*, the state-run news agency, after posting a status on his Facebook page criticizing the agency. He was told to either delete his post and write a redaction or resign.

In another incident, the investigative journalist Khadija Ismayilova became the victim of a blackmail campaign in March 2012 that attempted to silence her by publishing private personal footage aimed at damaging her reputation.. Known for her reporting on corruption in the country, including investigations into the president's conduct and business activities, Ismayilova had been regularly disseminating her reports on social-networking sites such as Facebook, where she has a wide following. The threats against her included intimate photographs of her being taken and then sent to her with a warning to "behave." Refusing to

[38] "Journalists among victims of regime's violent response to pro-democracy protests," Reporters Without Borders, April 6, 2011, http://en.rsf.org/azerbaijan-journalists-among-victims-of-05-04-2011,39953.html.
[39] "Azerbaijan: Justice for Rafiq Tagi," Article 19, November 25, 2011, http://www.article19.org/resources.php/resource/2877/en/azerbaijan:-justice-for-rafiq-tagi.
[40] Johann Bihr, "Impunity for violence against journalists," Chapter 3, *Running Scared: Azerbaijan's Silenced Voices*, Article 19: Global Campaign for Free Expression, 2012, http://www.article19.org/data/files/medialibrary/3003/12-03-26-azerbaijan.pdf.
[41] U.S. Department of State, "Azerbaijan," Country Reports on Human Rights Practices for 2011, Bureau of Democracy, Human Rights and Labor, http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper.
[42] "Youth Activist Etibar Salmanli Harassed By Local Police," Azeri Report, March 7, 2011, http://azerireport.com/index.php?option=com_content&task=view&id=2650.

be silenced, Ismayilova instead went public with the blackmail attempt, and in retaliation, an intimate video of Ismayilova filmed by hidden camera was distributed over the internet. While threats against journalists are not uncommon in Azerbaijan, Ismayilova's case received an unprecedented groundswell of attention and support through social-networking sites both domestically and globally, signifying civil society's increasing pushback against government efforts to restrict freedom of expression. Nevertheless, the individuals responsible for violating Ismayilova's privacy remained unknown and unpunished as of mid-2012.[43]

It is unclear to what extent security agencies monitor ICT activity or track user data in Azerbaijan. Most users do not have licenses for the software on their computers, which leaves them vulnerable to security threats such as viruses and other malicious programs that could be implanted to monitor their activity. While the law explicitly prohibits the arbitrary invasion of privacy and court orders are required for the surveillance of private communications, the law "On operative-search activity" (Article 10, section IV) authorizes law enforcement agencies to conduct surveillance without a court order in cases regarded as necessary "to prevent serious crimes against the person or especially dangerous crimes against the state."[44] The unclear parameters for what constitutes preventive action leave the law open to abuse. As such, it has long been believed that the Ministry of National Security and Ministry of Internal Affairs monitor the phone and internet communications of certain individuals, especially foreigners, known activists, and business figures.[45] Such suspicions were confirmed by many of those detained for their involvement in the March 2011 protests who reported that the authorities had referred to their Facebook activities and private communications during interrogations.

In a particularly worrying development ahead of the Eurovision Song Contest hosted in Azerbaijan in May 2012, a Swedish investigative documentary revealed in April 2012 evidence of a blanket mobile phone surveillance system employed by the telephone company Azercell.[46] With help from the Stockholm-based telecom TeliaSonera, Azercell has reportedly installed "black box" devices on its networks that allow government security services and the police to monitor all mobile phone communications—including text messages, internet traffic, and phone calls—in real time without any judicial oversight. In addition, insider reports described how Azercell has set aside special offices in their

[43] Robert Coalson, "Azerbaijani Journalist Defiant in Face of Blackmail Bid," Radio Free Europe/Radio Liberty, March 9, 2012, http://www.rferl.org/content/azerbaijan_ismailova_blackmail_rferl_journalists_threats/24509372.html.
[44] "Article 10. Operative-search measures," Law of the Azerbaijan Republic, On operative-search activity, accessed September 5, 2012, http://taxes.caspel.com/qanun/728_eng.pdf.
[45] U.S. Department of State, "Azerbaijan," Country Reports on Human Rights Practices for 2011, Bureau of Democracy, Human Rights and Labor, http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper.
[46] "Video: The Black Boxes," SVT.se, April 26, 2012, http://www.svt.se/ug/video-the-black-boxes-3.

headquarters for government authorities to conduct surveillance activities. While it is unclear exactly when the monitoring system was installed and put into practice, one source working for TeliaSonera noted that "the Arab Spring prompted the regimes to tighten their surveillance….There's no limit to how much wiretapping is done, none at all."[47]

Wrongful access to a computer, such as through the implantation of viruses or security breaches, is punishable under Chapter 30 of the Criminal Code.[48] Internet security is also dealt with in the Law on National Security of 2004 and the Law on Protection of Unauthorized Information of 2004. Hacking attacks aimed at Azerbaijani internet users and websites often come from Armenian internet protocol (IP) addresses, and the timing of such attacks typically coincides with politically sensitive dates related to the unresolved territorial conflict between the two countries. Sometimes attacks occur after high-profile political statements. The ostensibly Armenian-based attacks have targeted the websites of entities such as the MCIT, the National Library, and the public television broadcaster. The Anti-Cybercriminal Organization is the main body working against cyberattacks in Azerbaijan, and the country ratified the Council of Europe's Convention on Cybercrime in March 2010, which took effect in July 2010.

Throughout 2011, some opposition news websites, including Yeni Musavat, Radio Azadliq, and the personal blog of the Popular Front Party's chairman Ali Kerimli, were subject to constant attacks that resulted in temporary shutdowns.[49] The newspaper Yeni Musavat speculated that the cyberattack against it could have been launched by the Ministry of Defense as a response to its critical reporting, but the ministry denied the allegations.[50] In June 2011, the Popular Front Party issued a statement also accusing the government of cyberattacks against its website.[51] Nevertheless, the sites of state bodies and state-controlled media have also been subject to an increasing number of cyberattacks over the past year,

[47] Ryan Gallagher, "Your Eurovision Song Contest Vote May Be Monitored: Mass Surveillance in Former Soviet Republics," Slate.com, April 30, 2012, http://www.slate.com/blogs/future_tense/2012/04/30/black_box_surveillance_of_phones_email_in_former_soviet_republics_.html.

[48] An unofficial English translation of the criminal code is available at http://www.legislationline.org/download/action/download/id/1658/file/4b3ff87c005675cfd74058077132.htm/preview.

[49] "Two more Azerbaijani websites undergo hacker attacks," Azerbaijani News Network, April 9, 2012, http://ann.az/en/?p=70943.

[50] "Azərbaycan Müdafiə Nazirliyi "Yeni Müsavat" qəzetini məhkəməyə verir," APA Economics, September 16, 2011, http://az.apa.az/news.php?id=234649 [in Azerbaijani].

[51] Fatima Karimli, "AXCP hakimiyyəti kibercinayətdə suçladı" [Front Party cybercrime], Qafqazinfo, June 22, 2011, http://qafqazinfo.az/AXCP_HAKIMIYY%C6%8FTI_KIBERCINAY%C6%8FTD%C6%8F_SU%C3%87LADI-923-xeber.html.

with hackers targeting and defacing sites belonging to the Interior Ministry, State Security Service, Ministry of Education, and ruling New Azerbaijan party, among others.[52]

[52] Institute for Reporters' Freedom and Safety (IRFS), "Chapter Four: Freedom of Expression Online," *Azerbaijan's Critical Voices in Danger – Semi-annual Azerbaijan freedom of expression report, January 01-July 01, 2012*, http://www.ifex.org/azerbaijan/2012/08/16/irfs_freedom_of_expression_report.pdf.

BAHRAIN

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	11	12
Limits on Content (0-35)	22	25
Violations of User Rights (0-40)	29	34
Total (0-100)	**62**	**71**

* 0=most free, 100=least free

POPULATION: 1.3 million
INTERNET PENETRATION 2011: 77 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Bahrain has been connected to the internet since 1995 and currently has one of the highest internet penetration rates in the Middle East. However, as more people have gained access to new technologies, the government has increasingly attempted to curtail their use for obtaining and disseminating politically sensitive information. In 1997, an internet user was arrested for the first time for sending information to an opposition group outside the country,[1] and over the last three years, more internet users have been arrested for online activity.[2]

On February 14, 2011, Bahrainis joined the wave of revolutions sweeping across the Middle East and North Africa, taking to the streets in Manama to call for greater political freedom and protest against the monarchy of King Hamad bin Isa al-Khalifa. Similar to the other Arab Spring countries, online activism played a vital role in Bahrain's demonstrations. In response, the National Safety Status (emergency law) was initiated in March 2011 for two and a half months, leading to an intensive punitive campaign against bloggers and internet users (among others) that was characterized by mass arrests, incommunicado detention, torture, military trials, harsh imprisonment sentences, and dismissal from work and study

[1] Initiative For an Open Arab Internet, "Bahrain," *Implacable Adversaries: Arab Governments and the Internet*, December 2006, http://old.openarab.net/en/node/350.
[2] Freedom House, "Bahrain," Freedom on the Net 2011, April 2011, http://bahrainrights.hopto.org/BCHR/wp-content/uploads/2011/04/Bahrain2011.pdf.

based on online posts or mobile content. An online activist died in custody under torture in April 2011.[3]

Censorship of online media is implemented under the 2002 Press Law and was extended to mobile telephones in 2010.[4] The use of BlackBerry services to disseminate news is banned. In 2002, the Ministry of Information made its first official attempt to block websites containing content critical of the government, and today over 1,000 websites are blocked, including individual pages on certain social-networking sites.[5] Surveillance of online activity and phone calls is widely practiced, and officers at road security checkpoints actively search mobile content.[6]

OBSTACLES TO ACCESS

According to the United Nations' e-Government Readiness report of 2010, Bahrain ranks first on the telecommunications infrastructure index in the Middle East,[7] and the number of internet users has risen rapidly, from a penetration rate of 28 percent in 2006 to 77 percent in 2011.[8] In 2011, there were approximately 290,000 internet subscriptions, of which 19 percent were ADSL, 37 percent were wireless, and 44 percent were mobile broadband.[9] Dial-up connections are almost non-existent, and ADSL use has declined with the increased use of wireless internet. Broadband prices have fallen by nearly 40 percent between 2010 and 2011, but it remains significantly more expensive than the average among countries in the Organization for Economic Cooperation and Development (OECD),[10] and restrictions on speeds and download limits still exist. Nevertheless, internet access is widely available at schools, universities, shopping malls and coffee shops, where Bahrainis often gather for work and study.

3 "Journalists Killed in Bahrain," Committee to Protect Journalists, April 9, 2011, http://cpj.org/killed/2011/zakariya-rashid-hassan-al-ashiri.php.

4 Habib Toumi, "Bahrain imposes blackout on BlackBerry news sharing," habibtoumi.com (blog), April 8, 2010, http://www.habibtoumi.com/2010/04/08/bahrain-imposes-blackout-on-blackberry-news-sharing/.

5 "Bahrain: Government orders over 1,000 websites blocked," Index on Censorship, September 25, 2009, http://www.indexoncensorship.org/2009/09/bahrain-government-orders-over-1000-websites-blocked/.

6 "Political media in Bahrain: From the murals and publications to the online forums" [in Arabic], Bahrain Mirror, January 7, 2012, http://bhmirror.hopto.org/article.php?id=2712&cid=117.

7 The index is a measure of the population's connectivity in fixed telephony, mobile, internet, online, personal computing and television. "Bahrain scores the first position in the telecommunications infrastructure," AmeInfo.com, January 14, 2010, http://www.ameinfo.com/221108.html.

8 International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

9 Telecommunications Regulatory Authority (TRA), *Telecommunications Market Indicators in the Kingdom of Bahrain* (Manama: TRA, January 2012), slide 35, http://tra.org.bh/en/pdf/2011TelecommunicationsMarketsIndicators-ForPublic.pdf.

10 Telecommunications Regulatory Authority (TRA), "Broadband Prices fall by up to 40% while Mobile Prices fall by up to 25%," press release, September 14, 2011, http://www.tra.org.bh/en/pdf/2011PriceBenchmarkingPressRelease_en.pdf.

Bahrain has one of the highest mobile phone penetration rates in the region, with nearly 1.7 million mobile subscribers and a mobile penetration rate of 128 percent in 2011.[11] The latest generation of mobile phones such as Apple's iPhone is widely available in the country, but they are still very expensive. Although BlackBerry phones are popular among young people and the business community, in April 2010 the authorities banned BlackBerry users from sending news bulletins through text messages, threatening those who violated the ban with legal action.[12]

Following the February 14, 2011 protests, the government intensified censorship and surveillance of advanced Web 2.0 applications and blocked interactive exchanges online, particularly when its political agenda was not supported. Internet connections became very slow, making it difficult to upload media, and some locations were entirely offline. Internet traffic into and out of Bahrain dropped by 20 percent during the protests,[13] which could have been a result of intentional governmental throttling or a side effect of surveillance-related tinkering with the network.[14] Furthermore, phone lines were disrupted in many areas amid attacks on protesters on March 15 and 16, 2011.[15]

Access to the video-sharing site YouTube, social-networking site Facebook, and the micro-blogging site Twitter is available, although individual pages on each of those platforms are often blocked. Meanwhile, the most prominent online forum Bahrainonline.org has been blocked since its launch in 1998. The Arabic regional portal and blog-hosting service Al-Bawaba has also been blocked since 2006, and online newspapers have been banned from the use of video and audio reports on their websites since a 2010 order by the Information Affairs Authority (IAA), the government body that replaced the Ministry of Information in 2010 and oversees both traditional and online media outlets in Bahrain.[16] The ban applies to all online newspapers except the state-owned Bna.bh, which publishes video reports taken from state television.

[11] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#. Official statistics vary slightly, which cite a mobile phone penetration rate of 133 percent: TRA, *Telecommunications Market Indicators in the Kingdom of Bahrain*, January 2012, slide 8, http://tra.org.bh/en/pdf/2011TelecommunicationsMarketsIndicators-ForPublic.pdf.

[12] "Authorities Ban Blackberry Users from Sending News Bulletins," IFEX, April 15, 2010, http://ifex.org/bahrain/2010/04/15/blackberry_ban/.

[13] Dan Goodin, "Internet use disrupted in Bahrain as protests turn bloody," The Register, February 18, 2011, http://www.theregister.co.uk/2011/02/18/bahrain_internet_disruption/.

[14] Andrew McLaughlin, "Assessing Egypt's Echoes: How to Check For Yourself What's Happening With the Internet in Another Country," Andrew.McLaughl.in (blog), February 16, 2011, http://andrew.mclaughl.in/blog/2011/2/16/assessing-egypts-echoes-how-to-check-for-yourself-whats-happ.html.

[15] Bader Kamal, Twitter post, March 15, 2011, 9:19pm, http://twitter.com/baderkamal/status/47889717043273728; and Bader Kamal, Twitter post, March 15, 2011, 8:45pm, http://twitter.com/baderkamal/status/47881227499356160.

[16] "Ban on audio programs on daily newspaper Al-Wasat's website," Bahrain Center for Human Rights, September 9, 2010, http://www.bahrainrights.org/en/node/3327.

Since February 2011, most live broadcasting websites[17] that were popular among protesters have been blocked.[18] PalTalk, a chatting service that was used to conduct political seminars with prominent guests and mass online audiences, has been blocked since June 2011,[19] while many blogs critical of government views were also blocked in 2011, particularly those that documented the protests and government crackdown (see "Limits on Content").

Despite the obstacles to access, Bahrain's online community has grown rapidly in recent years, especially in social media. By the end of 2011, the number of Bahraini users on Facebook reached 315,000 with a penetration of 45 percent,[20] and there are more than 3,500 local entities (both government and civil society) with a Facebook page.[21] Around 62,000 Bahraini users were active on Twitter as of March 2011.[22] The word "Bahrain" was among the top hashtags used on Twitter in the Arab region,[23] and an Al Jazeera monitoring tool found Bahrain to be the most active on Twitter compared to other countries in the region during the Arab Spring events.[24]

There are 13 internet service providers (ISPs) serving Bahraini users, but the major providers are Batelco, Zain, MENA Telecom, and VIVA. The last two provide the increasingly popular WiMAX technology. According to Bahrain's Telecommunications Regulatory Authority (TRA), some 31 ISP licenses have been granted for internet services, but only 13 providers are in business, and only two of them are licensed to provide wireless internet.[25] Three of the major ISPs—Batelco, Zain, and VIVA—are also the only mobile operators in Bahrain. The largest telecom company and ISP in Bahrain, Batelco, has a majority of its shares owned by the government, while the other ISPs are owned by investors from the private sector, including non-Bahraini investors. There is no centralized

[17] These sites include bambuser.com, ustream.tv, justin.tv, and other websites that stream directly to Twitter like twitcasting.tv and twitcam.livestream.com. See, "Attacks on media continue across Middle East," Committee to Protect Journalists, February 16, 2011, http://cpj.org/2011/02/attacks-on-media-continue-across-middle-east.php.

[18] "Despotic regimes continue to obstruct coverage of revolutions," Reporters Without Borders, September 1, 2011, http://en.rsf.org/bahrain-despotic-regimes-continue-to-01-09-2011,40886.html.

[19] "Crackdown continues in Bahrain, Bloggers go on trial in Emirates," Reporters Without Borders, June 16, 2011.

[20] "Bahrain Facebook Statistics," Socialbakers, accessed July 16, 2012, http://www.socialbakers.com/facebook-statistics/bahrain.

[21] "To prevent its use in the buildup to the issues related to public affairs, Bahrain is considering the legalization of the use of Facebook similar to Arab countries" [in Arabic], Alwasat News, February 4, 2011, http://www.alwasatnews.com/3073/news/read/525216/1.html.

[22] Dubai School of Government, "Mapping Twitter: Twitter Users," Arab Social Media Report, Issue 2, May 2011, http://www.dsg.ae/en/ASMR2/twitterusers.aspx.

[23] Dubai School of Government, "Mapping Twitter," Arab Social Media Report, Issue 2, May 2011, http://www.dsg.ae/en/ASMR2/maptwitter.aspx.

[24] Bilal Randeree, "Twitter Dashboard," Al Jazeera, March 30, 2011, http://www.aljazeera.com/indepth/interactive/2011/03/20113108250282747.html/.

[25] TRA, "Market Information: Number of Licenses Issued," accessed February 1, 2012, http://www.tra.org.bh/en/marketstatistics.asp.

backbone to control the internet in Bahrain, but all ISPs are indirectly controlled by the government through orders from the TRA.

There have been no reported instances of ISPs being denied registration permits. However, on March 21, 2011, the TRA revoked all licenses of 2Connect Company[26] (a telecom provider and ISP) without providing a clear reason, though one of the shareholders of the company was a prominent opposition leader who was arrested a few days earlier on March 17.[27] All clients were given seven days to move to another service provider, but some Bahraini banks using 2Connect services for certain transaction platforms had difficulty switching these core systems to other providers on the very short notice.[28] Without much explanation, the TRA withdrew its decision on April 13, 2011 and allowed 2Connect to resume operations.[29]

Mobile phone services and ISPs are regulated by the TRA under the 2002 Telecommunications Law. Although the TRA is an independent organization on paper, its members are appointed by the government, and its chairman reports to the Minister of State for Cabinet Affairs responsible for telecommunications, Sheikh Ahmed bin Attiyatallah al-Khalifa, who is also a member of the ruling family. The TRA has issued several regulations that have not been welcomed by consumers, including measures that violate individual privacy rights (see "Violations on User Rights").[30]

LIMITS ON CONTENT

According to some estimates, the IAA has blocked and shut down more than 1,000 websites, including human rights websites, blogs, online forums,[31] and individual pages from social media networks, focusing on sites that are critical of the Bahraini government, parliament, and ruling family. In 2011, YouTube pages containing videos of torture testimonies[32] or police attacks against civilians were blocked,[33] as were other webpages

[26] "ANHRI: Bahrain to revoke licenses of 2Connect internet services company owner arrested over participating in peaceful protests," Bahrain Center for Human Rights, March 27, 2011, http://bahrainrights.hopto.org/en/node/3869.
[27] "ANHRI condemns blocking Al-Quds Al-Arabi newpaper website," Bahrain Center for Human Rights, May 24, 2011, http://bahrainrights.hopto.org/en/node/4126.
[28] Mark Sutton, "Bahrain TRA shuts down ISP 2Connect," ITP.net, March 23, 2011, http://www.itp.net/584255-bahrain-tra-shuts-down-isp-2connect.
[29] "2Connect set to resume operations," Gulf Daily news, April 13, 2011, http://m2m.tmcnet.com/news/2011/04/13/5441914.htm.
[30] Geoffrey Bew, "'Big Brother' Move Rapped," Gulf Daily News, March 25, 2009, http://www.gulf-daily-news.com/Print.aspx?storyid=246587.
[31] Reporters Without Borders, "Countries Under Surveillance: Bahrain," 2011, accessed July 16, 2012, http://en.rsf.org/surveillance-bahrain,39748.html.
[32] "Blocking the Documentary 'Systematic Torture in Bahrain' on YouTube," Bahrain Center for Human Rights, February 8, 2011, http://bahrainrights.hopto.org/en/node/3710.

chronicling the government's brutal crackdown. The IAA can order the blocking of a website without referring the case to a court. It has instructed all ISPs to "prohibit any means that allow access to sites blocked by the ministry,"[34] and the license of any operator that violates the decree will be revoked.

The filtering of websites in Bahrain is based on keyword density, the manual entry of URLs, and certain website categories, including potential circumvention tools like Google Translate and Google cached pages. The government regularly updates the list of websites to block, which is sent to ISPs.[35] Batelco, Bahrain's main ISP, filters the web using McAfee SmartFilter software and Blue Coat technology. In March 2011, plans were announced to switch to technology from Palo Alto Networks that can block activities within websites, such as video or photo uploading, and make it more difficult for users to circumvent censorship.[36]

Website administrators face the same libel laws that apply to print journalists and are held jointly responsible for all content posted on their sites or chat rooms. Following the March 2011 crackdown, moderators of online forums and administrators of Facebook pages that organized and shared news of the protests were specifically targeted.[37] Many forums were shut down under pressure from security officers,[38] resulting in the loss of a large amount of information on Bahrain's history and heritage that had been documented by online users and made available only through the local forums and websites.[39] Documentation of daily news and events on the forums also became inaccessible, and most of the sites remain closed as of April 2012.[40]

---

[33] Jillian York, "Bahrain Blocks YouTube Pages and More," Global Voices, February 14, 2011, http://advocacy.globalvoicesonline.org/2011/02/14/bahrain-blocks-youtube-pages-and-more/.

[34] Reporters Without Borders, "Authorities Step Up Offensive Against Journalists and Websites," news release, May 14, 2009, http://en.rsf.org/spip.php?page=article&id_article=33042.

[35] Ibid.

[36] Paul Sonne and Steve Stecklow, "U.S. Products Help Block Mideast Web," Wall Street Journal, March 27, 2011, http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html.

[37] Non exhaustive list of forum moderators who were subject to arrest found at: https://spreadsheets.google.com/pub?hl=en&hl=en&key=0ApabTTYHrcWDdEk0Q0pWYnlSa3JmbS1RbThtUkZrNkE&output=html; accessed via: "Bahrain: After destruction of the actual protesting site at "the Pearl," the government shifts to eliminate virtual protests," Bahrain Center for Human Rights, May 17, 2011, http://bahrainrights.hopto.org/en/node/4101.

[38] Moderator of the AlDair Forum talks about his detention, saying he was forced to show the interrogation officer how to close the website: "Ahmed al-Dairi Moderator of AlDair Forums in the first episode of his testimony: thus eased voice of Zakaria AlAsheeri forever" [in Arabic], Bahrain Mirror, January 4, 2012, http://bhmirror.no-ip.org/article.php?id=2678&cid=117.

[39] An example of a local website with information on Bahrain's history and heritage is the internet forum: http://aldair.net. It used to have a section called, "Know your village and your country," in which people would detail the history of their village, and provide information that is not taught in schoolbooks, including the origin of the village's name, the history of its economy, the dialect of Arabic spoken there, and its folk traditions.

[40] On this list of closed sites prepared on May 2011, which were tested again on April 2012, only two were working: https://spreadsheets.google.com/spreadsheet/pub?hl=en&hl=en&key=0ApabTTYHrcWDdEN2bkhXUGh6TUNaNEN4Y280Ty11bFE&output=html.

The authorities use various methods to force removal of unwanted content. For example, in February 2011 a non-Bahraini resident who was active in taking and uploading videos of the crackdown on protesters and whose YouTube videos became viral on the BBC and other news channels, was tracked by security agents who came to his apartment and forced him to delete all the videos on his computer, camcorder, and YouTube channel.[41] In other cases, YouTube administrators removed some videos of the crackdown on the basis of third-party notifications of copyright infringement, even though the videos were shot by civilian journalists. The Facebook and Twitter pages of *Rasad News*, a major source of news about human rights violations in Bahrain, were overtaken by regime agents who began posting anti-protest and pro-regime content after the arrest of one of the page's administrators in June 2011.[42]

Censorship of websites became increasingly prolific in Bahrain in 2011,[43] with the Facebook page that had called for protests on February 14, 2011 the first to be blocked.[44] Mainstream media outlets reporting on Bahrain were also targeted with censorship online. For example, the website of the local independent *Al-Wasat* newspaper was blocked for 24 hours in April 2011 after being accused of spreading falsehoods that distorted the reputation of the kingdom outside of Bahrain.[45] The website of the London-based *Al-Qudus Al-Arabi* newspaper was blocked in May 2011 after its editor criticized Saudi Arabia for sending troops to suppress the peaceful demonstrations in Bahrain.[46] Media outlets such as the Al-Alam TV channel,[47] PressTv,[48] and Lualua TV[49] that reported on the unrest also had their websites blocked during the year. The anti-government news site Bahrainmirror.com, which is published from abroad, was blocked in June 2011.[50]

[41] Tony Mitchell, "Part 2: Return to Pearl Roundabout," Bahrain Uprising (blog), December 8, 2011, http://tonydmitchell.wordpress.com/2011/12/08/bahrain-uprising-part-2-return-to-pearl-roundabout/. His YouTube channel is: http://www.youtube.com/user/ElliottsFather?blend=1&ob=0.

[42] "Crackdown continues in Bahrain, Bloggers go on trial in Emirates," Reporters Without Borders, June 16, 2011, http://en.rsf.org/bahrain-crackdown-continues-in-bahrain-16-06-2011,40467.html.

[43] "Bahrain: ARTICLE 19's Submission to the UN Universal Periodic Review," Article 19, November 22, 2011, http://www.article19.org/resources.php/resource/2861/en/bahrain:-article-19%E2%80%99s-submission-to-the-un-universal-periodic-review.

[44] "In Fear of Transmitting the Tunisian and Egyptian Demonstrations to Bahrain: Blocking a Facebook Group that Calls People to go Down the Streets and Demonstrate against the Authority's Policy," Bahrain Center for Human Rights, February 6, 2011, http://bahrainrights.hopto.org/en/node/3721.

[45] "Al-Wasat closed down, its senior journalists forced to resign," Reporters Without Borders, April 3, 2011, http://en.rsf.org/+al-wasat-closed-down-its-senior+.html.

[46] "Bahrain: 'Internet' the biggest victim of the war launched by the authorities on the general freedom ANHRI condemns blocking Al-Quds Al-Arabi newspaper website following its publishing of an editorial article criticizing the Saudi intervention in Bahrain," The Arabic Network for Human Rights Information, May 24, 2011, http://www.anhri.net/en/?p=2544.

[47] "Channel block site of the world in Bahrain" [in Arabic], Islam Times, March 8, 2011, http://www.islamtimes.org/vdcfcmdt.w6dcxaikiw.html.

[48] "Press TV's website blocked in Bahrain," PressTV, March 5, 0211, http://www.presstv.ir/detail/168269.html.

[49] LualuaTV also had its satellite broadcast jammed in Bahrain. Source: Simon Atkinson, "Bahrain TV station struggles as signal blocked," BBC News, November 14, 2011, http://www.bbc.co.uk/news/business-15699332.

[50] "Crackdown continues in Bahrain, Bloggers go on trial in Emirates," Reporters Without Borders, June 16, 2011, http://en.rsf.org/bahrain-crackdown-continues-in-bahrain-16-06-2011,40467.html.

In April 2011, the government of Bahrain censored one of its own websites belonging to the Jaffaria Waqf Directorate (www.jwd.gov.bh) to prevent public access to documents of registered mosques after the authorities had demolished a number of mosques amid the crackdowns against protestors.[51] The website gave an official block message even when accessed via a proxy or from outside Bahrain,[52] but the site was still accessible through its internet protocol (IP) address. The authorities removed the block when activists published mirrored content on a different site.[53]

The IAA officially blocks websites containing pornography or material that may provoke violence or religious hatred.[54] In practice, however, many websites run by national or international NGOs are inaccessible. For example, the websites of the Arab Network for Human Rights Information (ANHRI) and the Bahrain Center for Human Rights (BCHR) have been blocked since 2006. The websites of several political societies—including the Alwefaq Islamic Society, National Democratic Action Society, and Islamic Action Society—were blocked in September 2010 in the lead-up to the parliamentary elections and following the Alwefaq Islamic Society's plans to launch an audio-visual service online. The authorities claimed that the societies' publications, both print and online, were "misleading public opinion."[55] The websites were all unblocked in January 2012,[56] though the website of the opposition Bahrain Justice and Development Movement, which was established abroad and blocked a few weeks after its launch in August 2011, remains blocked as of May 2012.[57]

Blocking decisions and policies are not transparent. The official block page states, "This web site has been blocked for violating regulations and laws of Kingdom of Bahrain," but it does not specify which laws. Webmasters do not receive notifications that their sites have been banned or why they have been banned. Although the law does technically allow affected individuals to appeal a block within 15 days, no such case has yet been adjudicated. For

[51] The authorities claimed that the mosques were not licensed. Source: "Bahrain targets Shia religious sites," Al Jazeera, May 14, 2011, http://www.aljazeera.com/video/middleeast/2011/05/201151311201638934 8.html; See also, Rebekah Heacock, "Threats to the OpenNet: May 6, 2011," OpenNet Initative, May 6, 2011, http://opennet.net/blog/2011/05/threats-opennet-may-6-2011.

[52] Example of a site block message posted on the forum: http://bahrainonline.allowed.org/showthread.php?t=268335.

[53] The mirror site (http://jwd.homeip.net) is not working anymore. http://www.facebook.com/permalink.php?story_fbid=219273471418496&id=194843270559295.

[54] Frederik Richter, "Bahrain Web Crackdown Triggers Calls for Reform," Reuters, February 9, 2009, http://www.reuters.com/article/idUSTRE5183Y320090209.

[55] "Crackdown against Civil Rights and Free Expression Results in the blockage of the Website of the Largest Political Society," Bahrain Center for Human Rights, September 18, 2010, http://bahrainrights.hopto.org/en/node/3366; "Bahrain: public freedom in a dark tunnel," Bahrain Center for Human Rights, September 22, 2010, http://bahrainrights.hopto.org/en/node/3416.

[56] "Director of Press and Publications: Open blocked websites for political societies and the development of media legislation" [in Arabic], Alwasat News, January 2, 2012, http://www.alwasatnews.com/3404/news/read/619277/1.html.

[57] "Violence, blocked websites and prosecutions – Anti-media offensive continues," Reporters Without Borders, August 20, 2011, http://en.rsf.org/bahrain-violence-blocked-websites-and-20-08-2011,40811.html.

example, the Democratic National Work Society filed a case in January 2009 to appeal the blocking of its website, but its case has still not been adjudicated as of May 2012.

The use of proxy services, dynamic IP addresses, and virtual private network (VPN) applications allow users in Bahrain to access blocked websites, although many less savvy users are not as successful. In fact, the government regularly blocks access to proxy sites and tools that enable circumvention of online filters and censors, including applications that allow browsing of other websites, such as Google Translate, Google cached pages, and online mobile emulators, requiring users to be consistently creative and adaptable.

The government has also employed social networks for its own purposes. Since February 2011, an "army of trolls" has been active[58] with hundreds of highly organized accounts suddenly emerging on Twitter and working to cajole, harass, and intimidate online activists[59] as well as commentators and journalists who write about the protests,[60] including *New York Times* journalist, Nicholas Kristof ("@nickkristof").[61] For some, the Bahraini trolling efforts have been effective, at the very least in silencing opposition voices inside Bahrain[62] and abroad,[63] or in reducing their activity. The trolls have also played a vital role in spreading information that is controversial, offensive, or just plain false[64] to distort the image of the protesters, spread hate and conflict, and break confidence in the credibility of information on social networks.[65] They have organized mass email campaigns to defame activists, as seen in May 2011 when the Oslo Freedom Forum's email account was bombarded with messages defaming activist Maryam al-Khawaja, a speaker at the forum.[66]

[58] "Bahrain's Troll Army," Web 3.0 Lab (blog), February 17, 2011, http://web3lab.blogspot.com/2011/02/bahrains-troll-army.html.
[59] Brian Dooley, "'Troll' Attacks on #Bahrain Tweets Show Depth of Government Attempts to Silence Dissent," Huffington Post (blog), November 17, 2011, http://www.huffingtonpost.com/brian-dooley/troll-attacks-on-bahrain_b_1099642.html.
[60] J. David Goodman, "'Twitter Trolls' Haunt Discussions of Bahrain Online," The Lede (blog), *New York Times*, October 11, 2011, http://thelede.blogs.nytimes.com/2011/10/11/twitter-trolls-haunt-discussions-of-bahrain-online/.
[61] Solana Larsen, "Bahrain: #NickKristof Bullied on Twitter," Global Voices, February 19, 2011, http://globalvoicesonline.org/2011/02/19/bahrain-nickkristof-bullied-on-twitter/.
[62] iManamaa, Twitter post, May 13, 2011, 7:39am, http://twitter.com/imanamaa/status/69049206215684097; Sultan Al-Qassemi, "Pioneer Bloggers in the Gulf Arab States," Jadaliyya, December 20, 2011, http://www.jadaliyya.com/pages/index/3643/pioneer-bloggers-in-the-gulf-arab-states; "Disturbing Drop in Tweeting in Bahrain," Web 3.0 Lab (blog), March 22, 2011, http://web3lab.blogspot.com/2011/03/disturbing-drop-in-tweeting-in-bahrain.html.
[63] Jillian York, "Twitter Trolling as Propaganda Tactic: Bahrain and Syria," JillianCYork.com (blog), December 10, 2011, http://jilliancyork.com/2011/10/12/twitter-trolling-as-propaganda-tactic-bahrain-and-syria/.
[64] Marc Owen Jones, "So Many Trolls but so Few Leaders: The Information War in Bahrain," MarcOwenJones (blog), March 14, 2011 http://www.marcowenjones.hostbyet2.com/?p=176.
[65] David Wheeler, "In the Arab Spring's Wake, Twitter Trolls and Facebook Spies," The Chronicle of Higher Education, November 29, 2011, http://chronicle.com/blogs/planet/2011/11/29/in-the-arab-springs-wake-twitter-trolls-and-facebook-spies/.
[66] Thor Halvorssen, "PR Mercenaries, Their Dictator Masters, and the Human Rights Stain," Huffingtonpost.com (blog), May 19, 2011, http://www.huffingtonpost.com/thor-halvorssen/pr-mercenaries-their-dict_b_863716.html.

These troll accounts have a handful of followers (or sometimes none at all) and seem to belong to a well-organized system as they all appear and disappear around same time.

Heavy tweeting activity originating from the vicinity of the Ministry of the Interior in Manama was recorded right before the February 17, 2011 crackdown on protesters.[67] In addition, hoax journalists[68] linked to public relations (PR) agencies working for the government were writing on Twitter and blogs like BahrainViews and Bahrain Independent[69] to spread lies and sectarian propaganda.[70] Multiple Wikipedia entries linked to Bahrain were changed in favor of the government,[71] which may have been linked to another PR agency.[72] At least one agency working for the government was contracted to provide "web optimization & blogging" to Bahrain,[73] while other PR agencies known for online reputation management created fake blogs and websites.[74] Meanwhile, the government created new units within the IAA in May 2011 to monitor the output of foreign news webpages and social media sites such as Facebook and Twitter. According to the IAA's director of publishing, the initiative aims to "further help project the kingdom's achievements and respond to false information that some channels broadcast."[75]

Given severe restrictions on freedom of expression, Bahrainis have used the internet to debate sensitive issues and to exchange content that is not available in the traditional media. For example, Bahrain's February 14th demonstration first took shape in January 2011 on the popular site Bahrainonline.org that received over 100,000 visits, and then spread to social networks such as Facebook and Twitter. The demonstration later turned into a resilient social protest movement titled the "Coalition of February 14 Youth" that continued to rely on online supporters to generate ideas for dissent or particular kinds of activism in various digital forums.[76]

---

[67] "Continued high tweeting in this part of Bahrain, by why?" Web 3.0 Lab (blog), March 22, 2011, http://web3lab.blogspot.com/2011/03/continued-high-tweeting-in-this-part-of.html.

[68] Marc Owen Jones, "Hoax Journalist Liliane Khalil Returns, This Time as Habiba Dalal," MarcOwenJones, (blog), January 29, 2012, http://marcowenjones.wordpress.com/2012/01/29/the-return-of-liliane-khalil/.

[69] Marc Owen Jones, "Busted! Journalist Liliane Khalil Exposed," MarcOwenJones, (blog), August 2, 2011 http://www.marcowenjones.hostbyet2.com/?p=364.

[70] DR Majeed AL Alawi, Twitter post, January 2, 2012, 2:51am, https://twitter.com/#!/DrMajeedAlalawi/status/153790396231716865.

[71] Marc Owen Jones, "Truth Massages & the Intelligence Unknown," MarcOwenJones, (blog), December 7, 2011 http://www.marcowenjones.hostbyet2.com/?p=401.

[72] Ibid.

[73] "Trippi & Associates Manipulate Internet Content on Behalf of Bahrain Government," Bahrain Freedom Index (blog), July 20, 2011, http://bahrainindex.tumblr.com/post/15188201300/trippi-associates-manipulate-internet-content-on.

[74] Marcus Baram, "Lobbyists Jump Ship in Wake of Mideast Unrest," Huffington Post, March 25, 2011, http://www.huffingtonpost.com/2011/03/24/lobbyist-mideast-unrest-departures_n_840231.html; Marc Owen Jones, "Truth Massages & the Intelligence Unknown," MarcOwenJones, (blog), December 7, 2011.

[75] Andy Sambridge, "Bahrain sets up new units to monitor media output," Arabian Business, May 18, 2011, http://www.arabianbusiness.com/bahrain-sets-up-new-units-monitor-media-output-400867.html?parentID=401071.

[76] Toby Jones, Ala'a Shehabi, "Bahrain's revolutionaries," The Middle East Channel, ForeignPolicy.com (blog), January 2, 2012, http://mideast.foreignpolicy.com/posts/2012/01/02/bahrains_revolutionaries.

The role of online activism proved essential during the protests and even more after the March 2011 crackdown as activists used social media to report the events in real-time. By uploading images to YouTube or yFrog and then sharing them on Facebook and Twitter, protesters upstaged government news accounts and drew worldwide attention to their demands.[77] The internet became their only channel for expression and information as the official media censored anti-government views and tried to distort the protest's image, while international mainstream media outlets were either ignoring Bahrain or unable to get access. Google maps were used to document demolished mosques,[78] new blogs emerged to document daily events,[79] and an online crowdsourcing database was created to document arrests.[80]

Since April 2011, numerous e-protests have been organized online whereby users agree on an issue, possible target organization, and time, and subsequently disseminate protest details through Facebook and Twitter.[81] For example, on May 23, 2011, three days before a session on Bahrain in the European Union (EU) Parliament, an e-protest targeted members of the parliament with emails describing the demands of Bahraini protesters and the violations committed by the government against them.[82] In response, the EU Parliament posted a statement on its Facebook page recognizing its support for the e-protest and Bahraini activists.[83] In another example of successful mobilization, Bahraini users along with global supporters sparked a worldwide Twitter trend through the "#Hungry4BH" hashtag to show solidarity with the Bahraini detainees who were on hunger strike in February 2012.[84]

Despite numerous examples of online activism, the government crackdown in March 2011 led many regular internet users to exercise a higher degree of self-censorship, particularly after investigations of online posts were launched at work places and universities and after hundreds of user photos were published on pro-government online forums, Facebook pages,

[77] Jennifer Preston, "Cellphones Become the World's Eyes and Ears on Protests," *New York Times*, February 18, 2011, http://www.nytimes.com/2011/02/19/world/middleeast/19video.html?_r=2.
[78] "Demolished mosques in Bahrain," Google Maps, created on April 21, 2011, http://maps.google.com/maps/ms?ie=UTF8&t=h&oe=UTF8&hl=en&msa=0&msid=201183833019020787911.0004a17a0fd2cb6e24158.
[79] For example, the blog: http://feb14bh.com/.
[80] For example: http://bahrainlog.com/.
[81] Facebook page: https://www.facebook.com/Bahrain.eProtest
[82] "Bahrain's eProtest," Facebook page, accessed July 16, 2012, https://www.facebook.com/photo.php?pid=1001983&l=0e171b81ff&id=215921678418062.
[83] European Parliament, Facebook note, "Parliament's members condemn death sentences in Bahrain and ask for meeting with Ambassador," May 3, 2011, 10:45am, https://www.facebook.com/notes/european-parliament/parliaments-members-condemn-death-sentences-in-bahrain-and-ask-for-meeting-with-/10150171038217852.
[84] Mona Kareem, "Bahrain: #Hungry4BH Trends Worldwide," Global voices, February 27, 2012 http://globalvoicesonline.org/2012/02/27/bahrain-hungry4bh-trends-worldwide/

and the Twitter feed "@7areghum."[85] There were also calls on Facebook to reveal the names and workplaces of protesters,[86] prompting many users to change their last names on Facebook to "Lulu"[87] or their real names into unrelated pseudonyms, while others closed their accounts altogether.[88] Users also restricted their Facebook privacy settings, removed photos related to the protest—especially photos of the Pearl Roundabout where the first crackdown took place—and "un-liked" the revolution page which at one time had over 80,000 "likes."[89] Many websites with photos of protesters began displaying a message stating that the site was temporarily inaccessible as a way to protect protestors from the name and shame campaigns. Today, the majority of users on Twitter and online forums, and even those who leave comments on online editions of newspapers, still use pseudonyms out of fear of being targeted by the authorities.[90]

VIOLATIONS OF USER RIGHTS

Although freedom of expression is enshrined in the Bahraini constitution, the guarantees are qualified by the phrase "under the rules and conditions laid down by law," many of which essentially negate the guarantees.[91] Similarly, the 2002 Press Law promises free access to information but "without prejudice to the requirements of national security and defending the homeland." Bahraini journalists have argued that these loosely worded clauses allow for arbitrary interpretation.[92] On April 28, 2011, the government acknowledged that it had derogated from several provisions of the International Covenant on Civil and Political Rights (ICCPR) including Article 19, which upholds the right to freedom of expression.[93]

[85] Simeon Kerr, "Manama fights back in cyberspace," Financial Times, May 23, 2011, http://www.ft.com/intl/cms/s/0/7bce94b8-8560-11e0-ae32-00144feabdc0.html#axzz1lLZwkuOF.
[86] Suzi Dixon, "Facebook 'used to hunt down Bahrain dissidents,'" The Telegraph, August 4, 0211, http://www.telegraph.co.uk/expat/expatnews/8681230/Facebook-used-to-hunt-down-Bahrain-dissidents.html; "The Revolution Will Be Put on Trial… Via Social Media," Ta3beer (blog), May 2011, http://ta3beer.blogspot.com/2011/05/revolution-will-be-put-on-trial-via.html.
[87] Named after the now-demolished "Pearl Roundabout," which was the center of the protest.
[88] "Bahrain: After destruction of the actual protesting site at 'the Pearl,' the government shifts to eliminate virtual protests," Bahrain Center for Human Rights, May 17, 2011, http://bahrainrights.hopto.org/en/node/4101.
[89] Simeon Kerr, "Manama fights back in cyberspace," Financial Times, May 23, 2011, http://www.ft.com/intl/cms/s/0/7bce94b8-8560-11e0-ae32-00144feabdc0.html#axzz1lQt8t2ma
[90] Nancy Messieh, "Online anonymity: A gateway to freedom or abuse?" The Next Web, August 14, 2011, http://thenextweb.com/me/2011/08/14/online-anonymity-a-gateway-to-freedom-or-abuse/.
[91] Constitution of the Kingdom of Bahrain, available at http://www.shura.bh/en/InformationCenter/Pages/Documents.aspx.
[92] "Bahrain," in *Media Sustainability Index 2008* (Washington, DC: IREX, 2009), http://irex.org/programs/MSI_MENA/2008/MSIMENA_bahrain.asp.
[93] Tawfeeq Ahmed Almansoor (Bahraini Permanent Representative to the UN), Letter to the UN International Covenant on Civil and Political Rights (ICCPR), April 28, 2011, accessed 19 November 2011, http://treaties.un.org/doc/Publication/CN/2011/CN.430.2011-Eng.pdf.

There is no law that guarantees users' privacy. A proposed cybercrimes law that criminalizes unauthorized access to computer systems is under review at the representative house as of January 2012.[94] Although the Bahraini cyberspace is highly monitored, no action has been taken against dozens of pro-regime users who continue to spread online death threats against activists[95] and "defamation and incitement" messages, despite being documented by the Bahrain Independent Commission of Inquiry appointed by the king in July 2011.[96]

Online media in Bahrain are governed by the Press and Publications Law of 2002, which stipulates prison sentences of up to five years for publishing material that is offensive to Islam or the king, or that is perceived as undermining state security or the monarchy.[97] In addition, the 2002 Telecommunications Law contains penalties for illicit practices including the transmission of messages that are offensive to public policy or morals.[98] Under the penal code, any user who "deliberately disseminates a false statement" that may be damaging to national security or public order can be imprisoned for up to two years,[99] and the government has used this vague phrase to question and prosecute several bloggers and online users. In September 2011, Chief of Public Security Major-General issued a statement declaring that "the mere fact of posting instigative calls" via "social networking and Internet websites inciting people to break the law" constitutes "a penal crime punishable by the law."[100] In October 2011, the IAA announced that it was reviewing media laws to ensure their ability to provide protection from the "destructive use of social media."[101] The review is still outstanding as of May 2012.[102]

After the crackdown on protesters in March 2011, the government began a mass arrest campaign of online activists and bloggers, starting with those who used their real names while covering the protests. More than 20 online activists were arrested by masked security

[94] "External consultation to discuss draft law on cybercrime," Alwasat News [in Arabic], January 29, 2012, http://www.alwasatnews.com/3431/news/read/625198/1.html.
[95] "Bahrain: Death threats against Messrs. Mohammed Al-Maskati, Nabeel Rajab and Yousef Al-Mahafdha," World Organization Against Torture, December 7, 2011, http://www.omct.org/human-rights-defenders/urgent-interventions/bahrain/2011/12/d21549/.
[96] Mahmoud Cherif Bassiouni et al., "Report of the Bahrain Independent Commission of Inquiry," Bahrain Independent Commission of Inquiry (BICI), November 23, 2011, paragraph 1597, http://files.bici.org.bh/BICIreportEN.pdf.
[97] Press and Publications Law of 2002 of the Kingdom of Bahrain (No.47 of 2002). A copy can be found at: http://mahmood.tv/bahrain/bahrain-politics-2/bahrain-politics/press-law-472002-arabic/.
[98] Telecommunications Law of the Kingdom of Bahrain.
[99] Bahrain Penal code, 1976, article 168, http://bahrainrights.hopto.org/BCHR/wp-content/uploads/2010/12/Bahrain-Penal-Code.doc.
[100] "Public Security/Statement," Bahrain News Agency, September 21, 2011, http://www.bna.bh/portal/en/news/473522.
[101] "Bahrain plans for a social media law," Bahrain Freedom Index (blog), October 17, 2011, http://bahrainindex.tumblr.com/post/11616237908/bahrain-plans-for-a-social-media-law.
[102] "Laws on way to curb misuse of social media," Gulf Daily News, June 13, 2012, http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=331984.

men and held for periods ranging from few days to few months.[103] On Facebook and Twitter, pages appeared that called a group of known influential bloggers "traitors" and accused them of conspiring against the government.[104] Subsequently, Mahmood Al Yousif, known as the "godfather" of Bahraini bloggers, Manaf AlMuhandis "Redbelt," the founder of the popular "#UniteBahrain" Twitter campaign, and Mohammed Al-Masqati "emoodz" who was active in covering the uprising, were all arrested during midnight house raids on March 30, 2011. Supporters of the detained bloggers received threats on Twitter that they "will have [their] IP address taken and will get arrested."[105] All three bloggers were released within 24 hours to a week[106] under pressure created by an international media campaign and a statement from the U.S. Department of State.[107] Al-Masqati was released after signing a statement that he would no longer talk or write about Bahrain in any form of media.[108]

Many other arrested bloggers were held incommunicado and blindfolded for weeks without access to family or legal assistance, and some were put on trials that lacked fair trial guarantees[109] at the military court. Two detained bloggers, Abduljalil Alsingace and Ali Abdulemam,[110] who had been pardoned in February 2011 following six months in prison, became targets again three weeks later. Between August 2010 and February 2011, both had been detained, tortured,[111] and put on trial under the Terrorism Law at the criminal court.[112] After their release, their houses were raided again in the early hours of March 17, 2011, but only Alsingace was found and arrested, detained in a military prison, and reportedly tortured.[113] Both were subsequently put on a trial at the military court on charges of being connected to a terrorist organization aiming to overthrow the regime, and on June 22, 2011, Alsingace was sentenced to life in prison while Abdulemam was

[103] List of arrested Bahraini journalists: https://docs.google.com/spreadsheet/ccc?key=0ApabTTYHrcWDdFZocWpBRlp6ell6RkNWeGh5YXAtUFE#gid=0, accessed via bahrainrights.org.
[104] Screenshot of Facebook post, "Bahrain against false media's Photos," posted on March 24, 2011, http://wlcentral.org/sites/default/files/imagepicker/1998/@bloggers-targetd-on-facebook.jpg.
[105] "Bahrain: After destruction of the actual protesting site at 'the Pearl,' the government shifts to eliminate virtual protests," Bahrain Center for Human Rights, May 17, 2011, http://bahrainrights.hopto.org/en/node/4101.
[106] "I'm back!" Mahmood's Den (blog), April 1, 2011, http://mahmood.tv/2011/04/01/im-back/.
[107] "Bahrain releases 'Blogfather' after US criticism," Agence France-Presse, April 1, 2011, http://www.google.com/hostednews/afp/article/ALeqM5iDMfAxtRb_qYjSFj1uRnteiS3XWQ?docId=CNG.1fd1c4853d22c9c6fd2476a783525b0d.d1.
[108] Nancy Messieh, "Online anonymity: A gateway to freedom or abuse?" The Next Web, August 14, 2011, http://thenextweb.com/me/2011/08/14/online-anonymity-a-gateway-to-freedom-or-abuse/.
[109] Mahmoud Cherif Bassiouni et al., BICI Report, paragraph 1702.
[110] Alsingace is a blogger, academic, and leading figure in the Haq opposition group who had used his blocked blog (alsingace.katib.org) to denounce the deplorable state of civil liberties in Bahrain; while Abdulemam is one of Bahrain's internet pioneers, a contributor to the international bloggers network Global Voices, and the founder of the popular forum Bahrainonline.org.
[111] Ali Abdulemam describes the way he was tortured (minute 09:37), "People & Power – Bahrain: Fighting for change," Al Jazeera English, March 9, 2011, http://www.youtube.com/watch?v=IZdyiK-Z5Do.
[112] ""Terrorist Network's First Hearing – Trial Testimonies," Bahrain Center for Human Rights, October 28, 2010, http://www.bahrainrights.org/en/node/3540.
[113] Mahmoud Cherif Bassiouni et al., BICI Report, Annex B, Case #7.

sentenced (in absentia) to 15 years.[114] Abdulemam's whereabouts are unknown, but he is believed to be living in hiding.

In May 2011, several arrested photographers were charged for "broadcasting fake pictures detrimental to the Kingdom over the internet and Facebook," including the head of the Bahrain Society for Photography, who was detained for two months and tortured in an effort to force him to sign pre-written confessions.[115] Their cases were closed on November 2011 under international pressure by media watchdogs.

Throughout 2011, many online activists were summoned for interrogation for their posts and activities on social-networking sites. For example, 15-year old Eman Al-Aswami was detained at the police station for 11 hours and questioned about her participation on certain Facebook pages.[116] Bahrain's most prominent human rights defender, Nabeel Rajab, was summoned several times for questioning about his Tweets,[117] one time by the military prosecutor.[118] In February 2012, after a brief arrest, he was officially charged with calling for protests on Twitter.[119]

Violence against internet users and activists has become an alarming trend in Bahrain over the past year. In one disconcerting incident, online activist and moderator of the AlDair online forum, Zakaryia AlAshiri, was tortured and killed in police custody on April 9, 2011 six days after his arrest. While the authorities alleged at the time that AlAshiri died of illness,[120] the marks on his body showed clear evidence of being subjected to torture. After the publication of the Bahrain Independent Commission of Inquiry report, which confirmed

[114] "Detained blogger Abduljalil Al-Singace on hunger strike," Reporters Without Borders, September 6, 2011, http://en.rsf.org/bahrain-one-blogger-sentenced-to-life-22-06-2011,40507.html.

[115] "Bahrain regime continues to target freedom of expression by taking journalists and photographers to trials that criminalize their exercise of that freedom," Bahrain Center for Human Rights, October 14, 2011, http://www.bahrainrights.org/en/node/4767. Another user was sentenced by the criminal court to one year in prison on charges of "publishing of false information" and was acquitted after ten months detention. See, "Between two years jail and 5 years for 13 defendants with illegal assembly," [in Arabic], Alwasat News, October 26, 2011, http://www.alwasatnews.com/3336/news/read/604401/1.html.

[116] "Bahrain: After destruction of the actual protesting site at "the Pearl," the government shifts to eliminate virtual protests."

[117] "Summon of Nabeel Rajab for his tweets, Return of military trials and other news from Bahrain," Bahrain Center for Human Rights, August 23, 2011, http://www.bahrainrights.org/en/node/4548.

[118] "Front Line: Bahrain: UPDATE - Violence, harassment and intimidation of human rights defenders," Bahrain Center for Human Rights, May 31-June 1, 2011, http://bahrainrights.hopto.org/en/node/4160.

[119] Avinash Kalla , "'They charged me of indicting protests using Twitter' says Nabeel Rajab," wespeaknews.com, February 15, 2012, http://www.wespeaknews.com/world/they-charged-me-of-indicting-protests-using-twitter-says-nabeel-rajab-27080.html.

[120] "Zakariya Rashid Hassan al-Ashiri," Committee to Protect Journalists, April 9, 2011, http://cpj.org/killed/2011/zakariya-rashid-hassan-al-ashiri.php.

AlAshiri's death under torture,[121] the government placed five policemen on a show trial, even though they were previously acquitted by a military court.[122]

Many other online activists have given testimonies of being subjected to torture at detention centers. Ahmed AlDairy, another moderator of the AlDair online forum, was beaten on his face and body for several days and forced to stand facing a wall for long hours while handcuffed and blindfolded. He was also put on display during which an interrogator threatened to cut his off his genitals to force him to confess.[123] In December 2011, Twitter user "@Nezrad," who was arrested for his tweets and detained for 66 days, said he was "shackled, eyes blindfolded, beaten by hoses on butts, kicked and slapped."[124] Also in December, blogger Zainab AlKhawaja—who was famous for her coverage of protests and human rights abuses on Twitter ("@angryarabiya")—was arrested at a protest, hit in the face, dragged by the handcuffs on the ground, and further beaten at a detention center. She was released after four days, but her trial was still ongoing as of May 2012 on charges that include incitement against the regime.[125]

In a case of extra-legal detention, in March 2011, a court of appeal ignored the evidence of the wrongful arrest of Hasan Salman Abu Ali, who was detained in 2009 after being monitored without a judicial order.[126] The court instead confirmed the three-year sentence against him for publishing online the names of employees of the national security apparatus.[127] Despite his eligibility for early release in August 2011, he was held in detention until February 13, 2012.[128]

Between April and June 2011, posts from the Facebook and Twitter accounts of dissident students and employees were presented in interrogation meetings held at workplaces and universities as evidence of anti-government activities and used to justify dismissals and expulsions. Some meetings were shown during live trials on national TV.[129] As a result,

[121] Mahmoud Cherif Bassiouni et al., BICI Report, case no. 24, Paragraph 997.
[122] "Show Trial For The Policemen Accused of Torturing two detainees To Death, including an online journalist," Bahrain Center for Human Rights, January 13, 2012, http://www.bahrainrights.org/en/node/4966.
[123] "Ahmed al-Dairi Moderator of AlDair Forums in the first episode of his testimony: thus eased voice of Zakaria AlAsheeri forever" [in Arabic], Bahrain Mirror, January 4, 2012 http://bhmirror.no-ip.org/article.php?id=2678&cid=117.
[124] Mona Kareem, "Bahrain: Twitter User Jailed for 66 Days for Tweeting," Global Voices, December 5, 2011, http://globalvoicesonline.org/2011/12/05/bahrain-twitter-user-jailed-for-66-days-for-tweeting/.
[125] "More information: Zainab AlKhawaja beaten, dragged and arrested - Now Released," Bahrain Center for Human Rights, December 21, 2011, http://www.bahrainrights.org/en/node/4906.
[126] "Case Regarding Publication of Names of National Security Employees Postponed to May" [in Arabic], *Alwasat,* April 19, 2010, http://www.alwasatnews.com/2782/news/read/404013/1.html.
[127] "Bahrain: Citizen Sentenced to Three Years in Prison," Free Hasan Salman, September 18, 2009, http://freehasan.no-ip.org/?p=310.
[128] "Court fines three journalists," Reporters Without Borders, October 10, 2011, http://en.rsf.org/judicial-nightmare-for-journalists-10-10-2011,41155.html.
[129] "Bahrain: After destruction of the actual protesting site at 'the Pearl,' the government shifts to eliminate virtual protests," Bahrain Center for Human Rights, May 17, 2011, http://bahrainrights.hopto.org/en/node/4101.

many employees at governmental bodies were fired from their jobs, including the Bahrain Formula 1 staff.[130] Hundreds of students were expelled[131] from state universities or had their scholarships revoked for online posts that were considered "slander and incitement against government."[132] The political content of emails was also used to dismiss employees of the Arab Shipbuilding and Repair Yard Company (ASRY) in April 2011.[133]

The TRA requires users to obtain licenses to use WiFi and WiMAX connections,[134] and the government does not allow the sale and use of prepaid mobile phone chips without registration. In July 2011, the TRA issued an emergency order against the mobile service provider VIVA to deactivate all their pre-activated mobile prepaid SIM cards until all users registered.[135] Since March 2009, all telecommunications companies are required by the TRA to keep records of customers' phone calls, emails, and website visits in Bahrain for up to three years; the companies are also obliged to grant security services access to subscriber data.[136] In 2010, those records were used against rights activists such as Abdul Ghani Khanjar, who was tortured for refusing to explain his phone discussions and text messages presented during an interrogation.[137] Khanjar was detained between August 2010 and February 2011 and is today living in hiding with a military sentence of 15 years imprisonment.

During the National Safety Status, citizens were forced to allow security personnel to search mobile phones at checkpoints and give access to email and Facebook accounts in interrogation rooms. The contents of mobile phones and emails were often used as evidence against arrested citizens in court. In one case, an unidentified user was sentenced to three years imprisonment for sending images over email, despite evidence that he had only received the email attachments.[138] In another case, a woman was sentenced to three years for possession of images and text messages on her mobile phone that had called for the fall of

[130] As documented by Nicholas Kristof, blogged at Bahrain Freedom Index, December 11, 2011, http://bahrainindex.tumblr.com/post/14867034407/nicholas-kristof-december-11 and http://bahrainindex.tumblr.com/post/14867122527/nicholas-kristof-december-11-2011-this-woman.
[131] Bedlam Beggar, "In Bahrain you can be penalized for an Anti-government Facebook stats (2)," Mideast Youth (blog), June 13, 2011, http://www.mideastyouth.com/2011/06/13/in-bahrain-you-can-be-penalized-for-an-anti-government-facebook-status-2/.
[132] "Janahi: We have taken action against those involved in the events of the University and the investigation is ongoing" [in Arabic], Alwasat News, March 23, 2011 http://www.alwasatnews.com/3125/news/read/534562/1.html.
[133] Mahmoud Cherif Bassiouni et al., BICI Report, paragraph 1410, http://www.bici.org.bh/BICIreportEN.pdf
[134] Geoffrey Bew, "Technology Bill Rapped," Gulf Daily News, July 20, 2006, http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=149891.
[135] Emergency Order No. 3 of 2011, Telecommunications Regulatory Authority (TRA), July 10, 2011, http://www.tra.org.bh/en/pdf/20110710-Viva-EmergencyOrderNo3of2011.pdf.
[136] Bew, "'Big Brother' Move Rapped."
[137] BBC News, podcast, http://t.co/bvEGFgd8; Vernon Silver and Ben Elgin, "Torture in Bahrain Becomes Routine with Help from Nokia Siemens," Bloomberg News, August 22, 2011.
[138] Mahmoud Cherif Bassiouni et al., BICI Report, case 59, ANNEX B.

the regime.[139] A military man, Sayed Ahmed Al Alawi, was fired from his job and sentenced in the absence of a lawyer to four years for an SMS joke that he had sent over BlackBerry to his friend about the fall of the regime.[140] Another military man, Hussain Ebrahim, was sentenced to three years imprisonment and fired from work for a phone call that he had made to a human rights activist, informing him that the security forces were about to crackdown on protesters.[141]

The country's cybercafes are also subject to increasing surveillance. Oversight of their operations is coordinated by a commission consisting of members from four ministries, which works to ensure strict compliance with rules that prohibit access for minors and require full visibility of computer terminals.[142]

Cyberattacks against opposition pages and other websites are common in Bahrain and have intensified following the protests. Several online forums, websites, and Facebook pages related to the protesters were hacked in 2011.[143] In April 2011, a group calling itself the Delta Hacking Team tried to hack the website of the local *Gulf Daily News* and managed to attack four other publications belonging to same parent group, Al-Hilal.[144] The local online newspaper Manamavoice.com was forcefully stopped for a few months beginning in May 2011 after several hacking attempts.[145] Many of opposition forums, such as Bahraninet.net and Bhnation.net, have disappeared since their hacking.

Cyberattacks have also been launched against websites belonging to the government and its supporters. For example, in February 2011 the Anonymous hacktivist group announced Operation Bahrain ("#opbahrain") in solidarity with the dissidents,[146] launching a cyberattack against the government website Bahrain.bh on the anniversary of the Bahrain revolution on February 14, 2012.[147] The group also hacked government websites during the

[139] Mahmoud Cherif Bassiouni et al., BICI Report, paragraph 1257, a.
[140] "Non-Fiction Turns into Reality in Bahrain (1) – The Joke," In Praise of Arab Capital of Culture 2012, Manama –Bahrain (blog), http://manamacoac.blogspot.com/2011/12/non-fiction-turns-into-reality-in.html; also mentioned in BICI Report, paragraph 1382.
[141] SAIDYOUSIF, Twitter post, February 1, 2012, 7:26am, https://twitter.com/#!/SAIDYOUSIF/status/164731306612232195.
[142] Reporters Without Borders, "Countries Under Surveillance: Bahrain."
[143] As documented on YouTube: "Saudi hacker hacks bhrin.com" [in Arabic], YouTube, March 13, 2011, http://www.youtube.com/watch?v=vYA2Kk4APP4; "Saudi hacker hacks shia-albahrain.com" [in Arabic], YouTube, March 22, 2011, http://www.youtube.com/watch?v=BGARYAZCdtg.
[144] "Hacking bid foiled," Bahrain New Agency, April 7, 2011, http://www.bna.bh/portal/en/news/451978.
[145] "Bahrain: After destruction of the actual protesting site at 'the Pearl,' the government shifts to eliminate virtual protests," Bahrain Center for Human Rights, May 17, 2011, http://bahrainrights.hopto.org/en/node/4101.
[146] "Operation Bahrain (#opbahrain) – Anonymous Press Release!" The Hacker News, February 16, 2011, http://thehackernews.com/2011/02/operation-bahrain-opbahrain-anonymous.html.
[147] Kukil Bora, "Anonymous hacks Bahrain Gov & US Maker of teargas," IBTimes.com, February 14, 2012, http://www.ibtimes.com/articles/298107/20120214/anonymous-takes-down-bahrain-government-web-sites.htm.

Formula 1 race in Bahrain in April 2012. Websites of the Housing Ministry,[148] Health Ministry,[149] and House of Representatives were hacked by unknown groups between March and May 2011, and similar attacks have been launched against the Philippines Embassy in Bahrain. Several pro-government websites were hacked in the second half of the year, including the popular online forum Bahrainforums.org that had been behind the publication of hundreds of protester photos that led to their arrests. It remained closed for several weeks in November 2011.[150]

[148] "Bahrain blames hack attack on Iran," UPI.com, May 1, 2011, http://www.upi.com/Top_News/World-News/2011/05/01/Bahrain-blames-hack-attack-on-Iran/UPI-76351304306654/.
[149] Screenshot of hacked Health Ministry webpage: http://yfrog.com/kirlysj.
[150] As documented on YouTube: "Bahraini user hacks Bahrainforums.com" [in Arabic], YouTube, December 4, 2011, http://www.youtube.com/watch?v=kMr5B_qxMHw.

BELARUS

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	19	16
Limits on Content (0-35)	23	23
Violations of User Rights (0-40)	27	30
Total (0-100)	**69**	**69**

* 0=most free, 100=least free

POPULATION: 9.5 million
INTERNET PENETRATION 2011: 40 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ONLINE USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Belarus, often known as "Europe's last dictatorship," is run by the autocratic regime of President Alexander Lukashenka. There has been no separation of powers in Minsk since 1996, and Belarus regularly falls near the bottom of international rankings of media freedom. The authorities control the absolute majority of traditional mass media, including all broadcast outlets and daily newspapers, and approximately 70 percent of the economy remains in state hands. Due to this centralization, there is a high degree of government involvement in the electronic communications sector.

The BYnet, as Belarus' internet sector is known, experienced a dramatic year in 2011. The country's steady economic development and government's robust investment over the past several years, as well as a relative liberalization during the 2008-10 period of dialogue with the European Union, led to steady growth in internet penetration and usage. Meanwhile, the regime's control over traditional media pushed independent media outlets to be more creative and innovative online, where its websites have multiplied and consistently dominated those of the state in terms of quality and popularity. In 2011, web-based independent media played a much more visible role and attracted a larger audience than ever before. The expansion in internet penetration also led to the strong growth of Belarusians active on social-networking sites.

However, the country's political crisis—which followed a flawed presidential election in December 2010—the resulting economic crisis that spanned 2011, as well as the Arab Spring events, have intensified the government's fear of the internet and its determination to

exert greater control over it. Among the targets of an unprecedented crackdown at the end of 2010 were independent media, especially internet outlets and journalists. This repression of online activists was expanded to include bloggers after social-networking sites were used to organize a series of mass protests in summer 2011.

As a result, President Lukashenka repeatedly called for tighter regulation of the internet, blaming it for the country's unrest while praising China's internet restrictions. In August 2011, for example, Lukashenka stated that access to destructive websites must be blocked[1] and that the internet should be controlled in educational institutions to rule out its use for purposes other than education. In September 2011, Prosecutor General Ryhor Vasilevich called for an international agreement that would introduce internet censorship, suggesting that such an agreement could be drawn up at the level of the United Nations.[2]

During 2011, new amendments stipulating financial penalties for violating an already restrictive internet law were introduced. Independent websites and personal blogs were blacklisted and regularly blocked. Online activists were harassed, threatened, persecuted, arrested and imprisoned. Nevertheless, further legal restrictions and harsh repression have failed to halt the growth and dynamism of the Belarusian internet.

OBSTACLES TO ACCESS

Relatively strong economic growth in Belarus over the last half decade has led to a corresponding growth in internet and mobile phone usage. According to the International Telecommunications Union (ITU), Belarus had an internet penetration rate of 40 percent in 2011, up from 16 percent in 2006.[3] In addition, the country's four mobile phone operators had a combined 10.7 million subscribers, for a total penetration rate of 113 percent in 2011.[4] All four mobile operators offer internet access and approximately 4,100 of the

[1] Dzmitry Ulasaw, "Lukashenka: Students access to destructive websites should be blocked," Belapan, August 29, 2011, http://en.belapan.com/archive/2011/08/30/en_1055.

[2] Vyachaslaw Budkevich, "Prosecutor general calls for international agreement that could introduce Internet censorship," Belapan, September 14, 2011, http://en.belapan.com/archive/2011/09/14/en_14091257.

[3] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#. A more recent study by the international agency "Gemius" in November 2011 suggests that there are four million internet users and a penetration rate of over 50 percent. See, Mikhail Doroshevich, "Internet in Belarus, November 2011," E-Belarus.org, January 4, 2011, http://www.e-belarus.org/news/201201041.html.

[4] Alyaksey Areshka, "Number of mobile subscribers in Belarus reached 10.7 million by January 1, communications ministry says," Belapan, January 6, 2012, http://en.belapan.com/archive/2012/01/06/en_20140106.

country's 14,600 base stations are 3G capable, allowing faster internet and multimedia downloading.[5]

Internet use grew quickly in 2011 because and in spite of an economic and political crisis that followed the flawed December 2010 presidential election. An unprecedented crackdown against civil society, a series of public protests, a decline in citizens' confidence in the state media, and a currency collapse led to an increased demand for alternative sources of information, especially via the internet. At the same time, the economic crisis did not increase internet costs, prompting many to start using the internet as a key source for news, entertainment, and as a tool for social interaction.

Approximately 76 percent of users in Belarus access the internet on a daily basis.[6] The key divide in levels of access is not so as much between rural and urban populations—since some 70 percent of Belarusians live in urban areas—as between the country's capital and regions. Over 38 percent of all internet users live in Minsk and the Minsk region.[7] Another significant determinant of internet use is age: the majority of internet users in Belarus are young people and only 7 percent of users are aged 55 and above.[8] Almost 92 percent of all users regularly access the internet at home, and 31.8 percent do so at work. Internet cafes are the least popular point of access, with just 4.3 percent of users utilizing them frequently.[9]

In November 2011, more than 62 percent of users reported having broadband access, while 8.5 percent reported using dial-up, and 11.3 percent accessed via mobile phone connections. The cost of broadband access via DSL and cable is generally tied to volume, reflecting the pricing structure that Beltelecom—the state-owned telecommunications monopoly—uses when selling bandwidth to downstream internet service providers (ISPs). This makes it somewhat expensive to download large items like music or movies, but for common activities such as email and web browsing, the volume surcharges do not create a barrier for most users. Unlimited internet access service was launched by Beltelecom in 2007. Initially quite expensive, it has become more affordable, and prices in rubles (ranging from US$5-$35 per month, depending on the speed) remained unchanged in 2011, despite high inflation and several currency devaluations.

[5] Ibid.

[6] Ibid; "Цифры ИТ – статистика в Беларуси" [IT figures - statistics for Belarus], IT.tut.by, accessed January 21, 2012, http://it.tut.by/numbers.

[7] Doroshevich, "Internet in Belarus, November 2011."

[8] Mikhail Doroshevich, "Internet in Belarus, November 2011," E-Belarus.org, January 4, 2011, http://www.e-belarus.org/news/201201041.html.

[9] Ibid.

The rapid increase in internet penetration has also resulted in the growth of citizens' activity on social-networking sites. Since November 2010, the number of Facebook users has increased by 2.5 times, reaching over 370,000 accounts by May 2012.[10] As of October 2011, there were 315,000 users in the popular local social network Vceti.by, over 632,000 Belarusian bloggers on LiveJournal, and about 1.2 million Belarusian users of the Russian social network, Odnoklassniki.ru.[11] The Russian VKontakte continues to be the most popular social network service, counting 2.5 million accounts registered in Belarus, and is the third most accessed site in the country.[12] While Belarus has two official languages—Belarusian and Russian—the majority of citizens use Russian in daily life. As a result, most online software is in Russian, although some popular software is also available in Belarusian, often translated by local enthusiasts.

There is no independent regulator overseeing ICTs in Belarus. Rather, the Ministry of Communications and Information Technology handles regulatory functions. In addition, the Presidential Administration's Operational and Analytical Center (OAC) has the authority to oversee ISPs, conduct overseas online surveillance, and manage the country's top-level domain (".by").[13] Created in 2008, it replaced the State Center for Information Security, which was part of the Committee for State Security (KGB). Other key bodies include the State Telecommunications Inspectorate, State Control Committee, and Prosecutor General's Office.

Beltelecom and the National Center for Traffic Exchange, established by the government in 2011, remain the only entities with the right to handle connections with internet providers outside of Belarus. Plans to open up international connections to other operators, including private companies, were put on hold in January 2011 after the Ministry of Communications reported that no bids to compete for licenses were received.[14] Beltelecom also holds a monopoly over fixed-line communications and internet services inside Belarus. In July 2011, the government reiterated that it has no plans to privatize Beltelecom.[15] The Ministry of Communications has issued 180 licenses for secondary ISPs, though only 56 active secondary ISPs currently operate in Belarus. The Beltelecom subsidiary Belpak remains the largest ISP.

[10] "Belarus Facebook Statistics," SocialBakers, accessed May 1, 2012, http://www.socialbakers.com/facebook-statistics/belarus/last-3-months#chart-intervals.
[11] Mikhail Doroshevich, "Internet in Belarus, October 2011," E-Belarus.org, http://e-belarus.org/news/201112071.html.
[12] Alexa, "Top Sites in Belarus," accessed January 21, 2012, http://www.alexa.com/topsites/countries/BY.
[13] See "Instructions on the procedure of domain names registration in the field of hierarchical names of the national segment of the Internet network" at http://cctld.by/eng/rules.html.
[14] Alyaksey Areshka, "Communications ministry's contract for wholesale broadband services attracts no bids," Belapan, January 11, 2012, http://en.belapan.com/archive/2011/01/11/en_1531.
[15] Alyaksey Areshka, "There are no plans so far to reorganize Beltelecom into stock company, CEO says," Belapan, July 6, 2011, http://en.belapan.com/archive/2011/07/06/en_06071725/.

The controversial Decree No. 60, "On Measures to Improve the Use of the National Segment of the Internet," which was enacted on February 1, 2010 and came into effect on July 1, 2010, has had a mixed impact. In terms of regulation, one requirement of the edict is that all legal entities operating in the ".by" domain must use Belarusian hosting services.[16] This provision does not apply to sites belonging to individuals. However, a personal site that is hosted on a national provider, including internet resources providing free hosting, is subject to compulsory registration by the ISP. Media rights advocates interpret this aspect of the edict as a means of ensuring greater government control over the internet.[17] By December 2011, there were 44,000 domains in the ".by" zone—17,000 were registered in 2011 alone. Some of this increase was due not only to the new decree but also the financial crisis, which made registering a ".by" domain four times cheaper in 2011.[18]

In November 2011, Article 22.12 on "The Violation of Demands on the Use of the National Segment of the Internet" was added to the Administrative Code. The new amendments, which established fines for violations of Decree No. 60, came into force on January 6, 2012. A legal entity or a sole entrepreneur may now be penalized with a modest fine for "selling goods or providing services" in Belarus with the help of websites not registered in Belarus. However, the OAC, which is in charge of enforcing the decree,[19] denied that the new law effectively prohibits Belarusian businesses from advertising and selling their goods or services abroad with the help of foreign-registered websites,[20] despite the language in the law that suggests this.

The new regulations also include a modest fine for internet cafes that fail to keep records of users' personal data, time spent online, and internet traffic, as well as for ISPs that fail to keep similar records.[21] To date, the major impact of the edict has been on internet cafes, which are required to ask users to show identification before going online. This measure has proved to be unpopular with customers and, as a result, business has suffered and some cafes have closed. The new regulations have also threatened to increase costs for ISPs, who are required to install the necessary monitoring and filtering equipment. While heavily

[16] Decree of the Council of Ministers No. 644 of April 29, 2010, "On Some Questions of Improving Usage of the National Segment of the Global Internet Computer Network."
[17] Volha Prudnikova, "Authorities use both legal and illegal methods to control internet, expert says," Belapan, June 24, 2011, http://en.belapan.com/archive/2012/01/11/en_522094_522095/.
[18] The price for an initial year dropped from US$43 to $11. Mikhail Doroshevich, "45 thousand addresses registered in .by domain name zone in 2011," E-Belarus, December 26, 2011, http://www.e-belarus.org/news/201112261.html.
[19] Decree of the President of Belarus No. 60 of February 1, 2010, available in Russian at http://www.mininform.gov.by/documentation; "Decree on Internet Limitations Prepared in Belarus (Text of the Document)," Charter 97, December 14, 2009, http://www.charter97.org/en/news/2009/12/14/24572.
[20] "Доступ к оппозиционным ресурсам пока не блокируется," [Access to opposition resources is not being blocked yet], BelaPAN, January 6, 2012, http://naviny.by/rubrics/computer/2012/01/06/ic_news_128_384196/.
[21] "Fines for breaking Internet filtering regulations introduced in Belarus on January 6," Belarusian Association of Journalists, January 4, 2012, http://baj.by/en/node/9150.

criticized by media rights activists, Decree No. 60 and its amendments have not, to date, limited the growth or the dynamism of the Belarusian internet.

LIMITS ON CONTENT

Decree No. 60 introduced for the first time official mechanisms by which ISPs are required to block access to restricted information, such as pornography and material that incites violence, although by law the authorities are authorized to institute such blocking only in state institutions or when sought by individual users. In practice, however, the government has for a number of years engaged in ad hoc efforts to limit access to internet content deemed contrary to its interests,[22] though Beltelecom typically cited technical problems instead of admitting to blocking. The authorities have regularly blocked certain websites on election days, select holidays important to the democratic opposition, and during protests.

In June 2010, the Ministry of Telecommunications and the OAC issued a regulation that called for the creation of two lists cataloging the URLs of all websites that should be blocked; one list is open to the public, whereas the other list is accessible only by ISPs.[23] As of January 2012, the publicly accessible list did not contain any URLs,[24] while the number of URLs on the closed list remains unknown. The State Telecommunications Inspectorate claims that it has blacklisted 35 websites, most of which contain pornographic content.[25] But based on unofficial information leaked by an internet provider, the latter blacklist counts up to 60 websites[26] and includes two of the country's most popular independent news and information websites, Charter97.org and Belaruspartisan.org, the website of the Viasna Human Rights Center, and the political blog of the popular independent commentator Yauhien Lipkovich.[27] The Prosecutor General's Office confirmed that Charter97.org and Belaruspartisan.org are, indeed, on the restricted list.[28] State bodies authorized to add items to the blacklist include law enforcement agencies such as the Ministry of Internal Affairs, Prosecutor General's Office, and KGB. To date, the blocking is said to be limited to state

[22] Mikhail Doroshevich, "Internet Filtering in Belarus," E-Belarus.org, March 20, 2006, http://www.e-belarus.org/news/200603201.html.

[23] "БелГИЭ приступила к формированию "черного списка" [State Supervisory Body for Telecommunications Started Forming the "Black List"] Electroname, July 9, 2010, http://www.electroname.com/story/7329.

[24] "Списки ограниченного доступа" [Lists of Restricted Access], Ministry of Telecommunications, accessed on January 22, 2012, http://belgie.by/node/216.

[25] "Limited access to 35 websites," Belarusian Association of Journalists, November 10, 2011, http://baj.by/en/node/9081.

[26] "Список запрещенных в Беларуси сайтов вырос до 60" [In Belarus list of blocked sites increased up to 60], Electroname.com, January 6, 2012, http://electroname.com/story/9851.

[27] Zmitsier Lukashuk, "Websites restricted for state institutions since November 28," Euroradio, November 30, 2011, http://baj.by/en/node/9118.

[28] Vyacheslaw Budkevich, "Government begins blocking access to opposition websites," Belapan, April 11, 2011, http://en.belapan.com/archive/2011/04/11/en_20240411.

agencies, including cultural and educational institutions. However, independent sources suggest that, as of early 2012, the blocking was not being implemented and that a variety of opposition and independent sites, including those alleged to be on the blacklist, were still available at government offices and state universities.[29]

Under the November 2011 amendments—which stipulate fines for violating Decree No. 60—ISPs that provide customers with access to blacklisted websites will be required to pay a small fine. More generally and outside of the context of state institutions, ISPs seem to be quite inconsistent in their blocking practices; some have blocked access to blacklisted sites without users' request, which is technically illegal under the decree, while others have ignored the blacklist.[30] In December 2011, Beltelecom selectively blocked certain websites in the Vitebsk region that did not change their domain name system (DNS) servers' settings to comply with state recommendations. Consequently, Charter97.org and several other websites were temporarily unavailable in the Vitebsk region.[31]

Furthermore, access to Charter97.org, as well as Facebook, Vkontakte and Odnoklassniki, is blocked in the luxury hotel "Europe" in Minsk, based on a decision made by the hotel's administration.[32] In January 2012, the BelCel mobile phone operator acknowledged that it occasionally blocked access to opposition websites without clients' permission.[33] In order to limit access to information regarding the summer 2011 "silent protests" and prevent the organizing of new civic actions, one of the largest Vkontatke communities involved in calling for protests in Minsk with over 120,000 users was deleted from the website on July 2, 2011, under the pretext that this group was spreading spam.[34]

Local media rights groups have argued that the regulations adopted during the last two years reflect an alarming trend towards greater control of the internet and that many provisions remain vague and unclear. For example, the procedure of including sites in the blacklist is nontransparent. According to Andrey Bastunets, deputy chairman of the Belarusian Association of Journalists, the illegal methods used by the security services are a greater

[29] Alena Lawrentsyeva, "Access to opposition news sites still free at universities, government buildings, suggests Belapan's survey," January 6, 2011, http://en.belapan.com/archive/2012/01/06/en_1656.
[30] Volha Prudnikova, "Authorities use both legal and illegal methods to control internet, expert says," Belapan, June 24, 2011, http://en.belapan.com/archive/2012/01/11/en_522094_522095.
[31] "Beltelecom: If you don't block Charter97, We'll block Internet," Euroradio, December 28, 2011, http://baj.by/en/node/9144.
[32] "Social nets are banned in five-star hotel 'Europe,'" Nasha Niva, December 29, 2011, http://baj.by/en/node/9146.
[33] Maryna Nosava, "BelCel blocks access to opposition websites for clients without their permission, representative acknowledges," Belapan, January 6, 2012, http://en.belapan.com/archive/2012/01/06/en_1407/.
[34] "В Беларуси заблокировали 'Революцию через социальные сети'" ['Revolution Through Social Networks' is blocked in Belarus], Naviny.by, July 2, 2011, http://naviny.by/rubrics/politic/2011/07/02/ic_articles_112_174244.

threat to the internet than legal restrictions, but both are being used in tandem to further limit internet freedom.[35]

The government is also employing direct and indirect economic pressure to undercut financial support for certain sites. A series of restrictive amendments to the Law on Public Associations and Criminal Code were passed secretly in October 2011 and came into force a month later. Of importance were provisions that made it a criminal offense for nongovernmental organizations (NGOs) to receive foreign funding. Since most online independent media outlets are run as NGOs, the new amendments constitute a grave threat to civil society, including free media, in Belarus.[36]

Most independent news and information websites are at an economic disadvantage because state and private companies are afraid to place commercial advertisements on them. Moreover, there is an unwritten rule advising that companies connected with the state should not advertise in the independent media, including internet publications. As a result, even the most popular independent or opposition websites, such as Charter97.org and NN.by, generate little or no advertising revenue. Since this ban on advertising exists only in the form of an oral recommendation, media and human rights groups have been unable to effectively oppose it.

Another result of state pressure is self-censorship, which has become a pervasive phenomenon for both traditional and web-based media, especially state and commercial outlets. Like their counterparts working for print outlets and television and radio stations, online commentators and administrators of web portals avoid posting content that might put them at odds with the authorities.

The largest Belarusian portal, TUT.BY, has refused to post banners advertising certain independent and opposition websites, and has tightened control over discussion forums by employing moderators to screen comments before they are posted.[37] In October 2011, a live broadcast with the popular independent singer Liavon Volski on TUT.BY-TV was interrupted. The portal's editor explained the incident by saying that the performance

[35] Volha Prudnikava, "Authorities use both legal and illegal methods to control Internet, experts say," Belapan, January 11, 2012, http://en.belapan.com/archive/2012/01/11/en_522094_522095.
[36] See: "Belarus: Open Joint NGO Letter to the Parliament of Belarus," Human Rights Watch, October 20, 2011, http://www.hrw.org/news/2011/10/20/belarus-open-joint-ngo-letter-parliament-belarus.
[37] "Country Profiles: Belarus," OpenNet Initiative, May 9, 2007, http://opennet.net/research/profiles/belarus; Mikhail Doroshevich, "TUT.BY Premoderates Forums," E-Belarus.org, January 22, 2009, http://www.e-belarus.org/news/200901221.html.

contradicted TUT.BY's editorial policy; the portal's owner said that the program was halted after the singer began to openly mock government officials.[38]

The governing regime is attempting to counter the advances in quality, popularity, and trust made by independent civil society by increasing its own presence and influence online. For example, a special governmental program was launched in 2010 to assist regional and local state newspapers in creating and promoting their websites. The program includes the development of a website based on the Wordpress platform, a week-long training course on content management systems, SEO and audio/video editing basics for representatives of state media, and further technical support for optimizing a website. The program is implemented under the supervision of the Ministry of Information. In order to aggregate the content produced by local and regional state publications, a portal for their websites was created at Belsmi.by.

At the same time, the number of trolls and paid commentators, and their activities, has significantly increased on independent websites, the blogs of civic activists and commentators, and popular opposition communities on social networks. In 2011, the anonymous pro-government website "Traitors of Belarus" (Predateli.com) was created, which publishes a list of alleged "traitors of the state" and provides their personal data, including emails and mobile telephone numbers. The list includes the names, biographies, and contact information of opposition political leaders, civic activists, and independent journalists.

In 2011, traditional print and broadcast media continued to have a much stronger presence in society than new media and remained the main sources of news and information for most Belarusians. The internet is still viewed as more of a source of entertainment or as a place to explore contesting opinions. Nevertheless, in the run up to and aftermath of the 2010 presidential election, web-based independent media played a much more visible role and attracted a larger audience than ever before. While the gains in readership have not been uniform, independent news and information web sources continue to serve larger audiences than they did before December 19, 2010. Following the April 11, 2011 bomb blast in a Minsk subway station, hits on independent websites skyrocketed, indicating that citizens are relying less on state media.[39] According to the Belarusian ranking service Akavita.by, most of the Top 10 and a majority of the Top 50 news and information websites are run by independent or opposition groups, and the readership of the leading online independent

[38] "Скандалам завяршыўся візыт Лявона Вольскага на TUT.by" [Liavon Volski's visit to TUT.by ended with a scandal], Svaboda.org, October 25, 2011, http://www.svaboda.org/content/article/24371143.html.
[39] Iryna Vidanava, "Scenes from the battlefield," Eurozine, July 1, 2011, http://www.eurozine.com/articles/2011-07-01-vidanava-en.html.

media has increased on average by 2.5 times since November 2010.[40] The daily audience of Charter97.org, the most popular opposition website, has quadrupled to more than 100,000 unique visitors a day. Independent public opinion polls also indicated that, for the first time, Belarusians began trusting independent media more than the state media in 2011.

In Belarus, elections have had a strong impact on the development of ICTs. As the authorities moved to close down and restrict independent print newspapers before the 2006 presidential election, blogs, internet forums, online communities, and news websites became more prominent during and after the campaign. With the rapid rise of new media, independent online sources were able to compete with state-controlled newspapers, radio, and television during the 2010 campaign and the protests following the election. In addition to independent news and information websites, Facebook, Vkontakte, and Twitter played a significant role in educating citizens, turning out voters, and mobilizing those protesting electoral irregularities. In 2010, a crowd-sourcing platform was used for the first time to monitor election violations.[41]

After the December 2010 crackdown, a citizen solidarity campaign was launched by an activist's emotional blog post that described the awful prison conditions of those detained and called her friends to help by donating cloths, money, transport, etc. Her post was republished by other bloggers and mainstream independent online media. Hundreds responded. To better coordinate the effort to help those arrested and their families, a special website was set up where people could identify what kind of assistance was needed and become a "guardian angel" to a detainee. More than US$50,000 was collected, and over 700 parcels were prepared and delivered to prisons. The same campaign was used to mobilize support for those detained during the summer 2011 protests.[42]

In summer 2011, social networks were also used as a major tool in organizing the "Stop Gasoline" strike, which caught the police and authorities by surprise. On June 7, 2011, hundreds of cars blocked Independence Avenue, a major thoroughfare in downtown Minsk, at rush hour in protest against increasing gasoline prices. The next day, the government backtracked and reduced prices.[43]

[40] "Top ranker," Akavita.by, accessed on January 22, 2012, http://akavita.by/top/en/All/Mass_Media_and_News/daily/visitors/by.

[41] See report on Electby.org (in English) at http://belaruswahl2010.wordpress.com/2010/12/28/bericht-der-electby-wahlbeobachtungsplattform.

[42] Galina Abakunchik, "«Анёлы-ахоўнікі» вярнуліся ў Менск" ["Angels guards' return to Minsk], Svaboda.org, July 8, 2011, http://www.svaboda.org/content/article/24259862.html.

[43] "Пасля пратэсту аўтамабілістаў Лукашэнка загадаў знізіць кошты на бензін" [After the car owners' protest Lukashenka ordered to reduce the gasoline price], Nasha Niva, June 8, 2011, http://nn.by/?c=ar&i=55457.

The success of the "Stop Gasoline" strike sparked a series of large-scale silent protests across the country. Weekly peaceful demonstrations were organized in June-July 2011 through a "Revolution through Social Networks" campaign, launched by pro-democratic communities on Facebook and Vkontakte. The campaign brought thousands of citizens, mostly young people, to the streets in most major Belarusian cities. Fearing that online campaigns would lead to mass street demonstrations, social-networking websites were temporarily blocked on the days of the protests.[44] One of the Vkontakte communities calling for the protests in Minsk and consisting of over 120,000 users was deleted from the website on July 2, 2011.[45] The "Revolution through Social Networks" initiative was not the only example of Belarusian self-organizing online. There are at least five other anti-government communities on Vkontakte, which number between two and 20,000 people.

Internet tools have also been used to further online petitions on important political issues. In November 2011, almost 62,000 people signed an online petition against the death penalty sentence given to two Belarusians convicted of a terrorist act in the Minsk metro.[46] In November and December 2011, over 1,700 people added their names to an online petition for the release of the prominent Belarusian human rights defender, Ales' Bialiatski, who was sentenced to 4.5 years in prison on trumped up charges of tax evasion.[47]

Because Belarusian users have, until quite recently, had regular access to most online resources under ordinary circumstances, they generally have not employed proxy servers or other circumvention tools, leaving them vulnerable during politically sensitive periods when ad hoc disruptions occur. Most often, people are reminded about blocking, hacking, trolling and phishing only when it takes place.[48] The most popular circumvention tools are proxies and Tor, a software system that enables online anonymity.[49]

[44] "В Беларуси заблокирован доступ к Вконтакте" [Access to Vkontakte is blocked in Belarus], Naviny.by, July 13, 2011, http://naviny.by/rubrics/computer/2011/07/13/ic_news_128_372197.

[45] "В Беларуси заблокировали 'Революцию через социальные сети'" ['Revolution Through Social Networks' is blocked in Belarus], Naviny.by, July 2, 2011, http://naviny.by/rubrics/politic/2011/07/02/ic_articles_112_174244.

[46] "Innocent until proven guilty," Care2 Petition Site, accessed on January 23, 2012, http://www.thepetitionsite.com/1/15-days-left-to-save-lives-of-2-young-men-that-are-going-to-be-executed/.

[47] "Sign a petition for the release of Ales' Bialiatski," Freeales.spring96.org, accessed on January 23, 2012, http://freeales.spring96.org/en.

[48] Yegor Martinovic, "Што рабіць, каб не падчапіць вірус у Інтэрнэце" [What to do in order not to catch a virus in Internet], Nasha Niva, January 15, 2012, http://nn.by/?c=ar&i=66614; "ЖЖ заблокировано" [LJ is blocked], Community.livejournal.com/minsk_by, January 10, 2008, http://community.livejournal.com/minsk_by/4402235.html.

[49] "Как обойти блокировку сайта?" [How to circumvent a website blockade?], Charter 97, January 18, 2008, http://www.charter97.org/be/news/2008/1/18/3107.

VIOLATIONS OF USER RIGHTS

Civil rights, including the right to access information and freedom of expression, are guaranteed by the Belarusian constitution, although they remain severely restricted in practice. A 2008 law identified online news outlets as "mass media," and Article 33 requires every such website to include the names of the publication, its founder(s), and its chief editors, as well as the full address of the editorial office and the registration number.[50] Formally, there are no laws assigning criminal penalties or civil liability specifically for online activities, but internet activities can be prosecuted under laws applicable to mass media—mainly for defamation—or under any relevant criminal law. In addition, government officials have stressed the need to hold site owners and service providers legally accountable for prohibited content and to provide them with the tools to block such content.[51]

Decree No. 60 requires ISPs to maintain records of the traffic of all internet protocol (IP) addresses, including those at home and at work, for one year. As a result, the state can request information about the internet use of any citizen. Since 2007, internet cafes are obliged to keep a 12-month history of the domain names accessed by users and inform law enforcement bodies of suspected legal violations.[52] Mobile phone companies are required to turn over similar data when asked by the government. Individuals are required to present their passports and register when they buy a SIM card and obtain a mobile phone number.

Following the December 19th protests, security services raided more than a dozen editorial offices and journalists' private apartments, including those connected to popular online news and information sites. Over 114 pieces of professional media equipment were seized.[53] Scores of journalists were arrested and criminal proceedings were initiated against seven members of the Belarusian Association of Journalists; six were convicted and punished with sentences ranging from probation to four years in a maximum security prison for allegedly organizing and preparing actions that disturbed the public order, or for actively participating

[50] Law of the Republic of Belarus No. 427 of July 7, 2008, "On the Facilities of Mass Information," available in Russian at http://www.mininform.gov.by/documentation; "Экспертыза новага закона «Аб СМІ»" [Analysis of the New Law on mass media], Belarusian Association of Journalists, accessed on July 9, 2010, http://baj.by/m-p-viewpub-tid-12-pid-5.html; "International expertise of the Belarusian draft law on information, informatization and information protection," E-Belarus.org, March 2007, http://www.e-belarus.org/article/infolaw.html.

[51] "Пролесковский знает, как зачистить интернет" [Proleskovsky knows how to clean up the internet], Belaruspartisan.org, June 4, 2008, http://www.belaruspartisan.org/bp-forte/?page=100&news=25145.

[52] "Совет Министров Республики Беларусь Положения о порядке работы компьютерных клубов и Интернет-кафе" [Council of Ministers of the Republic of Belarus. Regulations on computer clubs and internet cafe functioning], Pravo.by, April 29, 2010, http://pravo.by/webnpa/text.asp?start=1&RN=C20700175.

[53] Iryna Vidanava, "Scenes from the battlefield," Eurozine, July 1, 2011, http://www.eurozine.com/articles/2011-07-01-vidanava-en.html.

in such actions, violating Article 342 of the Criminal Code. After the December 19th demonstrations, mobile phone providers reportedly assisted authorities in tracking down protesters and opposition activists.[54]

Over the past year, more than 3,500 citizens were arrested. The majority of these arrests took place during the summer 2011 "silent protests" related to the country's economic and political crisis. Of those arrested, no fewer than 95 were journalists. In 2011, more than 150 journalists were detained, 22 were tried, and 13 were sentenced for different alleged administrative infractions, including participating in unsanctioned mass protests, hooliganism, and slander.[55] As of early 2012, more than a dozen political prisoners remain behind bars, including three members of the Belarusian Association of Journalists.[56] Many of the journalists who were repressed in 2011 worked for independent websites or media outlets with an online presence.

In 2010, the authorities initiated several criminal cases against Charter97.org alleging the website's liability for objectionable comments posted by its readers.[57] In the wake of the post-election crackdown, Charter97 editor Natallya Radzina was detained on December 20, 2010 by the KGB. She was released on January 28, 2011 and placed under house arrest, but was able to flee the country on March 31, 2011. She was granted political asylum in Lithuania, and the editorial office of Charter97.org now operates in exile.

In addition to legal and technical attacks on independent news sites, there were numerous cases of prosecution of individual media activists for their online activities in 2011. The most prominent case involved the April arrest of journalist Andrzej Poczobut. He was convicted of insulting the president of Belarus in a series of articles, including those posted on the online version of the Polish daily *Gazeta Wyborcza*, Belaruspartisan.org, and his LiveJournal blog; he received a three-year suspended sentence.

In June 2011, criminal proceedings were launched against the civic journalist and blogger, Yauhien Lipkovich, who was charged with defaming state symbols in his LiveJournal blog. In August 2011, two Homyel residents were jailed for five and three days, respectively, over internet postings linked to the summer protests. Another Homyel resident was fined for

[54] "Ні дня бяз допытаў" [Not a single day without interrogation], Reporter.by, January 20, 2011, http://reporter.by/Belarus/N-dnja-bjaz-dopyta/function.mysql-connect.
[55] "Violations of Journalists' and Mass Media Rights in 2011: Brief Annual Review," Mass Media Belarus E-Newsletter, Belarusian Association of Journalists, http://old2.baj.by/index.php?module=p&type=file&func=get&tid=6&fid=pdf&pid=84.
[56] Helle Whalberg, "A year of turmoil – but change is on its way," International Media Support, December 20, 2011, http://i-m-s.dk/?q=article/belarus-year-turmoil-change-way.
[57] "Против сайта charter97.org возбуждено третье уголовное дело" [Criminal case brought against charter97.org website], Electroname, December 8, 2010, http://www.electroname.com/story/9100.

inviting his friends via Vkontakte to meet during a "silent protest" staged in the city. In September 2011, a young truck driver from Mazyr lost his job after being fined for online political postings.[58] In October 2011, a journalist in Mahilyow was questioned by the prosecutor's office regarding comments made about a local judge, which were posted on Charter97.org.[59] In January 2012, a student of Belarusian State University sent an open letter to a leading Belarusian newspaper describing how he was called to the dean's office and interrogated by unidentified KGB employees about his public sharing of opposition documentaries through an internal computer network in his dormitory.[60]

In October 2011, the government introduced and the parliament approved an "anti-revolutionary" package of amendments to laws on civic organizations and political parties, as well as to the Criminal Code. The amendments—which apply to internet-based media outlets—further criminalize protest actions, make receiving foreign funding a criminal offense, and extend the authority of the KGB. Under the amendments, the KGB is now freed from the oversight of other state bodies and has been given powers previously only granted during a state of emergency, including the right to break into the homes and offices of any citizen at any time without a court order.[61] Beginning in March 2012, a significant but unknown number of opposition political leaders, human rights defenders and independent journalists were banned from traveling abroad.[62] This violation of freedom of movement was a reaction to the extension of the European Union's visa ban list of Belarusian officials involved in the 2010-11 repression.

It is difficult to gauge the extent to which Belarusian security services monitor internet and mobile phone communications, but the surveillance is believed to be far-reaching. On December 19, the day of the 2010 presidential election, the government blocked international connections to ports 443 and 465, thereby preventing users from securely sending emails and posting messages on social-networking sites. In the cases of several of those convicted for political reasons after December 19, personal Skype conversations and emails were used by the prosecution as evidence during the trials. These communications were also cited in articles published in the leading state-run newspaper. It is unclear whether the electronic documents were intercepted by the government or taken from confiscated computers.

[58] Alena Hermanovich, "Young man in Homyel region loses job after being fined over political postings," Belapan, September 7, 2011, http://en.belapan.com/archive/2011/09/07/en_07091042.
[59] Uladzimir Laptsevich, "Journalist in Mahilyow questioned at prosecutor's office over 'abusive' online posts about local judge," BelaPAN, October 14, 2011, http://en.belapan.com/archive/2011/10/14/en_1159.
[60] "Можаце збірацца сваім пакоем і глядзець хоць некалькі раз у суткі" [You can gather in your room and watch them even several times a day], NN.by, January 19, 2012, http://nn.by/?c=ar&i=66886.
[61] "Belarus has adopted 'anti-revolutionary' amendments to the legislation," Human Rights House, October 20, 2011, http://humanrightshouse.org/Articles/17082.html
[62] For Belarusian Association of Journalists' reaction to the restriction on journalists' travel, see http://baj.by/en/node/11459.

Instances of extralegal intimidation and harassment for online activities have increased. During the course of 2011, there were reports of students being summoned by university administrators and interrogated by unidentified secret police agents about posts on their personal blogs and social networks. These students were threatened with expulsion and told that their parents would be fired from their jobs if they refused to cooperate with the authorities.

Instances of technical attacks against independent news sites and civil society have continued to grow. For example, the website of Radio Racyja, which is based in Poland and broadcasts independent news and information into Belarus, was hacked on November 26, 2011 and temporarily disabled.[63] At the end of December 2011, Charter97.org and the website of the opposition youth group "Young Front" (Mfront.net) experienced repeated distributed denial-of-service (DDoS) attacks. Nearly paralyzing the website, hackers deleted much of Charter97.org's content and posted a false report about the former presidential candidate and political prisoner, Andrey Sannikaw, and his wife, the prominent independent journalist Iryna Khalip. The Young Front site did not function for several days.

A January 2012 inquiry conducted by Electroname.com, a website covering computer and electronics issues, determined that the computers of several opposition politicians, independent journalists, human rights defenders, and online activists had been infected with Trojan viruses that had stolen their passwords and other private information. Electroname.com determined that unidentified hackers had used the same viruses known to be distributed by the KGB. In the December 2011 attack on Charter97.org, for example, the hackers used RMS, a virus developed by Russia's TeknotIT, which the KGB had attempted to use previously to infect an opposition activist's computer in July 2011.[64]

The authorities also tried to shut down Prokopovi.ch, an economic website that was created during the peak of the 2011 currency crisis. Satirically named after the former president of the National Bank of Belarus who was among those responsible for the crisis, the site was designed to facilitate illegal currency exchanges. It soon became very popular and actually influenced exchange rates. On August 30, 2011, Prokopovi.ch experienced a massive DDoS attack and was down for one day. It resumed working the following day. The Prosecutor General's Office attempted to track down the creators and moderators of the website but did not succeed.[65]

[63] "Radio Racyja website hacked," Belarusian Association of Journalists, November 29, 2011, http://old2.baj.by/m-p-viewpub-tid-1-pid-11992.html.

[64] "Кибероружие белорусского КГБ" [Cyberweapon of the Belarusian KGB], Electroname.com, January 9, 2012, http://electroname.com/story/9865.

[65] "Final solution to foreign currency problem: DDoS attack on prokopovi.ch," Charter97.org, August, 30, 2011, http://charter97.org/en/news/2011/8/30/42085.

Amid widespread technical attacks in the aftermath of the 2010 election and 2011 economic crisis—some of which have been traced to the authorities—it is important to note that Belarusian criminal law prohibits such activity. Specifically, Article 351 of the Criminal Code, covering "computer sabotage," stipulates that the premeditated destruction, blocking, or disabling of computer information, programs, or equipment is punishable by fines, professional sanctions, and up to five years in prison.[66] The government has stated its intention to accede to the Council of Europe's Convention on Cybercrime, but it has made no moves to sign on to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[66] "«Белтелеком»: Возможно, независимые сайты блокировали другие организации" [Beltelecom: Independent websites could be blocked by other organizations], Charter 97, January 10, 2008, http://www.charter97.org/ru/news/2008/1/10/2905.

BRAZIL

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	7	7
Limits on Content (0-35)	7	6
Violations of User Rights (0-40)	15	14
Total (0-100)	**29**	**27**

* 0=most free, 100=least free

POPULATION: 194 million
INTERNET PENETRATION 2011: 45 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

For a country with large social and economic disparities, Brazil has made significant gains in expanding internet access and mobile phone usage in recent years. The country first connected to the internet in 1990, and connectivity is now available in most areas through a variety of technologies, though some infrastructural limitations remain.[1] Further, Brazil continues to face low internet penetration and digital exclusion due to infrastructural problems, social inequality, and poor education, among other reasons, but the federal government has executed several policies over the years to remedy this. Nevertheless, in recent years, social network activity and civic participation on the internet have increased remarkably.

The Brazilian government does not employ any technical methods to filter or otherwise limit access to online content. In 2011, the main restrictions to online expression came from civil defamation suits and legal action by the judiciary and government officials following an ongoing trend in which private litigants and official bodies sue internet service providers (ISPs) and other internet companies and send takedown notices to blogging and social-networking platforms. Google's Transparency Report recorded Brazil as having the highest number of government requests to remove content among the countries assessed in 2011.

[1] Robert Hobbes Zakon, "Hobbes' Internet Timeline v8.2," Zakon Group LLC, accessed August 11, 2010, http://www.zakon.org/robert/internet/timeline/; Tadao Takahashi, ed., *Sociedade da Informação no Brasil: Livro Verde* [Information Society in Brazil: Green Book] (Brasilia: Ministry of Science and Technology, September 2000), http://www.mct.gov.br/index.php/content/view/18878.html; National Education and Research Network (RNP), "Mapa do Backbone" [Map of Backbone], accessed August 11, 2010, http://www.rnp.br/backbone/index.php.

As Brazil rises to the level of leading global economies and slowly comes closer to a networked society, issues such as cybercrimes and distributed denial-of-service (DDoS) attacks, access to public information, election campaigning on the web, and intellectual property protection are gaining the political spotlight. In a positive development, the Civil Rights Framework for the Internet was introduced in Congress in August 2011, which aims to guarantee access to the internet, safeguard freedom of speech and communication, protect privacy and personal data, and preserve net neutrality, among other provisions.

OBSTACLES TO ACCESS

Despite having a large population of internet users, Brazil still lags behind many developing countries in terms of relative internet penetration, with 45 percent of the population having access to the web in 2011, according to the International Telecommunication Union (ITU).[2] Penetration varies greatly among regions due to a lack of infrastructure that affects large segments of the population in rural areas. For instance, while the household penetration rate was 36 percent in the more urban southeast region in 2010, it was only 11 percent in the poorer and more rural northeast region of the country.[3] High costs and lack of infrastructure hinder the spread of household broadband connections, with the broadband subscription penetration rate reaching 8.6 percent in 2011.[4] While broadband access is increasing as prices fall, the market is still concentrated among major telecommunications and cable companies. Meanwhile, 13 percent of households with fixed internet in Brazil are still connected via dial-up.[5]

Brazil is currently the largest mobile phone market in Latin America. Statistics show an average annual increase of 18 percent in the rate of mobile phone use over the last five years,[6] and mobile phone penetration stood at 123 percent in 2011.[7] According to Nielsen

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[3] Brazilian Internet Steering Committee (CGI.br), "Survey On The Use Of Information And Communication Technologies In Brazil 2010," pg. 402, accessed February 6, 2011, http://www.cetic.br/tic/2010/index.htm.

[4] [4] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011.

[5] Brazilian Internet Steering Committee (CGI.br), "Survey On The Use Of Information And Communication Technologies In Brazil 2010," pg. 404-406.

[6] Teleco, "Seção: Telefonia Celular—Estatísticas de Celulares no Brasil" [Section: Cellular Telephony—Statistics of Cellular Telephones in Brazil], February 6, 2012, http://www.teleco.com.br/ncel.asp.

[7] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

Ratings, the sales of smartphones in Brazil increased by 165 percent in the first semester of 2011 compared to the same period in 2010.[8]

Great improvements in the development of information and communication technologies (ICTs) have been made in recent years as the government has initiated dozens of programs to connect the population to the internet. For example, the National Broadband Plan was launched in 2010, which aims to triple broadband access by 2014.[9] In many regions, "LAN (local area network) houses" have become the primary means of internet access for low income Brazilians. Research published by the Brazilian Internet Steering Committee in 2011 showed that nearly 70 percent of people from the lowest income brackets who access the internet do so via commercial venues such as LAN houses, a dramatic increase from 48.1 percent in 2006.[10] The sharp drop in desktop and laptop prices in the last five years has begun to alter this trend, but LAN houses nonetheless still play a key role in internet democratization in Brazil.[11] In February 2012, the government announced that tablets will benefit from a tax incentive[12] and will be distributed to public school teachers.[13]

Among changes to the national legal system brought about by the increase in internet-related ICTs in the last few years is a relevant amendment to the labor legislation that explicitly acknowledges telecommuting. The legislation also guarantees pay in exchange for time spent by employees answering professional emails on their mobile phones, even when outside of the office.[14] As Brazilians at all socioeconomic levels increasingly use the internet, a growing number have taken advantage of the country's e-commerce, e-government, and online banking services;[15] the latter have proved generally successful, with total online transactions surpassing those by other means, including ATMs, in 2010.[16]

---

[8] G1, "Vendas de smartphones crescem 165% no Brasil, diz pesquisa," August 16, 2011, http://g1.globo.com/tecnologia/noticia/2011/08/vendas-de-smartphones-crescem-165-no-brasil-diz-pesquisa.html.

[9] Ministry of Communications, "Um Plano Nacional para Banda Larga" [A national plan for high bandwidth], accessed August 30, 2012, http://www4.planalto.gov.br/brasilconectado/pnbl.

[10] Brazilian Internet Steering Committee (CGI.br), "Survey On The Use Of Information And Communication Technologies In Brazil 2010," pg. 418.

[11] Anna Heim, "Why Brazilian cyber cafés still matter," The Next Web, June 19, 2011, http://thenextweb.com/la/2011/06/19/why-cyber-cafes-still-matter/.

[12] Joe Aimonetti, "Apple gets tax incentives in Brazil to begin iPad production," CNET, January 25, 2012, http://reviews.cnet.com/8301-19512_7-57366337-233/apple-gets-tax-incentives-in-brazil-to-begin-ipad-production/.

[13] "Primeiros a receber tablets serão professores, anuncia MEC," Estadao.com.br, February 3, 2012, http://www.estadao.com.br/noticias/vidae,primeiros-a-receber-tablets-serao-professores-anuncia-mec,830914,0.htm [in Portuguese].

[14] "Brazil's Email Overtime: New Law Counts Checking Smartphones After Hours As Work," The Huffington Post, January 12, 2012, http://www.huffingtonpost.com/2012/01/13/brazils-email-overtime_n_1204343.html.

[15] "Brazil—Internet and Broadband Market," BuddeCom, May 2011, http://www.budde.com.au/Research/Brazil-Broadband-Market-Overview-Statistics-and-Forecasts.html.

[16] Brazilian Central Bank, "Diagnóstico do Sistema de Pagamentos de Varejo do Brasil Adendo estatístico – 2010," accessed February 6, 2012, http://www.bcb.gov.br/htms/spb/Diagnostico-Adendo-2010.pdf [in Portuguese].

National and international news sources are unrestricted, and Brazilians freely gather information through the internet, mobile phone technology, and other ICTs. Blogs, photoblogs, social-networking platforms, and citizen journalism have proliferated in recent years. As of 2011, Brazilians spend more of their time online (over 18 percent) on social networks and forums than any other people in the world.[17] The Google-owned social-networking site Orkut has been nearly omnipresent in Brazil in the last five years, constantly topping Facebook; however, Facebook finally beat out its rival in December 2011 when it accrued more unique visitors than Orkut (36 million against 34.5 million).[18] Nevertheless, these statistics fail to account for access on public computers and in cybercafes where most low-income individuals go to browse the web. The number of Facebook users has increased dramatically since 2009 as Brazilians have sought to connect with acquaintances outside the country where Orkut is less popular. Twitter's popularity has also grown significantly—40 percent in December 2011 when compared to the same month in 2010.[19] Unlike in previous years, there were no instances during 2011 of advanced web applications like the video-sharing site YouTube or the social-networking platform Orkut being completely blocked by court orders, though individual videos or comments have been removed.

Even though there are no specific legal or economic obstacles restricting the operation of ISPs or other businesses that provide access to digital technologies—which has enabled the number of broadband ISPs registered with the Federal Telecommunications Agency to boom in the last three years, going from a little over 1,000 in 2008 to over 3,000 in 2011[20]—the introduction of new technologies and continuous price drops in ICT services have been significantly impaired by market concentration. As of the third quarter of 2011, four companies (Oi, NET, Telefonica, and GVT) concentrated roughly 90 percent of the broadband market in the country.[21] Six private companies share the mobile phone market, the largest four of which amount to a market share of over 99 percent.[22]

The National Telecommunications Agency (ANATEL) and the Administrative Council for Economic Defense (CADE), an antitrust body, work to ensure that ICTs operate in a free, fair, and independent manner. The two agencies have an agreement of cooperation that

[17] That is the result presented in a study by: Experian, "The local network: Experian analysis highlights which countries spend longest on Facebook," September 27, 2011, http://www.experianplc.com/news/company-news/2011/27-09-2011.aspx.
[18] "Facebook overtakes Google's Orkut in Brazil – Comscore," BBC, January 18, 2012, http://www.bbc.co.uk/news/technology-16611554.
[19] Jeff Hughes, "Study: Twitter follows Facebook's overseas growth into Brazil," Yahoo News, February 2, 2012, http://news.yahoo.com/study-twitter-follows-facebooks-overseas-growth-brazil-060225652.html.
[20] Teleco, "Seção: Banda Larga—Prestadoras de SCM" [Section: Broadband—Multimedia Communication Service providers], January 20, 2012, http://www.teleco.com.br/scm_prest.asp.
[21] Teleco, "Seção: Banda Larga—Market Share de Banda Larga no Brasil" [Section: Broadband—Market Share of Broadband in Brazil], January 20, 2012, http://www.teleco.com.br/blarga.asp.
[22] Teleco, "Seção: Telefonia Celular—Operadoras de Celular, Jun/10" [Section: Cellular Telephony—Cellular Operators, June 2010], January 17, 2012, http://www.teleco.com.br/mshare.asp.

defines their competencies. The CADE is authorized by the General Telecommunications Law to have the final word when dealing with antitrust issues, such as market concentration and price setting.[23]

In a pioneering initiative, the Brazilian Internet Steering Committee (CGI.br), a multi-stakeholder organization, was created in 1995 to guarantee transparency and social participation in decisions related to the management of the ".br" country-code top level domain (ccTLD).[24] The CGI has played a substantive role in the Brazilian internet governance and regulation debate over the years;[25] its contributions include reliable and comprehensive yearly reports on the state of internet adoption in Brazil as well as funding for internet governance-related research and academic publications. Committee members come from the government, the private sector, academia, and nongovernmental organizations, with the last group chosen in 2004 in relatively democratic and open elections.

LIMITS ON CONTENT

The government does not employ any technical methods to filter or otherwise limit access to online content. Nonetheless, legal action by the judiciary and government officials has emerged as a possible barrier to free speech and a means of removing content deemed undesirable. Google's Transparency Report recorded Brazil as having the highest number of government requests to remove content among the countries assessed in 2011, with 418 requests, followed by the United States and Germany.[26] According to the report, "Government requests for content removal are high in Brazil relative to other countries partly because of the popularity of our social networking website, Orkut."[27]

[23] Maria Cecília Andrade, Ubiratan Mattos, and Pedro C. E. Vicentini, "Reforms in Brazilian Telecommunications Regulations and their Impact on Sector Competition," in *The Antitrust Review of the Americas 2009* (London: Global Competition Review, 2009), http://www.globalcompetitionreview.com/reviews/9/sections/31/chapters/361/reforms-brazilian-telecommunications-regulations-impact-sector-competition; Teleco, "Regulation: Legislation Guide," July, 28, 2010, http://www.teleco.com.br/en/en_legis.asp.

[24] See the website of the Brazilian Internet Steering Committee, http://www.cg.org.br/internacional/index.htm.

[25] See the Committee's Principles for the Governance and Use of the Internet, accessed February16, 2012, http://www.cgi.br/english/regulations/resolution2009-003.htm.

[26] Google, "Government," *Transparency Report*, (Mountain View, CA: Google, 2011), accessed February 6, 2012, http://www.google.com/transparencyreport/governmentrequests/removals/. Another explanation for Brazil's peculiar track record on court-ordered content removals is that lawsuits can be filed more easily in Brazil than in many other countries, where other forms of dispute resolution or regulation of online content prevail. See, Danny O'Brien, "Is Brazil the Censorship Capital of the Internet? Not Yet," CPJ Blog, April 28, 2010, http://cpj.org/blog/2010/04/is-brazil-the-censorship-capital-of-the-internet.php.

[27] Google, "Brazil," *Transparency Report*, (Mountain View, CA: Google, 2011), accessed August 15, 2012, http://www.google.com/transparencyreport/removals/government/BR/?p=2011-06.

While the federal and state governments have never sponsored systematic content filtering or online censorship, state efforts to place limits on content have occurred periodically. For example, in April 2011, a federal judge in the state of Tocantins forbade the *Arnaldo Filho* news portal from reporting accusations made by former employees of education institutions in the city of Araguaína.[28] The state's Professional Journalists Union published a statement condemning the court order.[29] In another example in early 2012, the Federal Ministry of Tourism sent a request to a web-hosting company to takedown a ".eu" domain name that associated the word "Brazil" with pornography, claiming that the association inadequately portrayed the nation as a "pole of sexual activities… interfer[ing with] the position and image of the country," which is a crime punishable by the Brazilian Penal Code.[30] The company took down the domain, which was not being used at the time, but put it back up soon afterward due to Brazil's lack of jurisdiction over the ".eu" domain.

In July 2011, a São Paulo court ordered Brazilian ISPs to block the blog of journalist Paulo Cezar Prado after receiving a complaint from a businessman who the blogger had accused of laundering money.[31] Prado subsequently vowed to mirror his site on different webhosts in other countries to circumvent the censorship and now has his blog hosted in France after it was removed by some American and Brazilian hosts.

In February 2012, the Brazilian Attorney General's office in the state of Goiás filed a suit against the microblogging website Twitter, requiring it to remove accounts that warned drivers about police traps meant to catch speeding and drunk drivers.[32] The state Federal Public Prosecutor's office, however, reacted firmly against the suit, emphasizing the curtailment of freedom of expression imposed by such measures.[33] The incident demonstrates that online censorship by the government is not a pervasive effort in Brazil.

[28] Natalia Mazotte, "Justiça do Tocantins proíbe site de publicar denúncias" [Court in Tocantins forbids website from publishing accusations], Knight Center for Journalism in the Americas, April 21, 2011, http://knightcenter.utexas.edu/pt-br/blog/justica-do-tocantins-proibe-site-de-publicar-denuncias [in Portuguese].
[29] Junior Veras, "Juiz proíbe publicação de material" [Judge forbids publication of piece], Observatório da Imprensa [Press Observatory], April 26, 2011, http://www.observatoriodaimprensa.com.br/news/view/juiz_proibe_publicacao_de_materia [in Portuguese].
[30] Mike Masnick, "Brazilian Government Ordering Web Hosting Firms To Kill Domain Names They Don't Like," Tech Dirt, February 8, 2012, http://www.techdirt.com/articles/20120207/03474017680/brazilian-government-ordering-web-hosting-firms-to-kill-domain-names-they-dont-like.shtml.
[31] Natalia Mazotte, "Judge orders Brazilian internet providers to censor blog that criticizes soccer executives," Journalism in the Americas (blog), July 20, 2011, http://knightcenter.utexas.edu/blog/judge-orders-brazilian-internet-providers-censor-blog-criticizes-soccer-executives.
[32] Gerald Jeffris, "Brazil Wants To Ban Tweets About Police Speed-Traps," Wall Street Journal, February 10, 2012, http://blogs.wsj.com/digits/2012/02/10/brazil-wants-to-ban-tweets-about-road-traffic/.
[33] Ministério Público Federal, Procuradoria da República em Goiás, "MPF/GO contrapõe-se à censura na internet," February 13, 2012, http://www.prgo.mpf.gov.br/direitos-do-cidadao/noticias/895-mpfgo-contrapoe-se-a-censura-na-internet.html [in Portuguese].

Over the last five years, intermediary liability has been the main arena for online free speech protection in Brazil. Facebook recently joined Orkut as the target of civil liability claims, which are made in most cases by people unhappy with the way they are portrayed on those social networks.[34] State courts are largely divided on this issue: some attribute strict liability to crowdsourcing websites and social networks; others have adopted a notice-and-takedown approach that would impose liability only if the intermediary fails to remove the unwanted content after extrajudicial notice. This latter position's origins can be traced to the arrangement established by the Digital Millennium Copyright Act in the United States.

Over the course of 2010 and 2011, two rulings in the Superior Court of Justice, the country's second highest court, demonstrated an apparent shift from a relatively restrictive to a jurisprudential understanding of online free speech. In 2010, one of the court's ministers upheld a lower court order in an appeal that required Google, under penalty of daily fines, to prevent certain "abusive" speech from being made available in the social network Orkut. The court minister's individual ruling called for online prior restraint, pointing out that if it was technically possible in China, it ought to be feasible in Brazil as well.[35] In August 2011, the court again ruled on the issue of Google's liability for content posted on Orkut. This time, however, it established that intermediaries could not be held liable unless they failed to remove content after being given specific notice.[36]

Intellectual property protection is a constant issue of discussion in the Brazilian online public sphere, but is not a great threat to online free speech. Discussions on the reform of the Brazilian Copyright Act has also attracted meaningful online participation, and civil society groups have joined forces with scholars to support or criticize the government and press for a transparent process and a more flexible copyright law.[37] There are still concerns about the bill's potential impact on internet access. The government has not yet introduced the Copyright Act reform for approval in Congress, but the new Minister of Culture, Ana de Hollanda, has declared that the reform would reach the legislators by 2012.[38] Hollanda has also pursued some changes in the ministry's policy regarding intellectual property

[34] This changed a common pattern in the last 4-5 years where Orkut was almost the sole social network to suffer legal suits. See cases against Facebook in two state high courts: "Offenses causing temporary injunction on Facebook," TJMG, news release, January 1, 2012, http://www.tjmg.jus.br/anexos/nt/noticia.jsp?codigoNoticia=38138 [in Portuguese]; "Facebook should remove defamatory messages about Christmas shop," Poder Judiciario, noticias, February 3, 2012, http://www.tjrn.jus.br:8080/sitetj/GerenciadorServlet.do?secaoSelecionada_id=9&id=8362&action=GerenciadorWeb&operacao=exibirInternet&exibir=E&registrarLeitura=true [in Portuguese].

[35] "Google fine for uncensored dirty jokes," News.com.au, March 24, 2010, http://www.news.com.au/technology/google-fine-for-uncensored-dirty-jokes/story-e6frfro0-1225844583476.

[36] Brazilian Superior Court of Justice, *Recurso Especial* no. 1.193.764 – SP, accessed February 7, 2012, http://www.stj.gov.br/webstj/processo/justica/detalhe.asp?numreg=201000512263.

[37] See the website of the copyright reform movement at http://www.reformadireitoautoral.org/.

[38] Luiz Fernando Vianna, "Ana de Hollanda apressa projeto de reforma da Lei do Direito Autoral," O Globo Cultura, April 20, 2011, http://oglobo.globo.com/cultura/ana-de-hollanda-apressa-projeto-de-reforma-da-lei-do-direito-autoral-2793479 [in Portuguese].

protection. In February 2011, for example, she had the Creative Commons[39] license taken out of the ministry's website, which was highly criticized and seen as a move favoring the copyright industry.[40] This, along with other political developments and backstage negotiations, has raised concern among civil society and academia that copyright could emerge as a relevant threat to freedom on the Brazilian net.[41]

Past state-initiated censorship attempts have primarily appeared in the context of elections. However, in a positive development following strong political pressure, the Senate in September 2009 approved changes to the electoral law to permit the use of the internet in political campaigns.[42] In addition, new legislation proposed in 2011 would create a legal environment more hospitable for free political speech. Under the draft introduced by Representative Rodrigo Garcia, individuals and parties would be able to carry out online campaigning before TV, radio, and press advertisements are authorized to commence, as long as it is performed freely and without commercial ads.[43] The government has shown, however, that it will not easily give up the regulation of political expression online. Furthermore, campaigning is usually forbidden before July in an election year (elections are held in October), and the Electoral Superior Court ruled in March 2012 that such a restriction was also applicable to political speech on Twitter.[44]

There have been positive developments regarding the issue of access to public information, with the Federal Prosecutor's office announcing that in 2012 it will make available on its website some 700 military court procedures held between 1979 and 1985, including accounts of torture of civilians.[45] Additional examples include projects promoting open

[39] Creative Commons is a type of copyright license that encompasses different versions of author-given authorizations to copy and distribute content.

[40] Mike Masnick, "Brazil's New Culture Minister Dumps Creative Commons From Ministry's Website," TechDirt (blog), February 11, 2011, http://www.techdirt.com/articles/20110209/04320213024/brazils-new-culture-minister-dumps-creative-commons-ministrys-website.shtml.

[41] Marília Macial, "Commons Strategy Group send an Open Letter to Brazilian President: Continue the most progressive culture policy in the world!" Cultura Livre, February 8, 2011, http://www.culturalivre.org.br/wp/en/2011/02/08/commons-strategy-group-send-an-open-letter-to-brazilian-president-continue-the-most-progressive-culture-policy-in-the-world/.

[42] Even under this more speech-protective framework, political speech by both the parties in power and those in the opposition has been restricted by the Electoral Judiciary. "TSE mantém multa por propaganda eleitoral antecipada em blog a favor de Dilma," Agência de Notícias da Justiça Eleitoral, March 17, 2011, http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1363510 [in Portuguese]; "TSE aplica multa a PSDB-MG por propaganda antecipada em favor de José Serra," Agência de Notícias da Justiça Eleitoral, November16, 2010, http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1345485 [in Portuguese].

[43] Rachel Librelon, "Proposta regula pré-campanha e propaganda eleitoral na internet," Agência Câmara de Notícias, May 13, 2011, http://www2.camara.gov.br/agencia/noticias/POLITICA/197033-PROPOSTA-REGULA-PRE-CAMPANHA-E-PROPAGANDA-ELEITORAL-NA-INTERNET.html [in Portuguese].

[44] "Candidatos só podem utilizar Twitter em campanha eleitoral a partir de 6 de julho" [Candidates can only user Twitter for electoral campaign starting July 6th], Tribunal Superior Eleitoral [Electoral Superior Court], March 2012, http://www.tse.jus.br/tse/noticias-tse/2012/Marco/candidatos-so-podem-utilizar-twitter-em-campanha-eleitoral-apos-6-de-julho.

[45] G1, "Documentos da época da ditadura militar estarão disponíveis na internet," June 14, 2011, http://g1.globo.com/jornal-da-globo/noticia/2011/06/documentos-da-epoca-da-ditadura-militar-estarao-disponiveis-na-internet.html.

access to public information and governmental data,[46] and projects tracking the quality and security of public schools through online platforms and mobile phones. A particularly important event was the enactment of the Right to Information Law, signed in November 2011.[47]

Brazilians use the web for political activism frequently and in a somewhat systematic, community-organized fashion. For example, on October 26, 2011, netizens launched the use of the hashtag "#QualidadeJa" (Quality Now) on Twitter in an effort to pressure the Brazilian federal telecom regulation authority (ANATEL) into changing the minimum actual speed required of broadband internet providers in advance of the authority's meeting on the matter the next day.[48] Despite pressure from telecom companies to maintain the status quo, the Twitter campaign managed to succeed in achieving its demands.[49]

VIOLATIONS OF USER RIGHTS

The constitution and federal law protect freedom of speech as well as cultural and religious expression. Specific laws also establish freedom of the press. However, some legislation limits these rights, and the constitution outlines a particularly complex legal framework, with a special effect on online speech.[50] For example, free expression of thought is ensured while anonymity is formally forbidden in the same paragraph. Bill 494/08, currently under consideration in the Senate as of mid-2012, aims to impose a series of obligations on ISPs, websites, and blogs to ensure cooperation with the police in pedophilia investigations.[51]

The Digital Crimes Bill,[52] first introduced in 2005 by Senator Eduardo Azeredo, has raised concerns that it would restrict technologies like open wireless networks, criminalize actions such as unlocking mobile phones, and oblige ISPs to record user information. Following public criticism of the draft—including a petition that gathered over 150,000 signatures—discussion surrounding the bill largely subsided in early 2010 and was substituted by a public

[46] See the website of the civil society group Fórum de Direito de Acesso a Informações Públicas [Forum for the Right of Access to Public Information] at http://www.informacaopublica.org.br/.
[47] "Brazil adopts access to information law," Article 19, November 22, 2011, http://www.article19.org/resources.php/resource/2862/en/brazil-adopts-access-to-information-law.
[48] Wikerson Landim, "Idec convida usuários a twittaço por banda larga de qualidade" [Consumer protection authority invites users to tweet in favor of broadband quality], Tecmundo, October 26, 2011, http://www.tecmundo.com.br/twitter/14737-idec-convida-usuarios-a-twittaco-por-banda-larga-de-qualidade.htm.
[49] The campaign succeeded in immediately changing the advertised speeds enforced by government from 10% to a minimum of 20% and established that it would rise to 30% in 2012 and 40% in 2013.
[50] An English translation of the constitution is available at http://www.v-brazil.com/government/laws/constitution.html.
[51] According to the Brazilian Senate website, PLS Senate Bill, #474, 2008 has been submitted to the Tariff Commission for review as of August 2012. See, http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=88695.
[52] Reporters Without Borders, "Legislators Urged to Oppose Cyber-crime Bill Likely to Threaten Online Free Expression," news release, July 23, 2008, http://en.rsf.org/brazil-legislators-urged-to-oppose-cyber-23-07-2008,27917.html.

debate over the Civil Rights Framework for the Internet, a bill that was introduced in Congress in August 2011. Lauded as a positive development for internet freedom in Brazil, the Framework was formulated through a multi-stakeholder consultation process and aims to guarantee access to the internet, safeguard freedom of speech and communication, protect privacy and personal data, and preserve net neutrality. The Framework also provides for intermediary liability only when service providers fail to comply with a court order to takedown or block access to content.[53] The bill will likely be passed in 2013.

Nevertheless, partly as a result of Brazil's experience with military dictatorship in its recent history, the tradition of guaranteeing freedom of expression is at times tenuous. This is illustrated by the Supreme Federal Court's two-decade delay in invalidating the press-muffling statute enacted during the repressive years that is now completely at odds with the 23-year old rights-oriented constitution. It also explains the ease with which online political speech was restricted prior to the 2008 elections.[54] Lastly, this tradition translates into the continuously aggressive practice of court orders issued to constrain the online speech of bloggers, journalists, and ordinary citizens. In one instance, blogger Noel Júnior had his home office equipment confiscated in October 2011 based on a court order. According to Júnior, the action was a result of critical commentary he posted on his blog about a company that provides services to the local city government.[55]

Bloggers also continue to face defamation lawsuits, sometimes for very high amounts. In February 2011, freelance journalist and blogger Carlos Santos based in Mossoró was ordered to pay roughly US$3,400 for posting three allegedly defamatory comments about the local mayor on his blog. Santos was also facing 27 other lawsuits and nine arrest orders for offending local officials.[56] In another case, a court in Rio de Janeiro found journalist Paulo Henrique Amorim guilty of defamation in September 2011 for criticizing a lawyer on his blog. Amorim was ordered to pay the lawyer more than US$54,000 in damages and to publish the outcome of the case on his blog.[57]

[53] Article 19, "Brazil: Civil Rights Framework for the Internet," legal analysis, July 26, 2012, http://www.article19.org/resources.php/resource/3389/en/brazil:-civil-rights-framework-for-the-internet.

[54] The court's resolution, No. 22.718, determined that electoral campaigns and advertisements could only be posted on a candidate's web page. It barred electoral campaigns from using such tools as Orkut, YouTube, e-mail, and text messaging, and prohibited them from buying advertising space on the internet. See Superior Electoral Tribunal, Resolution No. 22.718, available at http://www.tse.gov.br/internet/eleicoes/2008/pdf/r22718.pdf.

[55] Natalia Mazotte, "Brazilian blogger's computer equipment confiscated," Journalism in the Americas (blog), October 31, 2011, http://www.knightcenter.utexas.edu/blog/brazilian-bloggers-computer-equipment-confiscated.

[56] "Local Courts to Allow Multiple Lawsuits to be Used to Censor Journalists," Reporters Without Borders, February 25, 2011, http://en.rsf.org/brazil-local-courts-allow-multiple-25-02-2011,39629.html.

[57] Adriana Prado, "Blog post accusing lawyer gets Brazilian journalist $54,000 fine," Journalism in the Americas (blog), September 21, 2011, http://knightcenter.utexas.edu/blog/blog-post-accusing-lawyer-gets-brazilian-journalist-54000-fine.

Several legal provisions, including Article 57-D of the recently revised electoral law, place restrictions on anonymity. Users are generally required to register with their real names before purchasing mobile phones or opening a private internet connection, though the use of pseudonyms in discussion forums is common. Nevertheless, there have been no reports of such registration being employed to punish users for their online speech on political or social issues, largely because there are no government efforts to track these who participate in such discussions.

Surveillance of internet activities is not a major concern in Brazil, although government efforts to collect user data have increased in recent years, and illegal wiretapping remains a significant problem. Specific laws allow for surveillance, but only when authorized by judicial orders under due process. In August 2011 alone, the judiciary granted over 17,000 wiretaps, many of them to Voice over IP (VoIP) lines.[58] A special congressional commission was established in 2009 to analyze surveillance issues. The panel's report suggested that many individuals, politicians, and members of the police force should be investigated and condemned for illegal wiretapping. Privacy is also threatened by defamation suits and other such cases.

While Brazil's lead in Google's content removal ranking in 2011 does not fully transpose to the User Data Requests list, which documents government requests for user data from Google services, the country is one of the top contenders in this aspect as well, with 2,318 user data requests recorded in 2011.[59] This stems in part from the fact that judicial orders to remove content in private party disputes are often accompanied by a request to identify the publisher of the information.[60]

Some lawmakers have pushed for requirements to record internet communications from public access points such as LAN houses and to gather data from users to prevent crime. It would also allow LAN houses to avoid liability for acts committed by its users. Legislation of this kind already exists in states like São Paulo. In the state of Paraná, legislation in force since October 2009 requires LAN houses to register and file all their users. The law was passed after the police department released statistics showing that 30 percent of cybercrimes in the state had originated from LAN house computers. Most establishments in Paraná have failed to comply, however, alleging that they were not aware the legislation had been enacted and that the police had not enforced it.[61] On the federal level, draft legislation

[58] Revista Veja, "Tribunais autorizaram mais de 17.000 grampos telefônicos em agosto," Veja, September 19, 2011, http://veja.abril.com.br/noticia/brasil/justica-autorizou-17-mil-escutas-telefonicas-em-agosto.
[59] Google, "User Data Requests," Transparency Report (Mountain View, CA: Google, 2011), accessed February 7, 2012, http://www.google.com/transparencyreport/governmentrequests/userdata/.
[60] O'Brien, "Is Brazil the Censorship Capital of the Internet? Not Yet."
[61] "Lan houses ignoram lei e não cadastram clients," Gazeta do Povo, March 18, 2010, http://www.gazetadopovo.com.br/vidaecidadania/conteudo.phtml?id=983853.

introduced in 2004 that was approved by the House of Representatives in 2011 and is currently in the Senate as of early 2012, would regulate LAN houses as "multi-purpose entities of special interest for digital inclusion" and require them to register all users.[62]

While traditional media workers are often victims of violence and death threats in Brazil,[63] such attacks have yet to extend significantly to online journalists, bloggers, and commentators. There were no reports of violence or extralegal intimidation against such groups in 2011.

Cyberattacks are a large problem in Brazil, with targets ranging from online banking sites to energy plants.[64] An increasing amount of hacker instructional material is produced in Brazil, including information on how to conduct illegal mobile phone wiretaps or hack passwords.[65] In June 2011, the hacker group LulzSec undertook an attack of the Brazilian presidency website and several other governmental webpages, in what was seen as the largest cyberattack in the country to date and a part of a larger effort to disrupt governmental websites in several countries. In the endeavor, the group got a hold of allegedly personal data from São Paulo's mayor and President Dilma Rousseff.[66] In early 2012, the hacker group Anonymous also made a significant impact by launching distributed denial-of-service (DDos) attacks against the websites of different Brazilian banks,[67] including the largest in the country, Banco do Brasil. The attacks have been described as political manifestations against corruption and inequality in Brazil.[68]

[62] Draft Legislation no. 4361/2004, proposed by representative Vieira Reis, accessed February 7, 2012, http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=268907.

[63] Maira Magro, "Police Accuse Three Men of Torturing Editor in Northeast Brazil," Journalism in the Americas, June 10, 2010, http://knightcenter.utexas.edu/blog/?q=en/node/7449; Maira Magro, "Reporter Who Exposed Death Squad in Brazil Receives Threats," Journalism in the Americas, May 25, 2010, http://knightcenter.utexas.edu/blog/?q=en/node/7300; Maira Magro, "Escaped Killer of Brazilian Journalist Turns Himself In," Journalism in the Americas, May 25, 2010, http://knightcenter.utexas.edu/blog/?q=en/node/7302.

[64] Dmitry Bestuzhev, "Brazil: A Country Rich in Banking Trojans," Securelist, October 16, 2009, http://www.securelist.com/en/analysis/204792084/Brazil_a_country_rich_in_banking_Trojans.

[65] For examples of tools and hardware for "do-it-yourself wiretapping," see ItecDiffusion.com at http://www.itecdiffusion.com/PT/escuta_telemovel.html; See for example Apostila Hacker [Hacker Toolkit], at http://www.apostilahacker.com.br/.

[66] Angelica Mari, "Brazil suffers its biggest cyber attack – yet," Itdecs.com, June 23, 2011, http://itdecs.com/2011/06/brazil-suffers-its-biggest-cyber-attack-yet/.

[67] Kenneth Rapoza, "Hacker Group 'Anonymous' Gun For Brazil Banks; Itau Internet Banking Briefly Shut Down," Forbes, February 8, 2012, http://www.forbes.com/sites/kenrapoza/2012/01/30/hacker-group-anonymous-gun-for-brazil-banks-itau-internet-banking-briefly-shut-down/.

[68] "Hackers attack website of Brazil's largest state-run bank," Associated Press, February 1, 2012, http://finance.yahoo.com/news/Hackers-attack-Brazil-largest-apf-847070693.html.

BURMA

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	23	22
Limits on Content (0-35)	29	23
Violations of User Rights (0-40)	36	30
Total (0-100)	**88**	**75**

* 0=most free, 100=least free

POPULATION: 55 million
INTERNET PENETRATION 2011: 1 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

While the military junta that ruled Burma for decades was interested in expanding information and communication technologies (ICTs) for business and propaganda purposes, it also made aggressive attempts to restrict access to digital media and control online content. Elections in November 2010 changed this dynamic. Though widely condemned as flawed, the polls brought into office a nominally civilian government, led by former general Thein Sein and supported by a military-backed party, in March 2011. Since then, the political landscape has opened somewhat, with positive implications for internet freedom. Previously censored news websites have been unblocked, citizens imprisoned for their online activities have been released, and opposition political parties have been able to use online tools to mobilize supporters.

Nevertheless, significant obstacles to greater internet freedom persist. Harsh media laws remain in effect and could be used at any time to punish a wide range of online expression, the technical censorship system appears intact, and some opposition blogs continue to be blocked. Consumer prices for ICTs are still among the highest in the world. Meanwhile, even as some members of the government and private sector begin to explore reforms to the telecommunications sector, new challenges have emerged, including weak coordination between different agencies and resistance from the military and government cronies who have lucrative vested interests in retaining the status quo.
As such, the state continues to dominate the telecommunication sector, with few signs of upcoming fundamental reform. Although mobile phone use and the presence of cybercafes expanded in 2011, the quality of service for phones and internet connectivity is at times

excruciatingly poor and only a small percentage of the population has regular access to ICTs, particularly in rural areas.[1] Where network infrastructure has improved, it has been biased towards the business sector or preparation for international events Burma is scheduled to host, such as the summit of the Association of Southeast Asian Nations (ASEAN) in 2014.

The state-owned Myanmar Post and Telecommunications (MPT) company launched the first official email service in November 1997. The 2002 establishment of the first private internet service provider (ISP), Bagan Cybertech, helped to increase the number of users in the country, though the company was later taken over by the junta. The government's first attempt to restrict internet freedom was through the 1996 Myanmar Computer Science Development Law,[2] which made possession of an unregistered computer modem and connection to unauthorized computer networks punishable by up to 15 years in prison.[3] Other laws passed later have reinforced a climate of fear and self-censorship surrounding online interactions, though in 2011, internet users pushed the boundaries of permissible speech and mobilized successful campaigns for political or social change.

OBSTACLES TO ACCESS

Poor infrastructure, the economic interests of state-owned companies, and widespread poverty are among the key factors that continue to limit Burmese citizens' internet access and usage. Over the past two years, the number of internet users has notably increased, though it remains only a small fraction of Burma's population of 54 million people. The precise scale of usage is difficult to ascertain, as independent surveys are not available and government statistics lack credibility. Nevertheless, according to government sources and a Burmese telecommunications expert, there were an estimated 500,000 internet users as of early 2012, amounting to almost 1 percent of the population;[4] this was an increase from 110,000 (or 0.2) percent in 2009.[5]

[1] "Internet cafés must reapply for a business license," Mizzima, May 27, 2011, http://www.mizzima.com/business/5333-internet-cafes-must-reapply-for-a-business-license.html.

[2] In June 1989, the military junta changed the English rendering of the country's name from Burma to Myanmar. Democracy activists and their foreign supporters, including the U.S. government, have continued using Burma.

[3] *Computer Science Development Law*, September 20, 1996, Chapter X, https://www.myanmarisp.com/ICTnews/law10-96.

[4] In February 2012, MCPT Minister Thein Tun reported to the Third Regular Session of Parliament that internet users increased to 500,000 in 2011-2012. "Third regular session of First Pyidaungsu Hluttaw continues," *The New Light of Myanmar* XIX, no. 287 (February 2, 2012), http://www.burmalibrary.org/docs13/NLM2012-02-02.pdf. Kyaw Soe, head of the Burmese Telecom Training school also said at the Burmese Economic conference held on May 19, 2012 that there were 500,000 internet users in Burma. Author's interview with conference attendee, June 25, 2012. The International Telecommunications Union cites a similar estimate in its 2011 statistics, likely drawn from government sources: International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[5] In Soo Kang, "Strategies for Operating National CERT of Myanmar," ITU-ASEAN Subregional CSIRT/CIRT/CERT Workshop for CLMV, November 29 to December 1, 2011, Yangon, (Myanmar Korea Information Society Development Institute - KISDI) http://www.itu.int/ITU-D/asp/CMS/Events/2011/CIRTWkshp/S8_Dr_Insoo_Kang.pdf; "Myanmar introduces 1st

The price of a private internet connection is prohibitively expensive in a country where an estimated 26 percent of the population lives below the poverty line,[6] though there is significant regional variation.[7] According to the International Monetary Fund, the gross domestic product per capita was US$821 for 2011.[8] By comparison, the installation cost and fees for broadband access range from US$625 to US$1,500 depending on the speed and connection method.[9] For example, the monthly fee for ADSL service from the two main internet service providers (ISPs) ranges from US$35 for speeds of 128 Kbps to US$250 for 2 Mbps.[10] This is in addition to installation costs of US$625 and the requirement to have a landline, a rare commodity in Burma.[11] As a result of these barriers, according to the International Telecommunications Union (ITU), the fixed broadband subscription rate was only 0.06 percent in 2011, a figure that did not significantly change from the previous year.[12] In the process of registering an internet connection, consumers must present their national ID, as well proof of police clearance and a personal affidavit affirming they are not involved in political activities.

Because of such economic and regulatory barriers, most users rely on cybercafes, where access typically costs about 200 to 400 kyats (US$0.25 to US$0.50) per hour in major cities and about 500 to 600 kyats (US$0.60 to US$0.80) per hour in provincial towns, slightly less than two years ago.[13] From mid-October 2011 until January 2012, internet connection speeds slowed dramatically to the point that in provincial towns, it took 45 to 90 minutes to

telecommunication service call center," Xinhua, December 21, 2011, http://news.xinhuanet.com/english/sci/2011-12/21/c_131320009.htm.

[6] "Cooperative societies will be formed with bottom up initiative, not with top down policy," *The New Light of Myanmar*, June 20, 2011, http://www.myanmargeneva.org/11nlm/jun/n110621.htm. "Myanmar: Country Profile: Human Development Indicators," United Nations' Human Development Index, accessed January 2, 2011, http://hdrstats.undp.org/en/countries/profiles/MMR.html.

[7] For example, Chin State has the highest poverty level, at more than 70 percent. These figures are likely to be conservative, as they are based on data collected before significant increases in fuel prices in October 2005 and August 2007, and an inflationary public sector salary hike in April 2006. Charles Petrie, *End of Mission Report: UN Resident and Humanitarian Coordinator*, UNDP Resident Representative for Myanmar, 2003–2007, April 1, 2008, http://www.pyinnya.com/wp-content/uploads/2008/06/end-of-mission-report-by-charles-petrie-april-2008.pdf.

[8] International Monetary Fund, "World Economic Outlook Database," International Monetary Fund, April 2011, http://www.imf.org/external/pubs/ft/weo/2011/01/weodata/weorept.aspx?sy=2009&ey=2016&scsm=1&ssd=1&sort=country&ds=.&br=1&pr1.x=88&pr1.y=5&c=518&s=NGDPDPC%2CPPPPC&grp=0&a=#cs1.

[9] Interviews with local journalists who cover the IT sector, December 12, 2011. See also "WiMax Installation Charges Change from FEC to Kyat," *Popular Journal* [in Burmese],accessed January 2, 2012, http://popularmyanmar.com/mpaper/archives/28610

[10] The exchange rate fluctuated throughout 2011, varying from 750 to 860 kyats per US dollar. This paper uses an average of 800 kyats per dollar for consistency.

[11] "Internet Cafes Expect Lower Monthly Fee as the Number of Users Dwindles," *Popular Journal* [in Burmese], accessed January 4, 2012, http://popularmyanmar.com/mpaper/archives/29866.; "Initial Installation Cost Reduced for Wimax Internet Service," *Popular Journal* [in Burmese], http://popularmyanmar.com/mpaper/archives/32988.

[12] International Telecommunication Union, "Fixed Broadband Subscriptions, 2000-2010 Data," ITU, Updated in December 2011, http://www.itu.int/ITU-D/ict/statistics/index.html.

[13] "Declines in Cyber Cafe Users and Hourly Fee due to Slow Connection Speed," *Popular Journal* [in Burmese], accessed January 7, 2012, http://popularmyanmar.com/mpaper/archives/29371.

open a single webpage.[14] The government attributed the slowdown to a disruption in the SEA-ME-WE-3 fiber-optic cable that is the country's main source of internet bandwidth, an assessment that independent observers confirmed.[15] As a result, many cybercafe users shifted to playing games rather than using the internet.[16] Periodic power outages also continued, reflecting Burma's general lack of electricity and poor infrastructure. Officials from the state-owned MPT have pledged to increase internet connection speeds in time for the Southeast Asia Games in 2013 that Burma is scheduled to host. Chinese firms will reportedly provide technical support for this upgrade and broader ICT security efforts.[17] In November 2011, Chinese state-run media reported that an agreement had been signed for Beijing Xinwei Telecom Technology to supply wireless broadband technology across Burma within five years.[18]

Mobile phone penetration is higher than internet use and has grown dramatically since early 2011, though it remains concentrated in large cities like Rangoon and Mandalay. Figures vary as to the precise number of subscribers. According to the ITU, there were 1.2 million mobile phone subscriptions at the end of 2011 (2.5 subscriptions per 100 inhabitants),[19] double the figure from 2010.[20] By comparison, the government reported that 2.8 million mobile phones were in use as of February 2012, which would be a penetration rate of about 5 percent.[21] In April 2011, the government announced a project to expand the number of mobile phone lines to 30 million over the next five years, with the aim of adding four million new connections within the first year.[22] In an effort to realize these goals, in March 2012, the Ministry of Communications, Posts and Telegraphs (MCPT) announced that the cost of a SIM card would be halved, dropping from 500,000 kyats (US$625) to between

[14] Interviews with local internet users in Hinthada township, Irrawaddy Region, and in Prome, Pegu Division, January 7-8, 2012.
[15] "Internet Fiber Disruption be Repaired within this Month," [in Burmese] Popular Journal, November 11, 2011, http://popularmyanmar.com/mpaper/archives/31653.; Sai Zom Hseng, "Burma's Internet, Newly Opened, Slows to a Crawl," The Irrawaddy, November 3, 2011, http://www2.irrawaddy.org/article.php?art_id=22379&Submit=Submit.
[16] "Internet Cafes have to Rely on the uses of Pfingo and Games," [in Burmese] Popular Journal, accessed January 7, 2012, http://popularmyanmar.com/mpaper/archives/30157.
[17] "China Supports Burmese Internet Security," [in Burmese] Popular Journal, accessed January 8, 2012, http://popularmyanmar.com/mpaper/archives/33163.
[18] "Sino-Myanmar companies cooperate in telecom technology," The People's Daily Online English, November 13, 2011, http://english.peopledaily.com.cn/90778/7643265.html.
[19] International Telecommunications Union, "Mobile-cellular telephone subscriptions 2006-2011," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/CellularSubscribersPublic&ReportFormat=HTML4.0&RP_intYear=2011&RP_intLanguageID=1&RP_bitLiveData=False; "Myanmar (Burma) Telecoms Mobile and Internet," BuddeComm, accessed January 2, 2012, http://www.budde.com.au/Research/Myanmar-Burma-Telecoms-Mobile-and-Internet.html.
[20] International Telecommunications Union, "ICT Statistics 2009—Fixed Telephone Lines," http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#.
[21] "Myanmar Introduces 1st Telecommunication Service Call Center," Xinhua, December 12, 2012, http://news.xinhuanet.com/english/sci/2011-12/21/c_131320009.htm; As of February 2012, the MCPT newsletter reported that there were 2.8 million mobile phone users in Burma. *MCPT Newsletter* [in Burmese], February 29, 2012, http://www.mcpt.gov.mm/sites/default/files/pdf/1-1%20Smart-News-Journal%20.pdf.
[22] "Myanmar to install more mobile phone lines within 5 years," The Financial Express, April 23, 2011, http://www.thefinancialexpress-bd.com/more.php?news_id=11101&date=2011-04-24.

200,000 and 250,000 kyats (US$250-US$312), though even this reduced price remains beyond the reach of most Burmese.[23]

Internet access from mobile devices remains extremely limited. In early 2011, some mobile phone providers obtained permission to offer mobile internet access via prepaid cards, but the authorities interrupted this service for GSM users in July and December 2011.[24] In practice, mobile internet connectivity barely functions even in Rangoon.[25]

The government retains control over the country's international connection to the internet. There are two main ISPs: the government-owned MPT and the military-owned Yatanarpon Teleport (YTP).[26] In December 2007, the government opened the Yatanarpon Cyber City, where YTP is based.[27] According to several reports, the authorities restructured the ISP system in October 2010, dividing it into two main networks: the state-owned MPT ISP and a newly-created Ministry of Defense (MoD) ISP.[28] Under the new arrangement, the YTP (serving civilian users) and a newly-established Naypyitaw ISP (serving most government ministries) connect to the international internet via MPT. Meanwhile, the MoD ISP solely serves users from the Ministry of Defense. Such architecture would enable the government to cut off access for civilians, including government employees, at times of political turmoil while keeping the military's connection intact. According to Reporters Without Borders, the arrangement may also facilitate monitoring and hacking of civilian users without risking security breaches for military accounts.[29]

The MPT retains control over the mobile phone market, but grants distribution rights to a select set of trusted companies, either military-linked like Yantanarpon, or privately owned but closely linked to the government, like ELite, a subsidiary of Htoo Trading Company

[23] "Burmese SIM Card Price Slashed by Half," The Irrawaddy, March 6, 2012, http://www2.irrawaddy.org/article.php?art_id=23158.
[24] "CDMA 450MHz Not Allowed Internet Uses," [in Burmese] Popular Journal, accessed January 8, 2012, http://popularmyanmar.com/mpaper/archives/32811 .
[25] Interview with Rangoon phone users, January 2, 2012.
[26] Nilar Aye, "Current Status of PKI Development in Myanmar," The Workshop on CA-CA Interoperability Framework in ASEAN August 5-6, 2010, http://www.gits.net.th/Documents/CACA_Interoperability_ASEAN/CA_Workshop_2_8_10_Myanmar_updated.pdf (site discontinued). Xinhua News, "Myanmar Internet link continues to meet with interruption," People's Daily Online English, November 3, 2010, http://english.peopledaily.com.cn/90001/90781/90877/7187341.html.
[27] Ye Kaung Myint Maung, "Nation's First Cyber City Takes Shape," *The Myanmar Times*, December 24–30, 2007, http://mmtimes.com/no398/n001.htm.
[28] Author's interview with an official at the Information Ministry who asked to remain anonymous, July 27 and December 30, 2010.; Reporters Without Borders, *National Web Portal Development or Repression?*, November 2010, http://en.rsf.org/IMG/pdf/rap_birmanie-2.pdf.
[29] Author's interview with an official at the Information Ministry who asked to remain anonymous, July 27 and December 30, 2010.; Reporters Without Borders, *National Web Portal Development or Repression?*, November 2010, http://en.rsf.org/IMG/pdf/rap_birmanie-2.pdf.

owned by tycoon Tay Za.[30] Smaller firms seeking retail vending rights must purchase equipment from these larger distributors. In an example of the difficulties facing those wishing to offer lower prices, in January 2012, the private company Shwe Pyi Ta Khun announced it was seeking permission from the President's Office to sell a SIM card for 5,000 kyat (US$6) as part of the president's poverty reduction initiative. The news that phones would soon be affordable to average citizens was greeted with enthusiasm. Within a week, however, MCPT officials rejected the proposal, stating that the plan was not possible under existing regulations and without MCPT approval, and that more time would be needed to upgrade the country's mobile phone networks.[31] Some observers suspected the actual reason was reluctance to allow a private mobile phone operator.[32] The rejection sparked a small leaflet campaign calling for cheaper SIM cards; 11 people who took part in the protest were briefly detained for questioning.[33] The incident illustrated the MCPT's reluctance to allow meaningful liberalization, as well as the lack of coordination between government agencies and the influence that those with a vested financial interest in retaining the status quo have on ICT policy.[34]

Despite the government's control and the above-mentioned slowdown, there have been no credible reports of politically motivated disruptions to internet connectivity in 2011 and early 2012, unlike in previous years. Rather, the disruptions that occurred appeared due to technical problems.[35] In addition, the Yatanarpon Teleport ISP was more transparent than in the past in explaining the cause of the slowdown to customers.[36]

Alongside the unblocking of international and exile news outlets in September 2011 (see "Limits on Content"), the government also unblocked access to the video-sharing website YouTube for the first time in several years.[37] Burmese users thus have access to most Web 2.0 applications. At the same time, the government restricts mobile phones from receiving text messages from outside the country. This creates an obstacle for those wishing to set up a Gmail account or recover a lost password, as Google typically sends such information via

[30] "30 Million New GSM Mobile Phone Lines," Myanmar Business Network, http://www.myanmar-business.org/2011/05/30-million-new-gsm-mobile-phone-lines.htm (site discontinued).
[31] Shwe Aung, "Not Possible for 5,000 kyats per Sim Card, says the MPT official," [in Burmese] Democratic Voice of Burma, January 10, 2012, http://burmese.dvb.no/archives/19809.
[32] Ba Kaung, "Burmese SIM Card Provider Challenges Monopolistic State Interests," The Irrawaddy, February 15, 2012, http://www.irrawaddy.org/archives/77.
[33] Hpyo Wai Tha, "Burmese SIM Card Price Slashed by Half," The Irrawaddy, February 15, 2012, http://www2.irrawaddy.org/article.php?art_id=23158; Zarni Mann, "11 'SIM Card' Campaigners Detained for Questioning in Rangoon," The Irrawaddy, February 29, 2012, http://www.irrawaddy.org/archives/464.
[34] Ba Kaung, "Burmese SIM Card Provider Challenges Monopolistic State Interests," The Irrawaddy, February 15, 2012, http://www.irrawaddy.org/archives/77.
[35] Sai Zom Hseng, "Burma's Internet, Newly Opened, Slows to a Crawl," The Irrawaddy, November 3, 2011, http://www2.irrawaddy.org/article.php?art_id=22379&Submit=Submit.
[36] Interview with two cybercafe owners and three household subscribers in Rangoon, December 28-29, 2011.
[37] Qichen Zhang, "Burma's Government Unblocks Foreign Websites Including YouTube," OpenNet Initiative, September 20, 2011, http://opennet.net/blog/2011/09/burmas-government-unblocks-foreign-websites-including-youtube.

text message. A number of small businesses opened to resolve this problem for users in exchange for a small fee.[38]

In a negative development, in March 2011, the MCPT issued a directive banning the use of Voice over Internet Protocol (VoIP) services for making international calls, including applications such as Skype, Gtalk, Pfingo, VBuzzer, and VZO.[39] Those violating the regulation may face penalties ranging from fines to confiscation of property to five years imprisonment.[40] In April 2011, cybercafe owners reported visits by government bureaucrats to check if they were still providing VoIP services, which many were, but no arrests were reported.[41] The measure is apparently aimed at protecting revenue earned from international phone calls made via the network of the state-owned telecom[42] or via a new government-sponsored VoIP program called Ytalk launched in late 2011.[43] In recent years, VoIP has become a vital channel for both business and personal communication, particularly families with a member working overseas. As of May 2012, the ban remained in effect, with the MCPT issuing an additional warning in its April newsletter.[44] Two months after passage of the VoIP restrictions, the ministry also banned the use of USB sticks, CDs, floppy disks and other external data storage devices in cybercafes, and threatened heavy penalties if the prohibitions are ignored.[45]

There are a number of state institutions tasked with ICT development and management, including the Myanmar Computer Science Development Council, the e-National Task Force (e-NTF), the Myanmar Computer Federation (MCF), and three associations—the Myanmar Computer Professionals' Association (MCPA), the Myanmar Computer Industry Association (MCIA), and the Myanmar Computer Enthusiasts' Association (MCEA). These entities are not particularly active or exist only on paper. During the junta's rule, the authorities used intelligence agencies and the Information Ministry to implement arbitrary and ad hoc censorship decisions. Under the civilian government, the MCPT has demonstrated more authority on telecommunications issues. Nevertheless, there were various incidents in 2011

[38] Tun Tun, "Gmail for Sale," Mizzima, September 12, 2011, http://www.mizzima.com/business/5915-gmail-for-sale.html.
[39] Htet Aung, "Junta Make Internet Phones Illegal," The Irrawaddy, March 16, 2011, http://www2.irrawaddy.org/article.php?art_id=20949&Submit=Submit; Aung Myat Soe, "Government bans Internet overseas calls," Mizzima, March 16, 2011, http://mizzimaenglish.blogspot.com/2011/03/government-bans-internet-overseas-calls.html.
[40] "Action can be Taken against VoIP calls," *Internet Journal* Vol 12, Number 12, March 24, 2011.
[41] Nayee Lin Latt, "Burmese Authorities Crack Down on VoIP Calls," The Irrawaddy, April 7, 2011, http://www2.irrawaddy.org/article.php?art_id=21092&Submit=Submit.
[42] Aung Myat Soe, "Government bans Internet overseas calls," Mizzima, March 16, 2011, http://mizzimaenglish.blogspot.com/2011/03/government-bans-internet-overseas-calls.html.
[43] Interviews with two Burmese IT experts and four journalists, June 20- 25, 2012.
[44] *Smart News* [in Burmese], Vol 1, no. 4, April 25, 2012, http://www.mcpt.gov.mm/sites/default/files/pdf/1-6-smart-news.pdf.
[45] Shwe Aung and Francis Wade, "Internet cafes ban CDs, USB drives," Democratic Voice of Burma, May 16, 2011, http://www.dvb.no/news/internet-cafes-ban-cds-usb-drives/15659.

that point to a lack of coordination between different government agencies in terms of policy formulation, implementation, and enforcement.

LIMITS ON CONTENT

For years, the Burmese government systematically restricted access to political websites and online media outlets run by the Burmese exile community. This changed in September 2011 when the government lifted the blocks not only on foreign news sources such as Reuters, the British Broadcasting Corporation (BBC), Radio Free Asia, and the *Bangkok Post*, but also on major exile media sites such as the *Irrawaddy*, *Mizzima*, and Democratic Voice of Burma; the latter had long been on the regime's blacklist for their critical reporting.[46] The websites of international human rights groups were also unblocked.

This opening was followed by other steps that indicated a decline in the government's hostility towards independent media, online and offline, a change that seemed unimaginable a few years ago. A long-standing propaganda campaign in state-run media was discontinued in August 2011, visas were granted to exile journalists to visit, and a range of news outlets participated in government press conferences and media-related policy discussions in early 2012.[47] Despite these notable positive developments, the impact of the new opening has been tempered by the still low penetration rate and an atmosphere of uncertainty. In particular, harsh laws used to sentence bloggers and online journalists to long prison terms remain in effect and could be employed at any time to punish those accessing, disseminating, or providing information to the unblocked news outlets (see "Violations of User Rights"). As a result, self-censorship remains common among internet users, though less so than in the past.

The Burmese government retains the technological capability to reinstitute strict censorship at any time and some blogs of regime critics reportedly remain inaccessible. In November 2011, Citizen Lab, a research center at the University of Toronto, published evidence indicating that the technology used to filter and monitor online communications in Burma includes devices produced by the U.S.-based firm Blue Coat Systems, in possible violation of U.S.-imposed sanctions.[48] Citizen Lab's initial testing was conducted in August 2011, prior

[46] AP, "Myanmar authorities unblock some banned websites," Yahoo! News, September 16, 2011, http://news.yahoo.com/myanmar-authorities-unblock-banned-websites-050311492.html; Qichen Zhang, "Burma's Government Unblocks Foreign Websites Including YouTube," OpenNet Initiative, September 20, 2011, http://opennet.net/blog/2011/09/burmas-government-unblocks-foreign-websites-including-youtube.

[47] Joseph Allchin, "Govt drops DVB 'killer media' slogan," Democratic Voice of Burma, August 17, 2011, http://www.dvb.no/news/govt-drops-dvb-%E2%80%98killer-media%E2%80%99-slogan/17085.

[48] "Behind Blue Coat: Investigations of commercial filtering in Syria and Burma," The Citizen Lab, November 9, 2011, http://citizenlab.org/2011/11/behind-blue-coat/?utm_source=Media+Mailing+List&utm_campaign=3881bed4a1-Citizen_Lab_research_report_Behind_Blue_Coat_&utm_medium=email.; Andy Greenberg, "Researchers Spot Blue Coat Web

to the above-mentioned unblocking of websites. As expected, researchers found that the Yatanarpon ISP blocked numerous websites, including independent news outlets and content categorized by Blue Coat as pertaining to pornography, LGBT issues, and nudity. An update to the report indicated that as of October 2011, after the news websites were unblocked, some Blue Coat technology remained in place. Specifically, during the severe connectivity problems encountered that month (see "Obstacles to Access"), the error notification message that users in Burma received was clearly generated by a Blue Coat device.[49]

In another indication that the government has not entirely abandoned internet censorship, a small number of politically sensitive blogs, including that of Moethee Zun, one of the 1988 protest leaders living in exile, remained blocked as of May 2012.[50] The reason for their continued blocking remained unclear, but some observers believed it was because they tend to post embarrassing revelations of government corruption and complaint letters from civil servants about their superiors.

For websites that are not blocked, the Press Scrutiny Board has been known to order news outlets to delete articles that have been barred from publication in hard copy versions. When the weekly journal *Popular News* reported that five ministers had been fired in January 2012, the authorities called the journal within one hour of the information being posted and requested its removal.

In 2010, blogging appeared to be the fasted growing aspect of Burmese internet use.[51] Throughout 2011, however, social media tools gained prominence, including Facebook, Twitter, Friendfinder, Netlog, and the recently launched Google+. Facebook is the most popular of these tools, thanks to the ease with which users can share information, initiate collective action on social and political issues, and obtain news updates from exile media outlets (when their websites were blocked). Although no precise statistics are available on the number of Facebook users, one expert estimated that 80 percent of the country's internet users had a Facebook account, amounting to hundreds of thousands of people.[52]

Control Gear In Another Repressive Regime: Burma," Forbes, November 9, 2011, http://www.forbes.com/sites/andygreenberg/2011/11/09/researchers-spot-blue-coat-web-control-gear-in-another-bad-regime-burma/.

[49] "Behind Blue Coat: An update from Burma," The Citizen Lab, November 29, 2011, https://citizenlab.org/2011/11/behind-blue-coat-an-update-from-burma/.

[50] Users seeking to access his blog received a message of: "Access to the requested URL has been denied… To have the rating of this webpage reevaluated, please contact your web moderator." Interviews with six Internet users in Rangoon, two users from Mandalay, and one user from Prome Township, January 10-12, 2012.

[51] See *Freedom on the Net 2011*.

[52] Based on an estimated 500,000 internet users in Burma. Tun Tun, "Facebook's mini-revolution in Burma," Mizzima, August 17, 2011, http://www.mizzima.com/edop/features/5786-facebooks-mini-revolution-in-burma.html.

A turning point in the volume, intensity, and impact of public expression via Facebook was the controversy surrounding the Myitsone Dam. Under construction by China's state-owned China Power Investment Corporation (CPI), it was part of a multi-billion dollar project to build dams at eight locations along the Irrawaddy River, a crucial resource for Burmese people's livelihood and a national cultural symbol. The Myitsone Dam, intended to be the largest of the eight, was being constructed less than 100 kilometers (about 60 miles) from a major tectonic fault line. Experts warned that an earthquake could cause the dam to collapse, with devastating consequences. This sparked intense public outcry. When local media outlets and public figures, including National League for Democracy (NLD) leader Aung San Suu Kyi, criticized the project in August 2011, Facebook users shared news links, circulated video files, and posted comments. This information was then republished on popular blogs. Local private weeklies also adopted a practice of posting politically sensitive news online rather than submitting it to the censorship board for prior approval, as is required for print publication. This not only enabled readers to access uncensored breaking news, but also allowed them to post comments in response. These mutually reinforcing interactions created an emboldened online community and collective "Save the Irrawaddy" campaign. Subsequently, at the end of September 2011, President Thein Sein conceded to public demands by announcing a temporary suspension of the project. Despite this vibrancy, however, using Facebook for mobilization remains risky and could potentially draw a prison term.

Several ministries, including the Ministry of Information, have their own websites and blogs.[53] Several other blogs have also emerged—such as *Myanmar Express*[54]—that have launched malicious attacks against the opposition and Aung San Suu Kyi, including spreading damaging falsehoods. Many observers believe military hardliners may be behind the blog, as it has also criticized reformist President Thein Sein.

Besides employing online tools for social and political mobilization, users have organized gatherings, with government permission, to share general ICT-related knowledge. In February 2012, the third BarCamp in Burma was held. In a notable development, Aung San Suu Kyi attended as a guest of honor and spoke at the gathering, without encountering any interference from the authorities.[55] Many cybercafe owners provide assistance to their customers on how to open an email account, circumvent censorship, or use VoIP sites, though the authorities have banned them.

[53] See for example: Kyee Saytaman's Blog, http://kyeesaytaman.blogspot.com/.
[54] Myanmar Express, http://www.myanmarexpress.net/.
[55] Info.NLD, "Daw Aung San Suu Kyi Opened BarCamp Yangon 2012," National League for Democracy, February 14, 2012, http://www.nldburma.org/social-activity/education/477-daw-aung-san-suu-kyi-opened-barcamp-yangon-2012.html.; Jeremy Wagstaff, "Slow Connection: Myanmar faces an IT logjam," Firstpost Business, March 3, 2012, http://www.firstpost.com/business/slow-connection-myanmar-faces-an-it-logjam-232895.html.

VIOLATIONS OF USER RIGHTS

Although the new civilian-led government of President Thein Sien, who took office in March 2011, has introduced unprecedented improvements to the internet freedom landscape, the reforms lack a firm legal foundation. As a result, users remain at risk of prosecution and imprisonment under the repressive laws enacted by the previous military junta, and a small number of individuals imprisoned for online activities remain in custody.

The current constitution, drafted by the military-led government and approved in a flawed 2008 referendum, does not guarantee internet freedom. It simply states that every citizen may exercise the rights "to express and publish their convictions and opinions," but only if they are "not contrary to the laws, enacted for Union security, prevalence of law and order, community peace and tranquility or public order and morality."[56] In addition, three laws have been promulgated regarding ICTs: the Computer Science Development Law (1996), the Wide Area Network Order (2002), and the Electronic Transactions Law (2004).[57] The Printers and Publishers Registration Act (1962) is used to censor traditional media. These regulations are broadly worded and open to arbitrary or selective enforcement, generating a climate of fear. In February 2012, the government postponed introduction to parliament of a new media law, which has reportedly been drafted by the Ministry of Information but not yet been made public. According to one ministry official, it is expected to pass in 2012, but does not include changes to legislation related to electronic media.[58]

The most notorious and frequently used criminal law is the Electronic Transactions Law (ETL). Under Section 33 of the law, internet users face prison terms of 7 to 15 years and possible fines for "any act detrimental to" state security, law and order, community peace and tranquility, national solidarity, the national economy, or national culture.[59] This may include any act of "receiving or sending and distributing any information relating to" the above broadly defined proscribed areas. In August 2011, state-run media explicitly warned that the ETL could also apply to those who defame individuals and organizations on Facebook, and draw sentences of up to five years in prison.[60]

[56] *Burma Constitution* (English version), accessed December 20, 2011, http://burmadigest.info/wp-content/uploads/2008/11/myanmar_constitution-2008-en.pdf.
[57] Burma Lawyers' Council, *Myanmar Law (1988–2004)*, accessed December 20, 2011, http://www.blc-burma.org/html/Myanmar%20Law/Indexs/lr_law_ml_index.html.
[58] "New Burmese media law postponed," Mizzima News, February 6, 2012, http://www.mizzima.com/gallery/media-alert/6541-new-burmese-media-law-postponed.html.
[59] Electronic Transactions Law, *State Peace and Development Council Law No. 5/2004*, accessed December 20, 2011, http://www.blc-burma.org/html/myanmar%20law/lr_e_ml04_05.htm.
[60] Francis Wade, "Prison threat for Facebook 'defamers'," Democratic Voice of Burma, August 3, 2011, http://www.dvb.no/news/prison-threat-for-facebook-'defamers'/16865.

Throughout 2011, several internet users were sentenced under the ETL, though all were subsequently freed as part of a large-scale prisoner release in January 2012. Sithu Zeya, who was sentenced to eight years in prison in 2010 for taking pictures in the aftermath of a bomb blast in Rangoon and for his affiliation with an exiled media outlet, was brought before a judge again in August 2011. He was handed an additional 10-year prison sentence for violating Article 33 of the ETL for the same act.[61] According to his mother, Zeya was beaten during interrogations.[62] Nay Myo Zin, a former military officer and volunteer for an NLD-affiliated blood donation group, was arrested in April 2011. In August 2011, he was charged with violating the ETL and sentenced to 10 years in prison for allegedly writing articles online that were critical of the military, though under a pseudonym.[63]

Both Sithu Zeya and Nay Myo Zin were released in January 2012, along with hundreds of other political prisoners including bloggers Nay Phone Latt, Win Zaw Naing, and Hla Hla Win, whose cases were reported in *Freedom on the Net 2011*. Though celebrated, the releases were bittersweet. Human rights groups report that hundreds of other political prisoners continue to remain in custody. Moreover, for those freed, their release is conditional, as it was based on article 401(1) of the Criminal Procedure Code, which grants the president the power to suspend or decrease a prisoner's punishment.[64] As the sentences have been suspended, rather than overturned, the current or successive governments could arrest former political prisoners and return them to jail at any time, particularly if they participate in political activities. As of May 2012, no new arrests of internet users had been made. However, at least three former military or government officials remain imprisoned after they were sentenced in early 2010 for leaking sensitive information about junta activities to overseas groups via the internet.[65]

Despite the changes initiated by the new government, reforms have yet to reach the judiciary. Most judges were appointed by the previous junta and the government still interferes with judicial decisions. Trials for bloggers and other online activists that took place in 2011 were grossly unfair, lacking due process and typically held in special closed courts. Most defendants were denied access to legal counsel or adequate time to prepare a defense. Like other political prisoners in Burma, individuals detained on internet-related

[61] Joseph Allchin, "DVB VJ given additional 10 yrs in jail," Democratic Voice of Burma, September 14, 2011, http://www.dvb.no/news/dvb-vj-given-additional-10-yrs-in-jail/17646.
[62] Francis Wade, "Jailing of DVB reporters 'arbitrary': UN," Democratic Voice of Burma, November 24, 2011, http://www.dvb.no/news/jailing-of-dvb-reporters-'arbitrary'-un/18889.
[63] Aye Nai, "Ex-army captain sentenced to 10 years," Democratic Voice of Burma, August 29, 2011, http://www.dvb.no/news/ex-army-captain-sentenced-to-10-years/17316.
[64] Burma Lawyer Council, *The Code of Criminal Procedure in Burma*, accessed January 14, 2012, http://www.blc-burma.org/html/Criminal%20Procedure%20Code/cpc_16-30.html#401.
[65] In January 2010, a former military officer and a foreign affairs official were sentenced to death, and another foreign affairs official was sentenced to 15 years in prison, for the leak of information and photographs about military tunnels and a general's trip to North Korea. As of May 2012, the executions had not been carried out. Interview with Bo Kyi, cofounder of the Association for Assisting Political Prisoners (Burma), July 1, 2012.

charges are at risk of torture and medical neglect in custody. The above cases of Sithu Zeya and Nay Myo Zin illustrated the continued presence of these legal flaws even under the reformist government, though the pair was later released.[66]

The record of harsh punishments against critical internet users has fostered self-censorship and an impression of pervasive surveillance. In reality, however, surveillance is generally spotty due to the limited competence of the authorities, and corruption on the part of local officials. In many criminal cases, including the trials of bloggers and activists, materials such as online chat records and email messages have been used as evidence in court. The authorities either monitor internet activity before arrest, or abuse detainees during interrogation to obtain their passwords and electronic documents.

Cybercafe owners are required to keep records of the personal information and browsing history of their customers, be they Burmese or foreigners, and submit them once a month to the authorities.[67] They are also obliged to grant free access to the records to police, service providers, or ministerial representatives upon request. Many owners do not systematically carry out such monitoring, however, and the authorities' enforcement of their surveillance responsibilities is similarly inconsistent.

In addition to registering their identity when purchasing a mobile phone, individuals are required to register their computers with the state-owned MPT and obtain the company's permission to create a webpage.[68] Traditionally, these measures have been selectively enforced and implemented more rigorously for those suspected of engaging in political activism or transmitting information to overseas media outlets.

The previous junta was believed to engage in cyberattacks against opposition websites based abroad. This phenomenon persisted in 2011, and in some instances increased in sophistication, but it was difficult to determine whether the attacks were directed by the government as a whole or orchestrated by a hardline faction within the regime.[69] In September 2011, at the height of fighting between government forces and the ethnic minority resistance group the Kachin Independence Organization, the website of the Kachin

[66] Aye Nai, "Ex-army captain sentenced to 10 years," Democratic Voice of Burma, August 29, 2011, http://www.dvb.no/news/ex-army-captain-sentenced-to-10-years/17316.
[67] "Surveillance of Media and Internet Stepped up under New Civilian President," Reporters Without Borders, May 17, 2011, http://en.rsf.org/burma-surveillance-of-media-and-internet-17-05-2011,40296.html.
[68] OpenNet Initiative, "Country Profiles: Burma (Myanmar)," May 10, 2007, http://opennet.net/research/profiles/burma.
[69] According to an IT expert and company owner, top leaders no longer show an interest in procuring high tech devices that enable filtering, intercepting communications, or deploying cyberattacks, either because of the changing political environment or because of the high cost of these tools. Other IT experts and journalists noted that those who previously received ICT trainings in Russia and other countries, as well as the information minister, known as a hardliner, could still be playing a role in launching cyberattacks against opposition websites. Author's interviews with two journalists and two IT experts, December 28-30, 2011 and January 3, 2012.

News Group (KNG), which provided exclusive updates about the conflict and fleeing refugees, was temporarily shut down by a distributed denial-of-service (DDoS) attack.[70]

Prior to its unblocking in late 2011, the English-language edition of the exile Burmese news group, the *Irrawaddy*, was attacked by hackers in March 2011. In a more sophisticated attack than previous ones, the hackers penetrated *Irrawaddy*'s content management system and planted two pieces of highly sensitive false news on the website's front page, with the apparent aim of damaging the agency's reputation.[71] *Irrawaddy* staff said that the attacks had also potentially jeopardized the identity of confidential in-country sources and contributors. According to an expert investigation, the same IP addresses from which the hacking attack originated (located in London and using proxy servers in China) had also amended several sections on the Burmese military's Wikipedia page with impressive detail, indicating a current or previous connection to the military.[72] In 2011, several cases were reported of unidentified attackers hacking the email and Facebook accounts of Burmese exile dissidents, and in one case, the account of a defector from the Burmese army.[73]

[70] "KNG -Kachin News website attacked by cyber hacker since today 14.09," Kachin News Group, September 14, 2011, http://democracyforburma.wordpress.com/2011/09/14/kng-kachin-news-website-attacked-by-cyber-hacker-since-today-14-09/ (site discontinued).
[71] Ko Htwe, "The Irrawaddy Hacked," The Irrawaddy, March 14, 2011, http://www2.irrawaddy.org/article.php?art_id=20931.
[72] Shawn W. Crispin, "Burmese exile news site endures hacking, DDoS attacks," Committee to Protect Journalists, May 2, 2011, http://www.cpj.org/blog/2011/05/burmese-exile-news-site-endures-hacking-ddos-attac.php.
[73] Aye Lae, "Is Burma Really No. 1 in Internet attack traffic?," Mizzima, August 2, 2011, http://www.mizzima.com/news/inside-burma/5708-is-burma-really-no-1-in-internet-attack-traffic.html. According to exile sources, the e-mail account of a female journalist was also hacked. Author's interview with two Burmese exile journalists in Washington DC, December 20, 2011.

CHINA

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	19	18
Limits on Content (0-35)	28	29
Violations of User Rights (0-40)	36	38
Total (0-100)	**83**	**85**

* 0=most free, 100=least free

POPULATION: 1.3 billion
INTERNET PENETRATION 2011: 38 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Although China is home to the world's largest population of internet users, many of whom have shown increasing creativity in pushing back against censorship, the country's internet environment remains one of the world's most restrictive. This reflects the Chinese Communist Party's paradoxical "two-hand strategy" for managing digital technologies: promoting access for the purposes of economic advancement on the one hand while attempting to secure control over content, especially political communication, on the other.[1]

This paradox was especially evident in 2011 and early 2012. On the one hand, the Chinese authorities further enhanced an already sophisticated and multilayered system for censoring, monitoring, and manipulating activities on the internet, while abducting or imprisoning dozens of activists, lawyers, and bloggers. The scale and speed of the censorship effort—particularly the use of tens of thousands of human censors to identify and delete social media posts—was remarkable. One academic study reviewing censorship across nearly 1,400 blog-hosting and bulletin-board platforms in China estimated that 13 percent of posts were deleted, many within 24 hours of a particular term becoming sensitive or indicating collective action potential.[2] Such controls contributed to the Chinese internet increasingly resembling an intranet. Many average users, isolated from international social media

[1] Lena L. Zhang, "Behind the 'Great Firewall': Decoding China's Internet media policies from the inside," *The International Journal of Research into New Media Technologies*, Volume 12(3), 2006, 271-291.
[2] Gary King, Jennifer Pan, and Margaret Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," Working Paper, June 18, 2012, http://gking.harvard.edu/files/censored.pdf.

platforms and primarily exposed to a manipulated online information landscape, have limited knowledge of key events making news around the globe, including the publication of diplomatic cables by the antisecrecy group Wikileaks or anti-government protest movements sweeping the Middle East. Meanwhile, as one of the biggest domestic political scandals in recent memory unfolded in early 2012, many Chinese users were similarly left in the dark about events affecting the upcoming Communist Party's once-in-a-decade leadership change.

At the same time, due to the egalitarian nature and technical flexibility of the internet, the online environment remains freer and Chinese citizens more empowered than what is possible in the traditional media sector. Although Twitter remains blocked in China, a growing number of Chinese users are circumventing censorship to reach it and other restricted sites. Meanwhile domestic microblogging services like Sina Weibo have grown rapidly, surpassing 300 million users by early 2012. Their influence as a source of news and an outlet for public opinion has correspondingly grown. Microblogs' speed of transmission and other censorship loopholes enabled netizens to outpace censors, draw attention to incipient scandals, and mount online campaigns on various topics. The authorities responded with tightened controls on such services, including intensified censorship and real-name registration requirements, although the new restrictions' full effect on online discourse remains to be seen.

The Chinese public was first granted access to the internet in 1996, and the number of users has grown exponentially, from 20 million in 2001 to over 500 million in 2011.[3] Since it was first introduced, however, the ruling Chinese Communist Party (CCP) has consistently sought to assert its authority over the new medium. The underlying system of infrastructural control and filtering technology has been more or less complete since 2003,[4] while more sophisticated forms of censorship and manipulation have gained prominence recently.

OBSTACLES TO ACCESS

While the role and presence of information and communication technologies (ICTs) has continued to grow, users still face key obstacles to full and free access. These include centralized control over international gateways, a notable urban-rural gap, and sporadic, localized shutdowns of internet access at sites of protest.

[3] CNNIC, "Information and Updates on the Development of the Internet in China" [Hu Lian Wang Fa Zhan Xin Xi Yu Dong Tai], Issue 72 (Beijing: CNNIC, 2011), http://www.cnnic.cn/research/zx/qwfb/201112/W020111221472293628373.pdf.
[4] Zhang Jing, "Internet Monitor System Auto-Filters Reactionary Messages" [Wang Luo Shen Cha Xi Tong Yan Zhi Chen Gong, Fan Dong Xin Xi Zi Dong Guo Lv], Jing Hua Daily, February 26, 2003, http://www.people.com.cn/GB/it/53/142/20030226/931430.html.

The rate of internet adoption in China has slowed in recent years, as the market in urban areas begins reach a saturation point and most of the people with the literacy, interest, and economic capacity to use the internet are already online.[5] The government-linked China Internet Network Information Center (CNNIC) estimated in March 2012 that there were a total of 527 million users in the country, an increase of over 70 million since the end of 2010.[6] Given the country's large population and uneven economic development, however, the overall penetration rate remains just 39.4 percent,[7] slightly higher than the global average in 2011 (around 35 percent).[8] The average penetration rate in urban areas (73.5 percent) is over 45 points higher than that in rural areas (26.5 percent); in 2007, the gap was approximately 20 percentage points, suggesting a widening divide.[9]

Most users access the internet from home or work, with fewer using cybercafes than in the past, though these still account for 26.7 percent of users.[10] The vast majority of internet connections are via broadband rather than dial-up,[11] although access to international websites is slow due to the burden caused by the nationwide filtering and monitoring system.[12] Though generally affordable in urban areas, broadband prices are expected to drop in the near future. In the aftermath of an investigation into their dominance over the broadband market, telecommunications giants China Telecom and China Unicom announced in December 2011 that over the next five years, they would substantially raise broadband speeds while at the same time lowering costs.[13]

Use of mobile telephones has spread faster than internet access. According to the International Telecommunication Union (ITU), there were about 986 million mobile phone users in China at the end of 2011—an increase of 100 million over 12 months—giving the country a penetration rate of about 73 percent and the world's largest population of mobile

[5] CNNIC, "The 28th Report on the Development of the Internet in China" [Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong], July, 2011, http://www.cnnic.cn/research/bgxz/tjbg/201107/P020110721502208383670.pdf.
[6] CNNIC, "Information and Updates on the Development of the Internet in China" [Hu Lian Wang Fa Zhan Xin Xi Yu Dong Tai], Issue 76, May, 2012, http://www.cnnic.cn/research/zx/qwfb/201205/W020120504484883351802.pdf. The International Telecommunications Union (ITU) cited a similar rate of 38 percent in 2011: International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[7] Ibid.
[8] International Telecommunication Union, "The World in 2011: ICT Facts and Figures," October, 2011, http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.
[9] CNNIC, "The 29th Report on the Development of the Internet in China" [Zhong Guo Hu Lian Wang Fa Zhan Zhuang Kuang Tong], January, 2012, p.21, http://www.cnnic.cn/dtygg/dtgg/201201/W020120116337628870651.pdf.
[10] CNNIC, "The 28th Report on the Development of the Internet in China." [By comparison, in 2010, the percentage was 33.6 from cybercafés.
[11] CNNIC, "The 28th Report on the Development of the Internet in China," p.4.
[12] James Fallows, "The Connection has been Reset," The Atlantic, March 2008, http://www.theatlantic.com/magazine/archive/2008/03/-ldquo-the-connection-has-been-reset-rdquo/6650/
[13] Lu Hui, "China Telecom, China Unicom pledge to mend errors after anti-monopoly probe," English.news.cn, December, 2011, http://news.xinhuanet.com/english2010/china/2011-12/02/c_131285141.htm.

users.[14] Access to the internet via mobile phones is rapidly gaining popularity. By November 2011, 318 million people used this service,[15] often for accessing domestic microblogging applications offered by Sina, Tencent, Sohu, and other companies; CNNIC estimated that over 45 percent of Chinese internet users had signed up for one of these microblogging services by the end of 2011.[16]

The Chinese government has been known to shut down access to entire communications systems in response to specific events. The most dramatic such incident occurred in Xinjiang after an outburst of ethnic violence in the region's capital Urumqi; the blackout lasted from July 2009 to May 2010.[17] Since then, the authorities have similarly shut down internet communications at sites of unrest though on a smaller scale and lasting for shorter periods of time (usually several days or weeks): in December 2011, around the village of Wukan in Guangdong, after residents revolted against local officials over illegal land grabs;[18] and in February 2012 in Tibetan areas of Sichuan, after clashes surrounding a series self-immolations and reports that soldiers had opened fire on civilians.[19] In a partial shut down, beginning May 30, 2011, nearly all Mongolian chat rooms, discussion forums, blogs and instant messaging platforms, as well as many text-messaging services, were shut down for about a month in Inner Mongolia surrounding protests that erupted after a Mongolian herder was killed.[20]

Internet access service, once monopolized by China Telecom, has been liberalized and decentralized, and users can now choose from among scores of private internet service providers (ISPs). The government has been willing to liberalize the ISP market in part because of the centralization of the country's connection to the international internet, which is controlled by six to eight state-run operators that maintain advanced international gateways in Beijing, Shanghai, and Guangzhou.[21] This arrangement remains the primary infrastructural limitation on open internet access in the country, as all ISPs must subscribe

[14] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[15] CNNIC, "The 28th Report on the Development of the Internet in China," p.4.
[16] Chen Jian, "China Internet Polulation Reaches 485 Million, The Number of Microblogging Users Increases Dramatically" [Zhong Guo Wang Min Gui Mo Da 4.85 Yi, Wei Bo Yong Hu Shu Liang Bao Fa Zeng Zhang], Ren Min Wang, July, 2011, http://it.people.com.cn/GB/15192981.html; CNNIC, "Statistical Report on Internet Development in China," January, 2011, p.36, http://www.cnnic.cn/dtygg/dtgg/201201/W020120116337628870651.pdf.
[17] Chris Hogg, "China Restores Xinjiang Internet," British Broadcasting Corporation (BBC), May 14, 2010, http://news.bbc.co.uk/2/hi/asia-pacific/8682145.stm.
[18] "China police block access to protest village," Telegraph, December 12, 2011, http://www.telegraph.co.uk/news/worldnews/asia/china/8951275/China-police-block-access-to-protest-village.html.
[19] Tania Branigan, "China cut off internet in area of Tibetan unrest," Guardian, February 3, 2012, http://www.guardian.co.uk/world/2012/feb/03/china-internet-links-tibetan-unrest.
[20] Email communication with Enghebatu Togochog, director of the Southern Mongolia Human Rights Information Center.
[21] CNNIC, "Statistical Report on Internet Development in China," accessed March 23, 2009, list of documents: http://www.cnnic.cn/index/0E/00/11/index.htm; Actual document used: http://www.cnnic.cn/uploadfiles/doc/2009/1/13/92209.doc).

via the gateway operators and obtain a license from the Ministry of Industry and Information Technology (MIIT). The system essentially creates a national intranet and gives the authorities the ability to cut off any cross-border information requests that are deemed undesirable. Mobile telephone communication is dominated by three state-owned operators: China Mobile, China Telecom, and China Unicom. Under the oversight of the MIIT, connection to the internet via mobile phones is also monitored by the international gateway operators.

The authorities have sought to exercise increasingly tight control over the cybercafe business and other public access points. The issuance of cybercafe licenses is managed by the Ministry of Culture and its local departments, although to obtain a license, a proprietor typically must also communicate with various other state entities.[22] In January 2011, the Vice Minister of Culture announced that all sole-proprietor cybercafes would be replaced by chains within the next five years, a move that observers believed was aimed at increasing the efficiency of surveillance and censorship.[23] By December 2011, 40 percent of cybercafes in China were reportedly be owned by chains.[24] In another development affecting internet access in public spaces, in July 2011, police in central Beijing's Dongcheng district announced that all cafes, hotels, and other businesses offering wireless internet access must install surveillance software or face penalties and possible closure.[25] Some small business owners cut off their wireless service to avoid paying for the mandatory software (which cost about US$3,000), though some others reportedly ignored the directive.[26]

LIMITS ON CONTENT

The Chinese authorities continue to employ the most elaborate system for internet content control in the world. Government agencies and private companies together employ hundreds of thousands of people to monitor, censor, and manipulate online content. In recent years, additional layers have been added to this apparatus, particularly as the CCP seeks to restrict the use of social-networking and microblogging applications for political

[22] These include the Public Security, Bureau, State Administration for Industry and Commerce, among others. "A look at an illustration of the whole course of the cybercafe license application process" [Yi Kan Jiu Mingbai Quan Cheng Tu Jie Wang Ba Pai Zhao Shen Qing Liu Cheng], Zol.com, http://detail.zol.com.cn/picture_index_100/index997401.shtml

[23] "China Media Bulletin Issue No. 10," Freedom House, February 17, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-10#state.

[24] Zhou Zhi Jun, "Chianed Net Cafes Reached 40%, Government Calling For Establising Nationwide Net Cafe Association" [Quan Guo Wang Ba Lian Suo Lv 40%, Ni Chou Jian Quan Guo Wang Ba Hang Ye Xie Hui], Ren Min Wang, December 23, 2011, http://game.people.com.cn/GB/48644/48662/16697401.html.

[25] "Beijing, Surveillance Software Required Where Wifi Service is Provided" [Beijing: Ka Fei Dian Deng Chang Suo Ti Gong Wu Xian Wang Luo Xu An Zhuang 'Jian Kong Ruan Jian'], Beijing News, July 27, 2011, http://life.gmw.cn/2011-07/27/content_2349463.htm.

[26] Zhao Zhuo, "Some Cafe in Beijing Suspened Wifi Service" [Zhao Zhuo, Beijing Bu Fen Ka Fei Ting Ting Zhi Ti Gong Wu Xian Wang Luo], Beijing Youth Daily, http://www.mercicoffee.com/news/china/5565.html.

mobilization and sharing of uncensored information. Even this heavily censored and manipulated online environment, however, provides more space for average citizens to express themselves and air their grievances against the state than any other medium in China.

The CCP's content-control strategy consists of three primary techniques: automated technical filtering, forced self-censorship by service providers, and proactive manipulation. These techniques mutually reinforce each other to create a highly manipulated information landscape and one notably isolated from international news flows. The purported goal is to limit the spread of pornography, gambling, rumors, and other harmful practices, but web content related to sensitive political or social topics is targeted at least as forcefully.[27] The most systematically censored topics include criticism of top leaders, independent evaluations of China's rights record, violations of minority rights in Tibet[28] and Xinjiang, the Falun Gong spiritual group, the 1989 Beijing massacre, and various dissident initiatives that challenge the regime on a systemic level.[29] These standing taboos are supplemented by almost daily directives on negative developments, budding civic movements, or other forms of collective action. Criticism of the censorship system is also heavily censored.[30] In 2011, directives restricted reporting on a fatal high-speed rail collision, antigovernment protests in the Middle East, nuclear leaks related to the earthquake in Japan, tainted food scandals, environmental disasters, ethnic protests in Inner Mongolia,[31] and efforts by hundreds of independent candidates to run for seats on local people's congresses. Users' venting frustration at local governments or broader politically oriented terms like "democracy," "human rights," and "freedom of speech" are subject to less extensive censorship,[32] and

[27] Hung Huang, "Censorship in Chinese Media," Economix, September 25, 2008, http://economix.blogs.nytimes.com/2008/09/25/censorship-in-chinese-media/.

[28] For example, a study conducted in 2011 by scholars at Carnegie Mellon found that up to 53 percent of microblog posts generated from Tibet were deleted; http://www.cmu.edu/news/stories/archives/2012/march/march7_censorshipinchina.html

[29] These include, for instance, the prodemocracy manifesto Charter 08 and the "Nine Commentaries," a series of editorials analyzing the history of the party and encouraging an end to its rule. See graph, "Inaccessible Sites—Top 100 Google Search Results," from OpenNet Initiative, *Internet Filtering in China in 2004–2005: A Country Study*, available at Select Committee on Foreign Affairs, "Written Evidence Submitted by Sarah Cook, Student at the School of Oriental and African Studies, University of London," House of Commons, Session 2006–07, http://www.publications.parliament.uk/pa/cm200607/cmselect/cmfaff/269/269we08.htm; Nart Villeneuve, *Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform* (Toronto: Information Warfare Monitor/ONI Asia, 2008), http://www.nartv.org/mirror/breachingtrust.pdf; Julen Madariaga, "Charter 08: Why It Should Be Called Wang," Chinayourren, January 11, 2009, http://chinayouren.com/eng/2009/01/charter-08-why-it-should-be-called-wang/.

[30] Gary King et al., "How Censorship in China Allows Government Criticism but Silences Collective Expression."

[31] Sophie Beach, "Directives from the Ministry of Truth: May 1-31, 2011," June 4, 2011, China Digital Times, http://chinadigitaltimes.net/2011/06/directives-from-the-ministry-of-truth-may-1-31-2011.

[32] Gary King et al., "How Censorship in China Allows Government Criticism but Silences Collective Expression."

according to one study, their prevalence in the Chinese blogosphere has grown in recent years.[33]

The first layer of the censorship apparatus is the blocking of access to foreign websites via technical filtering or what is commonly referred to as the "Great Firewall." In some cases, whole websites are blocked based on their domain name. More common, however, is the authorities' use of deep-packet inspection technologies to enable filtering of particular pages within otherwise approved sites if the pages are found to contain blacklisted keywords in the URL path.[34] This nuance renders the effect of the censorship more subtle and less noticeable to users. Filtering by keyword is also implemented in mobile phone text-messaging,[35] as well as in instant-messaging services, such as Tom-Skype and QQ, and the necessary software is built into the application upon installation.[36] Academic research indicates that since 2008 the government has upgraded the sophistication of its nationwide technical filtering equipment.[37]

In practice, one of the most important uses the government has made of technical filtering has been to impose blanket blocks on certain Web 2.0 applications, thereby isolating the Chinese public from an international network of user-generated content. Since 2009, the video-sharing platform YouTube, the social-networking site Facebook, and Twitter have remained blocked most of the time in China.[38] Other international applications have sporadically complained of disruptions, particularly at politically sensitive times. The social-networking website LinkedIn was briefly blocked in February 2011, after a discussion group

[33] Shley Esarey and Xiao Qiang, "Digital Communication and Political Change in China," *International Journal of Communication*, 5 (2011), 298–319, http://ijoc.org/ojs/index.php/ijoc/article/viewfile/688/525.

[34] Ben Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control,'" Global Voices Advocacy, June 25, 2009, http://advocacy.globalvoicesonline.org/2009/06/25/study-deep-packet-inspection-and-internet-censorship/.

[35] Joseph Kahn, "China Is Filtering Phone Text Messages to Regulate Criticism," New York Times, July 3, 2004, http://www.nytimes.com/2004/07/03/world/china-is-filtering-phone-text-messages-to-regulate-criticism.html; "Well-red: Chinese communism's classic texts," Economist, February 18, 2010, http://www.economist.com/node/15546357.

[36] Xiao Qiang, "A List of Censored Words in Chinese Cyberspace," China Digital Times, August 30, 2004, http://chinadigitaltimes.net/2004/08/the-words-you-never-see-in-chinese-cyberspace/.

[37] For example, one academic study reported finding evidence that censorship technology had been placed at the provincial level, enhancing its effectiveness and opening the door to inter-provincial filtering, though there is no evidence to date that is has been used in this manner. See Polverini, Becker, When Form Follows Function: Finding and Modeling Censorware in the People's Republic of China, Princeton University Computer Science Department Thesis Work, 2009, http://www.cs.columbia.edu/~bpolveri/papers/bpolverini_pu_thesis.pdf; X. Xu, Z. Mao, and J. Halderman, "Internet Censorship in China: Where Does the Filtering Occur?" *Passive and Active Measurement*, Springer, 2011, 133–142, http://pam2011.gatech.edu/papers/pam2011--Xu.pdf.

[38] Tania Branigan, "Internet Censorship in China," The Guardian, January 14, 2010, http://www.guardian.co.uk/world/2010/jan/14/internet-censorship-china; Rebecca MacKinnon, "China Blocks Twitter, Flickr, Bing, Hotmail, Windows Live, etc. Ahead of Tiananmen 20th Anniversary," CircleID, June 2, 2009, http://www.circleid.com/posts/20090602_china_blocks_twitter_flickr_bing_hotmail_windows_live/; Google, "Mainland China Service Availability," accessed July 22, 2010, http://www.google.com/prc/report.html#hl=en; Michael Wines and Andrew Jacobs, "To Shut Off Tiananmen Talk, China Disrupts Sites," New York Times, June 2, 2009, http://www.nytimes.com/2009/06/03/world/asia/03china.html.

related to calls for a "Jasmine Revolution" in China was created. [39] In March, Google complained of disruptions to its Gmail email service.[40] At times, "web throttling," which slows the loading of web pages to render services nearly useless, is employed instead of a full block. Reports emerged during 2011 of web throttling being used against Google+ (a social-networking tool)[41] and the website of the anti-secrecy group Wikileaks after it published hundreds of U.S. diplomatic cables, some of which contained content normally censored in China.[42]

Simultaneously, the Chinese government has cultivated a wide range of domestic equivalents that have attracted hundreds of millions of users.[43] Chinese users thus have widespread access to video-sharing websites, social-networking tools, and email services. However, like other websites registered in China, the private Chinese companies that provide these services are required by law to ensure—either automatically or manually—that content banned by party and government censorship orders is not posted or circulated widely. Automated keyword filters are in place, but given the ease with which users can circumvent such filters via the complexities of the Chinese language, a huge percentage of deletions are implemented by human censors.[44] Editors and censorship staff reportedly receive as many as three notices per day—by text message, instant message, phone call, or email—that contain updates, adjustments, and minutiae pertaining to official censorship directives.[45] Firms risk losing their business licenses if they fail to comply, and many companies employ large staffs to carry out this task. Most postings on blogs, microblogs, comment sections of news items, and bulletin-board system (BBS) discussions that are deemed objectionable are deleted by company staff before they appear to the public or shortly thereafter. In addition, a growing army of volunteers, tens of thousands in Beijing alone, have been recruited to assist in identifying and reporting potentially undesirable content. [46]

---

[39] Keith B. Richburg, "Nervous about unrest, Chinese authorities block Web site, search terms," Washington Post, February 25, 2011, http://www.washingtonpost.com/world/nervous-about-unrest-chinese-authorities-block-web-site-search-terms/2011/02/25/ABPdw5I_story.html.

[40] David Barboza and Claire Cain Miller, "Google Accuses Chinese of Blocking Gmail Service," New York Times, March 20, 2011, http://www.nytimes.com/2011/03/21/technology/21google.html.

[41] Steven Millward, "Google+ Not Actually Blocked in China, Just Being Slowly Throttled," TechinAsia.com, June 30, 2011, http://www.penn-olson.com/2011/06/30/google-plus-china.

[42] Keith B. Richburg and Leila Fadel, "No audience for leaked cables in China and the Arab world," Washington Post, December 2, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/01/AR2010120106714.html.

[43] Rick Martin, "Ogilvy's 'Social Media Equivalents' in China 2011," TechinAisa.com, October 17, 2011, http://www.penn-olson.com/2011/10/17/china-social-media/.

[44] Gary King et al., "How Censorship in China Allows Government Criticism but Silences Collective Expression."

[45] Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space," Congressional-Executive Commission on China, November 17, 2011, http://www.cecc.gov/pages/hearings/general/hearing1/statement4.pdf.

[46] "Self-disciplined Practice and Thoughts of Chinesse Internet Industry in Web3.0" [Web3.0 Yuan Nian De Zhong Guo Hu Lian Wang Hang Ye Zi Lv Shi Jian Yu Xi Kao], Wenming.cn, April 2011, http://www.wenming.cn/xwcb_pd/yjpl/201104/t20110407_142975.shtml.

Two companies' required compliance with government censorship orders is especially notable because of their market dominance and the consequent impact of their actions on the online information landscape as a whole—Sina, which operates Sina Weibo, the most popular microblogging service, and Baidu, which operates the most used search engine. As of February 2012, Sina Weibo reportedly had 300 million users (of which 27 million were active daily), an exponential increase since its launch in 2009.[47] According to Sina executives, the firm has a "very powerful content censorship" system in place, which includes both automated and human monitoring 24 hours a day, run by hundreds of employees.[48] Sina Weibo users consistently report diverse measures employed by the company to prevent the circulation of politically sensitive content on a range of topics—deleting individual posts, deceiving users by making posts appear to them to have been published but actually rendering them invisible to followers, shuttering accounts, and removing results from the application's search function. For example, in September, citing government pressure, Sina shut down the account of a netizen who had used it to publish photos of Chinese ministerial-level officials wearing designer watches, a possible indication of corruption.[49] Tests conducted by Freedom House in July 2011 on the names of eight prominent human rights activists, lawyers, and journalists found that for seven of them, no results were returned to queries on Sina Weibo's search function.[50] A team of researchers from China Digital Times reportedly identified over 800 other filtered terms, including "Cultural Revolution" and "propaganda department."[51]

Baidu, which accounts for nearly 80 percent of China's search engine market,[52] has long been known to manipulate the results it offers based on government instructions, not only removing certain content, but also favoring state-approved information over content from non-governmental sources or content providers based outside of China. As an indication of the scale of information being removed, searches for the names of Gao Zhisheng, a prominent human rights lawyer who has been detained since 2010, yielded 2.25 million results on the uncensored Google.hk and only 495 on Baidu. For Ai Weiwei, an internationally renowned artist and digital activist, abducted by security forces from April to June 2011, Google.hk yielded 9.14 million results on and Baidu only 2.55 million.[53]

[47] "Sina Weibo Over 300 Million Users Now Who generate Over 100MM Posts Everyday," China Internet Watch, February 29, 2012, http://www.chinainternetwatch.com/1395/sina-weibo-users-2011/.
[48] Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."
[49] Kathrin Hille, "China's Censors Clamp Down On Watchblogger," Financial Times, September 21, 2011, http://www.ft.com/intl/cms/s/0/a5f7a660-e421-11e0-b4e9-00144feabdc0.html#axzz1ZAVEF2y1.
[50] "SPECIAL FEATURE, China Media Bulletin No. 29," Freedom House, July 14, 2011, http://freedomhouse.org/sites/default/files/inline_images/Cyberdisappearance%20in%20Action_special_feature-FINAL_0.pdf
[51] Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."
[52] Zhang Dan, "Alibaba vs Baidu: Can e-commerce trump search?" ZdNet Asia, September 27, 2011, http://www.zdnetasia.com/alibaba-vs-baidu-can-e-commerce-trump-search-62302246.htm.
[53] "SPECIAL FEATURE, China Media Bulletin No. 29," Freedom House.

Foreign corporations have also been required to implement censorship of political content in order to gain access to the Chinese market. In its tests, Freedom House found that Yahoo.cn produced search results that were as heavily restricted and dominated by Chinese government links as those of Baidu, and sometimes even more restrictive. In other cases, censorship has been indirectly incorporated into foreign internet products marketed in China. After being blocked in May 2011 for aggregating content from Facebook and Twitter, Flipboard, an application for Apple's iPad tablet computer, launched a Chinese version in December 2011. The new version aggregates content from Sina Weibo, social-networking site Renren, and other Chinese brands that have already implemented censorship per government requirements.[54] In March 2010, Google announced that it would stop censoring its search results and began redirecting mainland users to its uncensored Hong Kong-based search engine after Chinese officials made it clear that "self-censorship is a nonnegotiable legal requirement."[55] The authorities responded by blocking results of searches with flagged keywords that were initiated by mainland users on the Hong Kong engine. In September 2011, the Chinese government renewed Google's license to operate in China, though its business activities have mostly focused on non-political areas like its Android smartphone platform or Adsense advertising application.[56]

Routine censorship is often temporarily reinforced surrounding politically sensitive events. Throughout 2011, news and discussion of the anti-government protests in the Middle East that ousted authoritarian leaders were sharply curtailed. Fearing similar unrest at home, Chinese leaders put the online censorship apparatus into full gear to restrict Chinese users' knowledge of the events. Words like "Egypt"[57] and "Cairo"[58] were censored on popular online portals and Weibo sites. The word "jasmine," initially used to refer to the uprising in Tunisia, became a particularly sensitive word after calls for a "Jasmine Revolution" in China appeared online. The authorities responded with wide-ranging censorship of the word, including in contexts unrelated to politics, such as references to the flower, tea, or a popular folk song.[59] In other cases, when particular posts, blog entries, or multimedia clips that

[54] "China Media Bulletin: Issue No. 42," Freedom House, December 8, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-42#To.
[55] Ellen Nakashima, Cecilia Kang, and John Pomfret, "Google to Stop Censoring Search Results in China," Washington Post, March 23, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/22/AR2010032202041.html.
[56] Loretta Chao, "Chinese Regulators Renew Key License For Google," Wall Street Journal, September 7,2011, http://online.wsj.com/article/SB10001424053111904836104576556203077777200.html
[57] Edward Wong and David Barboza, "Wary of Egypt Unrest, China Censors Web," New York Times, January 31, 2011, http://www.nytimes.com/2011/02/01/world/asia/01beijing.html.
[58] Sarah Lovenheim, "In China, 'Egypt' and 'Cairo' have vanished," Washington Post, March 2, 2011, http://voices.washingtonpost.com/postpartisan/2011/02/imagine_if_you_typed_egypt.html.
[59] Ian Johnson, "Calls for a 'Jasmine Revolution' in China Persist," New York Times, February 23, 2011, http://www.nytimes.com/2011/02/24/world/asia/24china.html; Andrew Jacobs and Jonathan Ansfield, "Catching Scent of Revolution, China Moves to Snip Jasmine," New York Times, May 10, 2011, http://www.nytimes.com/2011/05/11/world/asia/11jasmine.html.

authorities find offensive attract massive public attention, they may be deleted after the fact.[60]

In early 2012, some of the most notable intra-CCP infighting in decades unfolded, and its repercussions were felt in the online sphere. The political scandal was sparked in February 2012 when Chongqing's police chief Wang Lijun attempted to defect to the U.S. consulate in Chengdu. The incident ultimately resulted in the downfall of the city's party secretary Bo Xilai (a CCP heavyweight who had been eying a seat on the powerful Politburo Standing Committee), his wife's arrest for murder, rumors of a coup plot, and reports that the party's security chief Zhou Yongkang's position may be in danger. As the events unfolded, the names of these top officials joined those of rights activists, returning no search results on Sina Weibo. Leftist websites that had been supportive of Bo and his neo-Maoist propaganda were shut down.[61] In an unprecedented step in late March, Sina Weibo and Tencent's microblogging service both disabled their comment feature for three days, reportedly to allow for the "concentrated cleansing" of "rumors and other illegal and harmful information."[62] Meanwhile, reports emerged of strange behavior on Baidu, which began returning unusually open results for sensitive queries like "June 4" (a reference to the 1989 Beijing massacre) and "Wang Lijun live harvest" (a reference to allegations that Wang had been involved in the forcible harvesting of organs from Falun Gong prisoners of conscience). The openings were fleeting, but caused observers to speculate that the CCP faction of President Hu Jintao and Premier Wen Jiabao was using Baidu to embarrass those aligned with former President Jiang Zemin by reducing censorship on human rights abuses the latter are closely associated with.[63]

Such dynamics illustrate the extent to which censorship decisions are frequently arbitrary and opaque. Some private companies are known to alert readers that content has been removed for unspecified reasons. However, attempts to access blocked URLs generally result in an error message similar to what one would encounter were a technical glitch at fault; there is no indication that content has been restricted due to a government decision. No avenue exists for appealing censorship decisions. Aware of the comprehensive nature of

[60] For instance, in January 2011, authorities ordered the removal of a satirical animated video that marked the upcoming Year of the Rabbit by mocking a series of scandals that had sparked public anger against the authorities; the clip concluded with an uprising. After initially garnering public attention, it began being systematically deleted from Chinese websites, though it remained available on YouTube, which is blocked. "Little Rabbit Kuang Kuang" [Xiao Tu Zi Kuang Kuang], http://www.youtube.com/watch?v=svwTTCxoJ3A; He Ping, "Animation 'Little Rabbit Kuang Kuang' Deleted from China's Internet" ['Xiao Tu Zi Kuang Kuang' Xi Lie Dong Hua Pian Zao Zhong Guo Hu Lian Wang Shan Chu], Radio Free Asia, January 26, 2011, http://www.rfa.org/mandarin/yataibaodao/tu-01262011164057.html.

[61] "China Media Bulletin No. 53," Freedom House, April 12, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-53#Microblog comments.

[62] Ibid.

[63] "China Media Bulletin No. 52," Freedom House, March 29, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-52#Users%20report

surveillance and censorship on the internet and mobile phone text messaging, ordinary users and bloggers engage in extensive self-censorship and often refrain from transmitting explicitly sensitive comments.

The existing censorship techniques have proven insufficient to completely overcome the flexibility of the technology, the sheer volume of communications, the creativity of users, and a sometimes intentional disregard for official directives by nonstate actors. The CCP and government agencies have taken various actions in the past year and a half to plug these gaps in the censorship system. They have included the following:

- **Creating a new agency to better coordinate internet regulation:** Over ten different government and Communist Party entities, at both the national and local level, are involved in internet censorship, with some instructions coming from the country's top leadership.[64] Much of this apparatus has remained unchanged, but in May 2011, the government also created a new agency, the State Internet Information Office (SIIO) to streamline procedures.[65] The agency was tasked with responsibilities such as managing online propaganda directives, punishing violators of online content rules, and overseeing the country's telecommunications companies.[66]
- **Increasing pressure on leading internet firms to tighten "self-discipline":** Beginning in February 2011, top officials—including several members of the powerful Communist Party Politburo Standing Committee—issued public statements or made personal visits to leading internet companies calling for tighter controls.[67] In August, the *People's Daily*, a CCP mouthpiece, published a full-page article on the political importance of controlling social media.[68] In November 2011, the SIIO organized a summit to "protect positive news online" and "reinforce self-discipline." Attending the meeting were executives of top telecommunications companies and popular websites, including China Telecom, China Mobile, China Unicom, Sina, Sohu, Netease, Baidu,

[64] See, for example, Politburo involvement in planning response to Nobel Peace Prize and Politburo member Liu Changchun's orders to state-run firms to stop doing business with Google: Jacobs, "Tirades Against Nobel Aim at Audience in China"; James Glanz and John Markoff, "Vast Hacking by a China Fearful of the Web," New York Times, December 4, 2010, http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?pagewanted=1&_r=3.

[65] The SIIO operates under the jurisdiction of the State Council Information Office. "China sets up State Internet information office," China Daily, May 4, 2011, http://www.chinadaily.com.cn/china/2011-05/04/content_12440782.htm.

[66] "China Media Bulletin No. 21," Freedom House, May 5, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-21#SIIO.

[67] Keith B. Richburg, "China Moves To Rein In Microblogs," Washington Post, October 4, 2011, http://www.washingtonpost.com/world/asia-pacific/china-moves-to-rein-in-microblogs/2011/10/03/gIQAXLLsKL_story.html.

[68] Michael Wines and Sharon LaFraniere, "Chinese Protest Suspensions of Bloggers," New York Times, August 26, 2011, http://www.nytimes.com/2011/08/27/world/asia/27weibo.html.

and Tencent. [69] The companies were urged to stop spreading "harmful information" online and to more efficiently self-censor.

- **Tightening controls on social media, especially microblogs:** After domestic social media tools, particularly popular microblogging sites like Sina Weibo, were used to channel public anger over a fatal train crash in July and then to circulate images of thousands of urban residents in the northeast city of Dalian protesting a polluting factory in August, the government redoubled its efforts to curb their influence and ability to quickly circulate undesirable information. Under such pressure and in an attempt to encourage users to self-censor, Sina Weibo notified its subscribers in August that several microbloggers deemed to have spread unfounded rumors were having their accounts suspended for one month.[70] In other instances, Sina staff have sent "friendly" reminders to users urging them to watch their words around politically sensitive periods or have deleted posts. Users boasting a large following have come under particular scrutiny.[71] Some activists also had their accounts shutdown, mostly notably, Ai Weiwei's Sina Weibo account was blocked in August after he used it to fundraise from supporters to pay a questionable tax charge levied against him by the authorities. [72] This trend continued in early 2012, with CCP representatives placed in microblog firms,[73] a real-name registration policy initiated (see "Violations of User Rights"), and a new "user contract" that would institute a point system to keep users in line announced.[74]

Realizing that they are unable to entirely control online content and increasingly viewing cyberspace as a field for "ideological struggle,"[75] the Chinese authorities in recent years have

[69] Ming De, "Bosses from Leading Telecommunications Companies Attended Authority's Meeting" [Zhong Guo Ge Da Wang Lu Ji Tuan Zong Cai Bei Ban Ban Zuo Bao Zheng], Soundofhope.org, November 6, 2011, http://big5.soundofhope.org/programs/162/202778-1.asp; "China Upgraded Censorship with Cooperation from Telecommunication Industry" [Zhong Guo Kong Zhi Wang Lu Yan Lun Sheng Ji, Ke Ji Ye Zhe Pei He 'Zu Zhi You Hai Zi Xun Chuan Bo'], Taiwan News, November 7, 2011, http://www.taiwannews.com.tw/etn/news_content.php?id=1751337.

[70] Michael Wines and Sharon LaFraniere, "Chinese Protest Suspensions of Bloggers," New York Yimes, August 26, 2011, http://www.nytimes.com/2011/08/27/world/asia/27weibo.html.

[71] Twitter of Hu Yong, https://twitter.com/#!/huyong/status/38988441538666496; David Bandurski, "Brutality and Tragedy Unseen," China Media Project, February 1, 2012, http://cmp.hku.hk/2012/02/01/18380/; David Bandurski, "Thank Goodness for Hong Kong," China Media Project, January 31, 2012, http://cmp.hku.hk/2012/01/31/18311/.

[72] C. Custer, "Ai Weiwei and Politics on Weibo," TechinAisa.com, November 8, 2011, http://www.penn-olson.com/2011/11/08/ai-weiwei-and-politics-on-weibo/; C. Custer, "Sina Blocks Weibo Accounts in Wake of Ai Weiwei's Fundraising Campaign," TechinAisa.com, November 7, 2011, http://www.penn-olson.com/2011/11/07/sina-blocks-weibo-accounts-in-wake-of-ai-weiweis-fundraising-campaign/.

[73] "China Media Bulletin No. 47," Freedom House, February 16, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-47#Party

[74] "Sina Weibo Introduces 'User Contract,'" Caijing.com.cn, May 9, 2012, http://english.caijing.com.cn/2012-05-09/111842544.html; "Censorship 3.0? Sina Weibo's New 'User Credit' Points System," China Real Time Report (blog), Wall Street Journal, May 29, 2012, http://blogs.wsj.com/chinarealtime/2012/05/29/censorship-3-0-sina-weibos-new-user-credit-points-system/.

[75] Oiwan Lam, "China: The Internet as an Ideology Battlefield," Global Voices Advocacy, January 6, 2010, http://advocacy.globalvoicesonline.org/2010/01/06/china-internet-as-an-ideology-battlefield/.

also introduced measures to proactively sway public opinion online and amplify the party's version of events over alternative accounts. This effort has taken a number of forms.

First, online news portals are prohibited from producing their own content and are only authorized to repost information from state-run traditional media.[76] Second, in addition to removal orders, propaganda directives are often accompanied by specific instructions to marginalize or amplify certain content, particularly from state media like the official Xinhua News Agency or the *People's Daily* Communist Party mouthpiece.[77]

Third, since 2005, paid web commentators known collectively as the 50 Cent Party have been recruited to post pro-government remarks, lead online discussions in accordance with the party line, and report users who have posted offending statements. Recent accounts of their activities highlight that posts do not only praise or support the CCP and government policy, but also target government critics with negative remarks or involve deliberate attempts to muddy the facts of a particular incident, such as a sighting of police abuse.[78] Estimates from 2008 placed the number of these commentators at over 250,000, but with internet usage having doubled since then, their number has likely expanded as well.[79] Since 2009, this strategy appeared to have become both more institutionalized and more decentralized, with commentators trained and used by "government units at all levels."[80] Increasingly, government employees have been directed to engage in online discussions to respond to criticism, though in some cases they are transparent about their ties to the state, a difference from the 50 Cent Party model. Training workshops for internet commentators were held throughout the country in 2011, including for police and prison personnel.[81]

[76] "Interim Provisions on the Administration of Internet Websites Engaged in News Posting Operations," November 1, 2000, excerpts available at http://www.cecc.gov/pages/virtualAcad/exp/explaws.php.

[77] Keith B. Richburg, "Chinese Editors, And A Web Site, Detail Censors' Hidden Hand," Washington Post, April 13, 2011, http://www.washingtonpost.com/world/chinese-editors-and-a-web-site-detail-censors-hidden-hand/2011/04/01/AFpMiRSD_story.html; "China Media Bulletin No. 17," Freedom House, April 7, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-17.

[78] David Bandurski, "Ai Weiwei Chat With Opinion Manipulator Surfaces," China Media Project, May 5, 2011, http://cmp.hku.hk/2011/05/09/12125/; Wu Nan, "Chinese Bloggers on the History and Influence of the 'Fifty Cent Party,'" China Digital Times, May 15, 2008, http://chinadigitaltimes.net/2008/05/chinese-bloggers-on-the-history-and-influence-of-the-fifty-cent-party/.

[79] David Bandurski, "China's Guerrilla War for the Web," Far Eastern Economic Review, July 2008, http://feer.wsj.com/essays/2008/august/chinas-guerrilla-war-for-the-web; Sarah Cook, "China's Growing Army Of Paid Internet Commentators," Freedom House (blog), October 11, 2011, http://blog.freedomhouse.org/weblog/2011/10/chinas-growing-army-of-paid-internet-commentators.html.

[80] David Bandurski, "Internet Spin for Stability Enforcers," China Media Project, May 25, 2010, http://cmp.hku.hk/2010/05/25/6112/.

[81] Sarah Cook, "China's Growing Army Of Paid Internet Commentators."

Fourth, mobile phone communication is now treated as another medium for spreading party ideology. In 2010, a campaign was launched to encourage the dissemination of pro-government "Red text messages" through economic incentives.[82]

Despite these government restrictions, the internet has emerged in recent years as a primary source of news and forum for discussion for many Chinese, particularly among the younger generations. Chinese cyberspace is replete with online auctions, social networks, homemade music videos, a large virtual gaming population, and spirited discussion of some social and political issues.[83] Civil society organizations involved in charity, education, health care, and other social and cultural issues that are deemed acceptable by the authorities often have a dynamic online presence. The growing popularity of microblogs in 2011 amplified these dynamics and generated a strong sense of empowerment among many Chinese users at being able to directly express their opinions to large numbers of fellow citizens, even if some such posts were subsequently deleted.[84] The government's censorship of social media, which many netizens have directly encountered, has generated resentment as well. It has become increasingly common for users—including those who would not normally consider themselves politically active—to criticize censorship itself by using humor.[85]According to Xiao Qiang of China Digital Times, "the Internet has became a quasi-public space where the CCP's dominance is being constantly exposed, ridiculed, and criticized, often in the form of political satire, jokes, videos, songs, popular poetry, jingles, fiction, Sci-Fi, code words, mockery, and euphemisms."[86]

In several cases in 2011, Chinese users successfully mobilized opposition to government decisions online, prompting a change in policy. In June, officials in Nanjing revised plans for a subway expansion after an online outcry—including posts by a Sina Weibo user with five million followers—emerged claiming the plan would sacrifice too many of the city's revered Wutong trees.[87] In July, a deadly high-speed train collision in Wenzhou was first reported by Weibo users who circulated real-time reports, calls for help, and photos. When initial signs emerged that the government might be covering up the true cause of the

[82] Chen Jian, "Sixty Million People Have Participated in 'Red Text Message' Efforts" [Zhong Guo Liu Qian Wan Ren Can Yu Zhuan Fa Shou Ji 'Hong Duan Zi'], Beijing Ren Min Wang, March 16, 2010, http://news.163.com/10/0316/21/61UI6BNGM000146BD.html; "China Telecom: Red Text Message – 'Love in China, Opportunities in Guang Dong' Writing Contest" [Hong Duan Zi Zhi 'Ai Wo Zhong Hua Chuang Ye Guang Dong' Wang Luo Chuang Ye Da Sai - - Mei Li Yang Jiang], Baidu, August 21, 2008, http://hi.baidu.com/liming10liming/blog/item/24de0a234ea6cbfad6cae224.html.

[83] H. Yu, "Blogging Everyday Life in Chinese Internet Culture," *Asian Studies Review* 31 (2007): 423–33.

[84] David Barboza, "Despite Restrictions, Microblogs Catch on in China," New York Times, May 15, 2011, http://www.nytimes.com/2011/05/16/business/global/16blogs.html.

[85] Brook Larmer, "Where an Internet Joke Is Not Just a Joke," New York Times, October 26, 2011, http://www.nytimes.com/2011/10/30/magazine/the-dangerous-politics-of-internet-humor-in-china.html.

[86] Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."

[87] Sharon LaFranierea, "Grass-Roots Fight to Save a 'Supertree,'" New York Times, June 4, 2011, http://www.nytimes.com/2011/06/05/world/asia/05china.html?pagewanted=1.

accident and as traditional media censored coverage per official directives, public outrage erupted online—including over 25 million messages on Sina Weibo—ultimately spurring the authorities to conduct a serious investigation into the accident.[88] In other cases, incidents of corruption were exposed, strikes were organized, and kidnapped children were identified. One group of users began using Google Maps to aggregate and track incidents of forced evictions and related protests.[89] Though the authorities have yielded to public pressure in some such instances, the resulting solutions and procedures typically fall short of systemic reforms or democratic decision making and are at times complemented by increased censorship.[90]

As controls have tightened in recent years, a growing number of individuals are reportedly seeking out knowledge and techniques for circumventing censorship. According to anecdotal accounts and data obtained from managers of circumvention tools, there were spikes in usage of these tools at politically important moments in early 2012—such as surrounding Bo Xilai's ouster or Chinese activist Chen Guangcheng's daring escape from house arrest to the U.S. embassy—when state-run media were conspicuously silent and heavy online censorship was in place. As importantly, there was an overall increase in the baseline number of users by mid-2012 when compared to late 2011, indicating that a contingent of first-time users decided to continue circumventing even during non-crisis periods.[91] In some cases, users' specific aim is to join Twitter, which is blocked in China. An activist community of some 200,000 people—an increase from 50,000 in 2010—use the tool to rapidly transmit news, connect with other socially conscious individuals, and take advantage of an uncensored medium.[92] Such growth in the use of circumvention tools occurred despite reports throughout 2011 that the government was increasing its efforts to

[88] Sharon LaFranierea, "China Finds More Bodies, and a Survivor, in Trains' Wreckage," New York Times, June 25, 2011, http://www.nytimes.com/2011/07/26/world/asia/26wreck.html; Michael Wines and Sharon LaFranierein, "Baring Facts of Train Crash, Blogs Erode China Censorship," New York Times, June 28, 2011, http://www.nytimes.com/2011/07/29/world/asia/29china.html; "China Media Bulletin No. 31," Freedom House, July 28, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-31.

[89] Bloody Map: A map created by Chinese internet users on forced eviction, immolation, and other local government power abuse, at: http://maps.google.com/maps/ms?brcurrent=3,0x35cab73c2e5c4465:0x946f70601c3d2630,0,0x34354978b41cab51:0xf168d14d8f0a2226%3B5,0,0&ie=UTF8&hl=zh-CN&msa=0&msid=111560301092049321699.0004921f02f43f6c4f07e&ll=35.532226,100.283203&spn=55.026174,79.013672&source=embed[2]%20Image:%20http://www.flickr.com/photos/shichuan/5085224907/.

[90] J. Lacharite, "Electronic Decentralization in China: A Critical Analysis of Internet filtering Policies in the People's Republic of China," *Australian Journal of Political Science* 37 (2002): 2, 333–46; Guobin Yang, *The Power of the Internet in China: Citizen Activism Online* (New York: Columbia University Press, 2009), http://www.chinese.rfi.fr/%E4%B8%AD%E5%9B%BD/20110216-%E4%B8%AD%E5%AE%A3%E9%83%A8%E8%A6%81%E6%B1%82%E5%AA%92%E4%BD%93%E5%AF%B9%E6%89%93%E6%8B%90%E8%BF%90%E5%8A%A8%E2%80%9C%E9%80%82%E5%BA%A6%E9%99%8D%E6%B8%A9%E2%80%9D.

[91] Email communication with circumention tool developer who wished to remain anonymous, June 2012.

[92] Jason Ng, "Investigation of Random Sampling in Chinese Twitter Users" [Zhong Wen Twitter Yong Hu Qun Chou Yang Diao Cha], Kenengba, January 27, 2010, http://www.kenengba.com/post/2540.html.

block users access to them.[93] Other methods for getting around censorship include using witty alternatives and homonyms for banned keywords, opening multiple blogs on different hosting sites, and using peer-to-peer technologies to circulate banned information.

Overtly political organizations, ethnic minorities, and persecuted religious groups remain underrepresented among websites that are freely accessible within China, though they have been able to use some ICTs to advance their causes. After being driven underground by a violent persecutory campaign, adherents of the Falun Gong spiritual practice have used the internet and mobile phones to maintain contact with one another and communicate with overseas practitioners. They have also downloaded censored information and disseminated it via vast amounts of offline leaflets and video discs (VCDs) that expose rights violations and cast doubt on party propaganda.[94] Tibetans have similarly used the internet and VCDs to circulate banned magazines, songs, and documentary films. Meanwhile, overseas Chinese-language media and human rights groups have reportedly sent millions of emails into the country, supplying users with news summaries on Chinese and international events, instructions on anticensorship technology, and copies of banned publications.

VIOLATIONS OF USER RIGHTS

Article 35 of the Chinese constitution guarantees freedoms of speech, assembly, association, and publication, but such rights are subordinated to the CCP's status as the ruling power. In addition, the constitution cannot, in most cases, be invoked in courts as a legal basis for asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive freedom of expression cases. A wide variety of regulations have been issued by different government agencies to establish censorship guidelines. The National People's Congress in April 2010 adopted an amendment to the State Secrets Law[95] that requires telecom operators and ISPs to cooperate with authorities on investigations

[93] For example, in March 2011, several popular VPNs reported being crippled. In November, administrators of TOR found that many of its "bridge nodes" had become inaccessible to Chinese users shortly after being set up. The managers of other circumvention tools like Ultrasurf and Freegate also witnessed intensified efforts to disrupt their services, though at year's end, Chinese users were still able to access them. Internet security experts confirmed suspicious activity in late 2011, suggesting that Chinese ISPs may have been testing a new system for identifying the type of encrypted services often used by circumvention tools in order to them disconnect them. See, Sharon LaFraniere and David Barboza, "China Tightens Censorship of Electronic Communications," New York Times, March 21, 2011, http://www.nytimes.com/2011/03/22/world/asia/22china.html?_r=2&pagewanted=1; Andy Greenberg, "China's Great Firewall Tests Mysterious Scans On Encrypted Connections," Forbes, November 17, 2011, http://www.forbes.com/sites/andygreenberg/2011/11/17/chinas-great-firewall-tests-mysterious-scans-on-encrypted-connections/.

[94] "Written Statement of Li Hai, Falun Gong practitioner and former member of Department of Treat and Law, Ministry of Foreign Affairs, People's Republic of China," Hearing of Foreign Affairs Committee regarding human rights in China, July 25, 2012, http://foreignaffairs.house.gov/112/HHRG-112-FA00-WState-HaiL-20120725.pdf.

[95] "The President Order of The People's Republic of China, No.28" [Zhong Hua Ren Min Gong He Guo Zhu Xi Ling, Di Er Shi Ba Hao], http://www.gov.cn/flfg/2010-04/30/content_1596420.htm.

involving the leaking of state secrets.[96] The law took effect on October 1 and has been generally met with compliance from companies, mostly because the economic stakes of disobedience and loss of business license are so high.

Vague provisions in the criminal code and state-secrets legislation have been used to imprison citizens for their online activities, including publication of articles criticizing the government or exposing human rights abuses, transmission of objectionable email messages, and downloading of censored material from overseas websites. Trials and hearings lack due process, often amounting to little more than sentencing announcements.

Prison sentences for online violations tend to be longer in China than in many other countries, often a minimum of three years and sometimes as long as life imprisonment, while punishments elsewhere typically range from six months to four years. Some users are also sentenced without trial to "reeducation through labor" camps for up to three years. Once in custody, detainees frequently suffer abuse, including torture and denial of medical attention. Though the targeted individuals represent a tiny percentage of the overall user population, the harsh sentencing of prominent figures has a chilling effect on the fairly close-knit activist and blogging community and encourages self-censorship in the broader public.

The year 2011 was notable, in particular, for a spate of extralegal abductions and long prison terms imposed in connection with online calls for a Jasmine revolution in China. The calls, which were first posted on the U.S.-based website Boxun and then spread over Twitter, sparked no serious protests, in part because of the strong show of security forces sent to the alotted sites.[97] Some observers noted, therefore, that the authorities may have used the calls as a pretext for a crackdown that had been brewing for some time as CCP officials grew wary of the growing influence of certain activists and their outspokenness online. Beginning in February 2011, dozens of lawyers, activists, and bloggers who had been active both on domestic and international social media were abducted one after another in what became one of the worst crackdowns on free expression in China in recent memory.[98] According to Chinese Human Rights Defenders, at least 78 people were known to have been taken into

[96] Reporters Without Borders, "Amendment Enlists ICT Companies in Protectino of State Secrets," news release, April 29, 2010, http://en.rsf.org/china-amendment-enlists-ict-companies-in-29-04-2010,37238.html; Jonathan Ansfield, "China Passes Tighter Information Law," New York Times, April 29, 2010, http://www.nytimes.com/2010/04/30/world/asia/30leaks.html.

[97] Ian Johnson, "Call for Protests in China Draws More Police than Protesters," New York Times, February 27, 2011, http://www.nytimes.com/2011/02/28/world/asia/28china.html; Andrew Jacobs and Jonathan Ansfield, "Well-Oiled Security Apparatus in China Stifles Calls for Change," New York Times, February 28, 2011, http://www.nytimes.com/2011/03/01/world/asia/01china.html.

[98] Edward Wong, "Human Rights Advocates Vanish as China Intensifies Crackdown," New York Times, March 11, 2011, http://www.nytimes.com/2011/03/12/world/asia/12china.html.

custody as of June 2011, either formally or extralegally.[99] In most cases, families were not notified of the detainee's whereabouts or grounds for detention. Many of the activists later reported abuse in custody, including beatings, forcible medication, sleep deprivation, and other forms of mistreatment that caused one lawyer to contract tuberculosis in only 21 days.[100]

The highest profile victim of disappearance was Ai Weiwei,[101] the prominent artist and outspoken blogger, who was abducted from early April to late June 2011. He was kept in isolation and suffered psychological pressure and threats, but no physical abuse. After his release, the authorities launched a formal prosecution on tax evasion charges, which were widely perceived as trumped up.[102] Ai and others reported being forced to sign statements promising not to be active on Twitter as a condition for their release.[103] This generated an eerie online silence for several months, but by year's end many were defying the authorities and had resumed posting to social media.[104]

Several of the individuals arrested in the crackdown were formally charged with "inciting subversion of state power" and in some cases, sentenced to long prison terms throughout the year. Ran Yunfei, a prominent blogger from Sichuan known for his advocacy of democratic reforms was charged in March 2011, but released in August and placed under house arrest on condition that he would not speak publicly.[105] Also in March, Liang Haiyi, a 35-year-old woman from Harbin, was charged with subversion after putting information about the

[99] Prepared Statement of Xiaorong Li, Independent Scholar, Congressional-Executive Commission on China Roundtable on "Current Conditions for Human Rights Defenders and Lawyers in China, and Implications for U.S. Policy," June 23, 2011, http://www.cecc.gov/pages/roundtables/2011/20110623/statement4.php.

[100] "Tortured, dissident Christian lawyer talks about his ordeal," Asianews.it, September 15, 2011, http://www.asianews.it/news-en/Tortured,-dissident-Christian-lawyer-talks-about-his-ordeal-22641.html; Paul Mooney, "Silence of The Dissidents," South China Morning Post, July 4, 2011, http://pjmooney.com/en/Most_Recent_Articles/Entries/2011/7/4_Silence_of_The_Dissidents.html.

[101] Kate Taylor, "Arts Group Calls for Worldwide Sit-In for Ai Weiwei," New York Times, April 14, 2011, http://artsbeat.blogs.nytimes.com/2011/04/14/arts-group-calls-for-worldwide-sit-in-for-ai-weiwei/?scp=9&sq=&st=nyt.

[102] "Wu Yu, Ai Weiwei Was Criticized for Pornography, Netizens Fought Back" [Ai Wei Wei Bei Zhi 'Se Qing', Wang Min 'Ai Luo Luo'], Dw.de, November 19, 2011,http://www.dw-world.de/dw/article/0,,15543929,00.html.

[103] Sui-Lee Wee, "No interviews, Twitter, travel for Ai Weiwei," Reuters, June 24, 2011, http://www.reuters.com/article/2011/06/24/us-china-artist-idUSTRE75L3U520110624.

[104] Prepared Statement of Elisabeth Wickeri, Executive Director and Adjunct Professor of Law, Leitner Center for International Law and Justice, Fordham Law School; Member, Committee to Support Chinese Lawyers, Congressional-Executive Commission on China Roundtable on "Current Conditions for Human Rights Defenders and Lawyers in China, and Implications for U.S. Policy"; Paul Mooney, "Silence of The Dissidents."

[105] "China Charges Well-Known Internet Activist with Subversion," Voice of America, March 27, 2011, http://www.voanews.com/english/news/asia/China-Charges-Well-Known-Internet-Activist-with-Subversion-118788199.html; Andy Yee, "China: Ran Yunfei's Blogging for Political Change," Global Voices, April 9, 2011, http://globalvoicesonline.org/2011/04/09/china-ran-yunfei%E2%80%99s-blogging-for-political-change; C. Custer, "Ran Yunfei's Release and Online Activism in China," TechinAsia.com, August 11, 2011, http://www.penn-olson.com/2011/08/11/ran-yunfeis-release-and-online-activism-in-china; Silvia Duarte, "Ran Yunfei Released After Ai Weiwei Asks for Blogger's Support on Twitter," Sampsoniaway.org (blog), August 16, 2011, http://www.sampsoniaway.org/blog/2011/08/16/ran-yunfei-released-after-ai-weiwei-asked-for-bloggers-support-on-twitter.

protests in a chat room; she remained in incommunicado detention at year's end.[106] Hua Chunhui from Jiangsu was detained for "inciting subversion" after transmitting details of the revolution calls via his Twitter account and in April was sent to a "reeducation through labor camp."[107] In September, Wang Lihong, a prominent female online activist, was sentenced to nine months in prison.[108] In the most severe set of punishments, in December 2011, Chen Wei from Sichuan and Chen Xi from Guizhou were sentenced to nine and ten years in prison, respectively.[109]

More common than long-term imprisonment or abduction are other forms of extralegal harassment, including house arrest. According to some estimates, thousands of individuals have been summoned for questioning and warned in recent years by security officials, a tactic also applied in 2011 regarding the Jasmine Revolution and other issues.[110] In addition, according to Chinese Human Rights Defenders, over 80 people were placed under house arrest.[111] Even after release from prison, prominent activists have been kept under tight surveillance, house arrest, and had their internet and mobile phone connections cut of. In 2011, internationally renowned activists Hu Jia from Beijing and Chen Guangcheng from Shandong and their families were subjected to such treatment.[112] Liu Xia, the wife of democracy advocate and Nobel Peace Prize laureate Liu Xiaobo, was similarly kept under house arrest and in isolation from the outside world.[113] Liu himself remained imprisoned, serving an 11-year sentence on charges of "inciting subversion of state power" for publishing

[106] "Document - Futher Information: Chinese Activist Sentenced To Nine Years," Amnesty International, January 6, 2012, https://www.amnesty.org/en/library/asset/ASA17/002/2012/en/888cba41-1a6b-462c-b639-c85f27c6b5ab/asa170022012en.html; "China's 'Jasmine' activists," Amnesty International, May 6, 2011, http://www.amnesty.org.nz/news/china%E2%80%99s-jasmine-activists.

[107] "China detains, censors bloggers on 'Jasmine Revolution'," Committee to Protect Journalists, February 25, 2011 http://www.cpj.org/2011/02/china-detains-censors-bloggers-on-jasmine-revoluti.php; Prepared Statement of Xiaorong Li, Independent Scholar, Congressional-Executive Commission on China Roundtable on "Current Conditions for Human Rights Defenders and Lawyers in China, and Implications for U.S. Policy."

[108] Charles Hutzler, "Wang Lihong, Chinese Online Activist, Sentenced To Prison For Staging Protest," Huffington Post, September 9, 2011, http://www.huffingtonpost.com/2011/09/09/wang-lihong-prison_n_955226.html; "Internet Activist Wang Lihong Tried in Beijing," China Digital Times, August 16, 2011, http://chinadigitaltimes.net/2011/08/internet-activist-wang-lihong-tried-in-beijing/.

[109] "Jailed Human Rights Lawyer Allowed Visit By Brother," Reporters Without Borders, March 29, 2012 http://en.rsf.org/chine-authorities-step-up-pressure-on-30-03-2011,39918.html

[110] Cara Anna, "China's Troublemakers Bond Over 'Drinking Tea,'" Associated Press, March 10, 2010, http://abcnews.go.com/Technology/wirestory?id=10062829&page=1; "@StonyWang: Forced to Drink Jasmine Tea," China Digital Times, March 25, 2011, http://chinadigitaltimes.net/2011/03/stonywang-forced-to-drink-jasmine-tea/; "China detains, censors bloggers on 'Jasmine Revolution,'" Committee to Protect Journalists.

[111] Andrew Jacobs, "Chinese Government Responds to Call for Protests," New York Times, February 20, 2011, http://www.nytimes.com/2011/02/21/world/asia/21china.html.

[112] "China Media Bulletin No. 27," Freedom House, June 30, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-27#jailed; "China Media Bulletin No. 10," Freedom House, February 17, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-10#activist.

[113] "Liu Xiaobo Briefly Leaves Jail; Wife's House Arrest Continues,"China Digital Times, October 4, 2011, http://chinadigitaltimes.net/2011/10/liu-xiaobo-briefly-leaves-jail-wifes-house-arrest-continues/.

pro-democracy writings online, including drafting and circulating the prodemocracy manifesto Charter 08.[114]

The above forms of suppression were also applied during the year on topics unrelated to the Jasmine Revolution. Throughout 2011, hundreds of intellectuals, business executives, and activists attempted to compete as independent candidates in elections for local People's Congresses, whose seats are typically secured only by candidates handpicked by the CCP. [115] Many used their Sina Weibo microblog accounts to campaign and connect with potential voters. The authorities responded with deletions, account shut downs, harassment, and occasional arrests. In May, Liu Ping from Jiangxi was detained by police,[116] while He Peng from Jiangsu was also called in for questioning. [117] Shanghai businessman Xia Shang received a visit from the Ministry of State Security and two companies he runs were "randomly" selected for a tax audit.[118] Separately, in April 2011, Fang Hung, a retired civil servant in Chongqing, was ordered to serve one year in a "re-education through labor" camp after mocking the municipal party secretary, Bo Xilai, in a microblog post.[119] Towards year's end, officials were increasingly warning users of Sina Weibo that they could face prosecution for "spreading rumors." In December 2011, state-run media reported that two men had been detained in Hunan and would be held for five days.[120] In March 2012, human rights groups reported that several people had been detained over microblog posts they published related to CCP infighting, particularly rumors of a coup attempt.[121] In recent years, local officials

[114] Sharon Hom, "Google and Internet Control in China: A Nexus Between Human Rights and Trade?" (testimony, U.S. Congressional-Executive Commission on China, Washington, DC, March 24, 2010), http://www.cecc.gov/pages/hearings/2010/20100324/homTestimony.pdf?PHPSESSID=0e7517d795355cc4cd7132dcb51f2004.

[115] Jiang Xun, "New Trend of Chinese Citizens Running for Local People's Congress," The World and China Institute, http://www.world-china.org/newsdetail.asp?newsid=3421

[116] "China's New Independents Tap Social Media to Challenge Communist Party (Updated)," China Digital Times, June 8, 2011, http://chinadigitaltimes.net/2011/06/chinas-new-independents-tap-social-media-to-challenge-communist-party/.

[117] John Kennedy, "China: Independent Candidates Busy Building Up Support Photos," Global Voices, July 17, 2011, http://globalvoicesonline.org/2011/07/17/china-independent-candidates-busy-building-up-support/.

[118] "China's New Independents Tap Social Media to Challenge Communist Party (Updated)," China Digital Times.

[119] In July 2012, a Chongqing court ruled in Fang's favor in a lawsuit he filed for administrative compensation over his one year served in the camp. Given the rarity of such victories for labor camp detainees, most observers interpreted the ruling more as a reflection of the change in Bo Xilai's political fortune than as signaling a larger loosening of restrictions on free expression; "China Media Bulletin No.63," Freedom House, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-63#2; "China Media Bulletin No.24," Freedom House, June 9, 2011, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-24#netizen.

[120] The pair had uploaded a video online that claimed thousands of police officers were guarding a wedding convoy, suggesting misuse of public resources; local police said the officers were in a training drill and happened to be passing by. Brian Spegele and Josh Chin, "China Detains Pair for Spreading Rumors Online," Wall Street Journal, December 12, 2011, http://blogs.wsj.com/chinarealtime/2011/12/12/china-detains-pair-for-spreading-rumors-online/?mod=google_news_blog; "China detains two for spreading online rumor," China Daily, December 12, 2011, http://www.chinadaily.com.cn/china/2011-12/12/content_14252920.htm.

[121] "Six netizens arrested, sixteen websites shut down," IFEX, April 11, 2012, www.ifex.org/china/2012/04/02/netizens_arrested; Wu Ming, "China Human Rights Briefing April 3-10, 2012," Chinese Human Rights Defenders, April 11, 2012, http://chrdnet.com/2012/04/11/china-human-rights-briefing-april-3-10-2012/.

have also resorted to criminal defamation charges to detain and in some cases imprison whistleblowers who post corruption allegations online, though no high-profile cases were reported in 2011.

Members of religious and ethnic minorities are targeted for particularly harsh treatment for their online activities. In the aftermath of ethnic violence in Xinjiang in July 2009, several individuals involved in websites reporting on Uighur issues were sentenced to prison terms ranging from 15 years to life imprisonment. Tibetans and Falun Gong practitioners who transmit information abroad often suffer repercussions, while some have been arrested solely for accessing or quietly disseminating banned information. In January 2012, Tibetan groups reported that Gyitsang Takmig had been sentenced to four years in prison for distributing 2,500 VCDs discussing Tibetan history and aspirations for greater freedoms.[122] Some have also been detained for circulating text-messages. In Inner Mongolia, people who disseminated text-messages about widespread protests that occured in May 2011 were summoned by the authorities.[123] According to the Falun Dafa Information Center, two women were sentenced to 5.5 and 6 years in prison in March 2011 for having sent text messages urging people to gather outside a courthouse to show solidarity during the trial of a fellow Falun Gong practitioner.[124]

The space for anonymous online communication in China is steadily shrinking as real-name registration requirements expand. Most major news portals such as Sina, Netease, and Sohu implemented real-name registration for their comment sections during 2009.[125] It had already been required in cybercafes, university BBS, and major blog-hosting sites.[126] An internet content provider (ICP) license from the MIIT is required to establish a personal or corporate website within China, and the process requires applicants to submit personal identification information. In February 2010, the authorities added a requirement that

[122] "TCHRD condemns China sentencing of Tibetan Filmmaker Dhondup Wangchen," press release, January 8, 2012, http://www.tchrd.org/report/press/2010.pdf.
[123] "Mongolian Professors Held," Radio Free Asia, June 7, 2011, http://www.rfa.org/english/news/china/professors-06072011123731.html/.
[124] "Falun Gong News Bulletin: June 10, 2011," Falun Dafa Information Center, June 10, 2011, http://www.faluninfo.net/article/1139/#6.
[125] Jonathan Ansfield, "China Web Sites Seeking Users' Names," New York Times, September 5, 2009, http://www.nytimes.com/2009/09/06/world/asia/06chinanet.html; Reporters Without Borders, "Government Crusade Against Online Anonymity," news release, May 7, 2010, http://en.rsf.org/china-government-crusade-against-online-07-05-2010,37412.html.
[126] "Ministry of Culture Will Curb Trend of Internet Indecency in 2009" [Wen Hua Bu 2009 Jiang Da Li Zhen Zhi Hu Lian Wang Di Su Zhi Feng], Net Bar China, January 6, 2009, http://www.netbarcn.net/Html/PolicyDynamic/01061954388252.html; Chen Jung Wang, "Real Name System Intimidates High School BBS" [Shi Min Zhi Rang Gao Xiao BBS Bian Lian], CNHubei, November 29, 2009, http://www.cnhubei.com/200511/ca936578.htm; "Internet Society of China: Real Name System for Bloggers is Set" [Zhong Guo Hu Lian Xie Hui: Bo Ke Tui Xing Shi Min Zhi Yi Chen Ding Ju], Xinhua News, October 22, 2006, http://www.itlearner.com/article/3522.

individuals registering a website have their photograph taken and placed on file.[127] In late 2011, real-name registration was expanded to domestic microblogging services, amidst broader restrictions imposed on social media tools. In December 2011, five major cities (Beijing, Guangzhou, Shanghai, Tianjin, and Shenzhen) announced they would begin requiring microblog services, including the popular Sina Weibo and Tencent, to implement real-name registration. The deadline set for registration was March 16. Those who refused would reportedly have the function enabling them to post messages disabled.[128] In March, Sina announced that it anticipated that about 60 percent of subscribers (over 150 million users) would verify their identity by the deadline, but a counter on the company's website reportedly said only 19 million had registered as of March 16.[129] The counter was then removed and no clear statistics were subsequently available on the scale of the policy's implementation for either Sina or other microblogging services. In April, Sina noted in its annual report to the U.S. Security and Exchange Commission (SEC) that many users had not yet complied, that it feared full implementation would cause its traffic and usage to decline dramatically, and that its ongoing failure to execute full registration exposed it to potentially "severe punishment" by the government.[130] Verification is apparently being done through a government-linked contractor or via users providing their mobile phone number,[131] whose acquisition has required real-name registration since September 2010.[132] This factor led some sources to estimate that by early 2012, approximately 50 percent of microblog users' real identities were indirectly known to providers because they accessed the platform via their already registered mobile phones.[133]

Surveillance of internet and mobile phone communications by security services is pervasive. The same deep-packet inspection technology used to censor content based on banned key words is also used to monitor and detect users trying to access or disseminate similar

[127] Donnie Hao Dong, "Wanna Setup a Personal Website in China? BEING TAKEN a Portrait Please," Blawgdog, February 23, 2010, http://english.blawgdog.com/2010/02/wanna-setup-personal-website-in-china.html; Elinor Mills, "China Seeks Identity of Web Site Operators," CNET News, February 23, 2010, http://news.cnet.com/8301-27080_3-10458420-245.html.

[128] "China Media Bulletin No. 46," Freedom House, February 3, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-46#3.

[129] Melanie Lee, "Weibo, China's Twitter, Estimates 60 Percent Of Users Verified By Deadline," Huffington Post, March 12, 2012, http://www.huffingtonpost.com/2012/03/12/weibo-china-twitter_n_1338246.html; Malcom Moore, "China moves to control Sina Weibo social network with real names," The Telegraph, March 16, 2012, http://www.telegraph.co.uk/technology/news/9147767/China-moves-to-control-Sina-Weibo-social-network.html.

[130] "China Media Bulletin: Issue No. 46," Freedom House, May 3, 2012, http://www.freedomhouse.org/article/china-media-bulletin-issue-no-56#3.

[131] Ibid.; "Real-name Verificationof Weibo Suspected Monopolized by Guo Zheng Tong" [Du Zi He Cha Wei Bo Shi Ming Guo Zheng Tong She Long Duan], Hong Kong Commercial Daily, December 30, 2011, http://www.hkcd.com.hk/content/2011-12/30/content_2875001.htm; "Beijing Users of Weibo Required for Real-name Verificationof" [Beijing Yao Qiu Wei Bo Yong Shi Ming Fa Yan], BBC, December 16, 2011, http://www.bbc.co.uk/zhongwen/trad/chinese_news/2011/12/111216_beijing_weibo.shtml.

[132] "Mobile phone real name system implemented today, SIM card purchasers have to present their ID documents" [Shou Ji Shi Ming Zhi Jin Qi Shi Shi, Gou Ka Xu Chi Shen Fen Zheng], News 163, October 1, 2010, http://news.163.com/10/0901/00/6FF3HKF8000146BD.html.

[133] Net.China.com.cn, March 15, 2012 [in Chinese], http://net.china.com.cn/txt/2012-03/15/content_4875947.htm.

information. In some free expression cases, private instant-messaging conversations or text messages have been directly cited in court documents. During 2011, two lawsuits were filed in U.S. courts against the American technology company Cisco Systems, asserting there was evidence the firm had customized its surveillance equipment to assist Chinese security agencies in apprehending Falun Gong practitioners and democracy activists; Cisco denied the allegations and the cases were pending as of May 2012.[134] Separately, one academic study reported observing that queries on the search engine Baidu that contained banned keywords were being automatically redirected with the user's IP address to a location in Shanghai suspected of being related to the city's Public Security Bureau.[135] Given the secrecy surrounding such capabilities, however, it is difficult to verify their existence or extent of their use.

Various service providers (including ISPs, bulletin boards, and email providers) are required to retain user information for 60 days and provide it to the authorities upon request without independent judicial oversight.[136] Cybercafes require users to present photo ID and must record user activities. In some regions, video surveillance cameras in cybercafes are reportedly directly connected to the local police station.[137] In recent years, additional intrusive elements have been added to the surveillance apparatus. In March 2011, Beijing's municipal government announced that it would begin using technology to track the location of the city's 17 million mobile phone users in real time.[138] The declared purpose was to be able to provide up-to-date traffic information to relieve congestion, but the announcement sparked concerns it would be used to identify and punish dissent.[139]

China has emerged as a key global source of cyberattacks. Although not all attacks originating in the country have been explicitly traced back to the government, their scale,

[134] Somini Sengupta, "Group Says It Has New Evidence of Cisco's Misdeeds In China," New York Times, September 2, 2011, http://www.nytimes.com/2011/09/03/technology/group-says-it-has-new-evidence-of-ciscos-misdeeds-in-china.html; "Suit claims Cisco helped China repress religious group," Thomson Reuters News & Insight, May 20, 2011, http://newsandinsight.thomsonreuters.com/Legal/News/2011/05_-_May/Suit_claims_Cisco_helped_China_repress_religious_group/; Don Tennant, "Second Lawsuit Accuses Cisco of Enabling China to Oppress Citizens, " IT Business Edge, June 9, 2011, http://www.itbusinessedge.com/cm/blogs/tennant/second-lawsuit-accuses-cisco-of-enabling-china-to-oppress-citizens/?cs=47334; Mark Chandler, "Cisco Supports Freedom of Expression, an Open Internet and Human Rights," The Platform, Cisco Blog, June 6, 2011, http://blogs.cisco.com/news/cisco-supports-freedom-of-expression-an-open-internet-and-human-rights/.

[135] Becker Polverin and William M. Pottenger, "Using Clustering to Detect Chinese Censorware," Eleventh Annual Workshop on Cyber Security and Information Intelligence Research, Article No. 30, 2011, http://www.cs.columbia.edu/~bpolveri/papers/Polverini-abstract-4pgs.pdf.

[136] "China," OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/china-including-hong-kong.

[137] Ibid.; Naomi Klein, "China's All-Seeing Eye," NaomiKlein.org, May 14, 2008, http://www.naomiklein.org/articles/2008/05/chinas-all-seeing-eye.

[138] "Beijing plans to track mobile phone users in real-time" [in Chinese], Yahoo News, March 3, 2009, http://news.cn.yahoo.com/ypen/20110303/237829.html.

[139] Cecilia Kang, "China Plans to Track Cellphone Users, Sparking Human Rights Concerns," Washington Post, March 3, 2011, http://voices.washingtonpost.com/posttech/2011/03/china_said_it_may_begin.html.

organization, and targets have led many experts to believe that they are either sponsored or condoned by Chinese military and intelligence agencies. The assaults have included distributed denial-of-service (DDoS) attacks on domestic and overseas groups that report on human rights abuses, such as Human Rights in China, Aizhixing, Boxun, Falun Gong websites, ChinaAid, and Chinese Human Rights Defenders.[140] In April 2011, the website Change.org, which at the time was carrying a petition calling for the release of Ai Weiwei that had quickly garnered tens of thousands of signatures, was disabled by a sophisticated DDoS attack reportedly originating in China.[141] In June 2011, Google reported that hundreds of Gmail accounts had been targeted by attacks originating in China. Among those targeted were "senior U.S. government officials, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists."[142] Other attacks appeared to have economic motives behind them. In February 2011, U.S. computer security firm McAfee reported that computer networks of at least five multinational oil and gas companies were attacked by a group of hackers based in China for information on oil and gas production systems and financial documents related to these companies' field operation.[143] Extensive cyberespionage networks traced back to China have been detected extending to 103 countries in an effort to spy on the Tibetan government-in-exile and its contacts, including Indian government facilities and foreign embassies.[144] In August 2011, the opposition Democratic Progressive Party in Taiwan charged that hackers from China and Taiwan had accessed their email accounts.[145]

The Chinese government has vigorously denied any involvement in these attacks.[146] Such denials were undermined by archive footage aired on a state-run television program in July

[140] Maggie Shiels, "Security Experts Say Google Cyber-Attack Was Routine," BBC, January 14, 2010, http://news.bbc.co.uk/2/hi/technology/8458150.stm; "ChinaAid Websites Collapse Under Repeated Malicious Cyber Attacks," Persecution.org, December 2, 2010, http://www.persecution.org/2010/12/02/chinaaid-websites-collapse-under-repeated-malicious-cyber-attacks/ .

[141] Benjamin Joffe-Walt, "Chinese Hackers Attack Change.org Platform in Reaction to Ai Weiwei Campaign," Change.org (blog), April 19, 2011, http://blog.change.org/2011/04/chinese-hackers-attack-change-org-platform-in-reaction-to-ai-weiwei-campaign/.

[142] "Ensuring your information is safe online," Google Official Blog, June 2, 2011, http://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html.

[143] "John Markoff, Hackers Breach Tech Systems of Oil Companies," New York Times, February 10, 2011 http://www.nytimes.com/2011/02/10/business/global/10hack.html.

[144] Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," April 6, 2010, http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0; Information Warfare Monitor, "Tracking Ghostnet: Investigating a Cyber Espionage Network," March 29, 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

[145] Chris Wang, "Hackers Attack DPP's Presidential Campaign Office," Taipei Times, Augest 10, 2011, http://www.taipeitimes.com/News/front/archives/2011/08/10/2003510374/1

[146] Michael Wines, "China Rejects Google's Hacking Charge," New York Times, June 6, 2011, http://www.nytimes.com/2011/06/07/world/asia/07china.html; Reuters, "China state newspaper disputes cyber-hacking involvement," Guardian, August 5, 2011, http://www.guardian.co.uk/technology/2011/aug/05/china-cyber-hacking-denied-mcafee; Michael Riley, "Morgan Stanley Attacked By China-Based Hackers Who Hit Google," Bloomberg, March 1, 2011, http://www.bloomberg.com/news/2011-02-28/morgan-stanley-network-hacked-in-same-china-based-attacks-that-hit-google.html.

2011, which included a demonstration of software designed by the Chinese military being used to carry out an attack on a Falun Gong-related website in the United States.[147] Similarly, in October 2011, the *Financial Times* reported that many of the 500 employees of Nanhao Group, a technology company based outside Beijing, are part of a militia unit organized by the People's Liberation Army (PLA) to specialize in cyberattacks and cyber defense.[148]

Chinese users have also been victims of cybercrime both from hackers based both inside and outside the country. The government-run National Computer Network Emergency Response Technical Team reported that Chinese computers were targeted in 2010 by about 480,000 Trojan horse viruses, nearly half originating from outside China.[149] In 2012, a military source reported that 8.9 million computers in China were infected with Trojan horse viruses controlled by IP addresses from outside the country.[150]

[147] Edward Wong, "China State TV Deletes Video Implying Hacking of Western Sites," New York Times, August 26, 2011, http://www.nytimes.com/2011/08/27/world/asia/27china.html; Ellen Nakashima and William Wan, "China's Denials About Cyberattacks Undermined By Video Clip," Washington Post, August 25, 2011, http://www.washingtonpost.com/world/national-security/state-media-video-candidly-depicts-chinas-developing-cyber-weaponry/2011/08/22/gIQAqyWkbJ_story.html; Ellen Nakashima and Jason Ukman, "Chinese cyberwar video goes missing," Washington Post, Auguest 25, 2011, http://www.washingtonpost.com/blogs/checkpoint-washington/post/chinese-vanish-cyberwar-video-that-caused-stir/2011/08/25/gIQAAK8edJ_blog.html; CCTV subsequently deleted the clip, but it is still viewable on YouTube: http://www.youtube.com/watch?v=L_Wu1HlZbBk&feature=youtu.be&t=36s.

[148] "China Tech Companies Have Army-Linked 'Cybermilitias,'" China Media News, October 13, 2011, http://www.chinamedia.com/2011/10/13/china-tech-companies-have-army-linked-cybermilitias/.

[149] Michael Kan, "China Hit by 480,000 Trojan Horse Attacks in 2010," PCWorld, Auguest 10, 2011, https://www.pcworld.com/businesscenter/article/237662/china_hit_by_480000_trojan_horse_attacks_in_2010.html.

[139] Jia Lei and Cui Meng, "Ma Xiaotian Appeals for Suppressing 'Cyber Armament Race'" [Ma Xiao Tian Yu E 'Wnag Luo Jun Bei Jing Sai'], Takungpao, May 29, 2012, http://www.takungpao.com.hk/news/12/05/29/ZM-1484251.htm.

CUBA

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	24	24
Limits on Content (0-35)	30	29
Violations of User Rights (0-40)	33	33
Total (0-100)	**87**	**86**

* 0=most free, 100=least free

POPULATION: 11 million
INTERNET PENETRATION 2011: 5 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/I USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Despite a slight loosening of restrictions on the sale of computers in 2008 and the important growth of mobile-phone usage in 2011, Cuba remains one of the world's most repressive environments for the internet and other information and communication technologies (ICTs). There is practically no access to internet applications other than email, given the slowness of the country's connectivity and high prices, and most users are restricted to an intranet for obtaining information. Hopes that a new fiber-optic cable announced in early 2011 would soon dramatically increase speeds were dashed a year later, as the project was engulfed with official silence and speculations about corruption. Surveillance is extensive, including special software designed to monitor and control many of the island's public internet access points.[1] Nevertheless, a growing community of bloggers has consolidated their work, creatively using online and offline means to express opinions and spread information about conditions in the country. In a positive development, access to many blogs was unblocked in early 2011, though they continued to be subjected to periodic travel bans and stints of arbitrary detention.

Cuba was connected to the internet for the first time in 1996, and the National Center for Automated Interchange of Information (CENIAI), the country's first internet service provider (ISP), was established that year. However, the executive authorities continue to

[1] "Prestaciones efectivas para redes informáticas" [Effective Features for Computer Networks], Radio Surco, April 11, 2009, http://www.radiosurco.icrt.cu/Ciencia.php?id=415 (site discontinued); Danny O'Brien, "The Malware Lockdown in Havana and Hanoi," CPJ Blog, June 8, 2010, http://cpj.org/blog/2010/06/the-malware-lockdown-in-havana-and-hanoi.php.

control the legal and institutional structures that decide who has access to the internet and how much access will be permitted.[2]

OBSTACLES TO ACCESS

According to the National Statistics Office, there were 2.6 million internet users in Cuba in 2011, representing 23.2 percent of the population.[3] However, the vast majority of internet users are only able to connect to a government intranet rather than the internet proper. Experts estimate that about 5 percent of Cubans periodically have access to the worldwide web via black market sales of minutes by those permitted to have such accounts.[4]

The Cuban government maintains tight control over the sale and distribution of internet-related equipment. After a nearly decade-long ban, in early 2008, the government began allowing Cubans to buy personal computers, and some individuals can now legally connect to an ISP with a government permit. However, this permit is granted only to certain people, mostly Cuban officials or "trusted journalists." The Nationl Statistics Office claimed a 46 percent gain in internet users in 2011, but only an 8 percent increase in networked computers, confirming the high percentage of people using shared computers and the lack of development in Cuba's ICT sector. Similarly, there was only a 3 percent increase in the number of domains registered, indicating that few enterprises or organizations are creating new websites.[5]

One segment of the population that enjoys approved access to the internet is the professional class of doctors, professors, and government officials. Facilities like hospitals, research institutions, and local doctors' offices are linked by an online network called Infomed. Home connections are not yet allowed for the vast majority of Cubans and only those favored by the government are able to access the internet from their own homes. However, even these users are typically restricted to e-mail and sites related to their occupations. For example, students at the Latin American School of Medicine in Havana are reportedly granted 40 minutes a week of internet access. During this time, students

[2] Ben Corbett, *This Is Cuba: An Outlaw Culture Survives* (Cambridge, MA: Westview Press, 2002), 145.
[3] National Office of Statistics and Information (ONEI), *Tecnología de la Información y la Comunicaciones en Cifras, Cuba 2011* [Information and Communication Technology, Cuba 2011] (Havana: ONEI, June 2012), http://www.one.cu/publicaciones/06turismoycomercio/TIC%20en%20Cifras%20Cuba%202011/TIC%20en%20Cifras%20Cuba%202011.pdf.
[4] "In Cuba Mystery Shrouds Fate of Internet Cable," Emerging Frontiers (blog), May 23, 2012, http://emergingfrontiersblog.com/2012/05/23/in-cuba-mystery-shrouds-fate-of-internet-cable/.
[5] Larry Press, "Updated Cuban ICT statistics," The Internet in Cuba (blog), July 26, 2012, http://laredcubana.blogspot.com.es/2012/07/updated-cuban-ict-statistics.html.

furiously upload pre-drafted emails and copy-paste content from their inbox to read later. Conducting online research or accessing academic journals is unfeasible.[6]

Most individuals who are able to access the internet face extremely slow connections, making the use of multimedia applications nearly impossible. In January 2010, the government announced that it had expanded the national bandwidth and achieved a 10 percent increase in international connectivity. According to official data, Cuba now has speeds of 209 Mbps for downloading and 379 Mbps for uploading.[7] However, once this national bandwidth is divided among even a small number of users, average speeds are still extremely slow.[8] Access over the intranet is similarly slow due to the weak domestic infrastructure.

In November 2010, the government announced that a fiber-optic cable was being installed between Cuba, Venezuela, and Jamaica, at a cost of approximately US$72 million, to improve the island's internet connection.[9] In February 2011, officials celebrated the arrival of the 1,600km (1,000 mile) cable laid by a consortium that included France's Alcatel-Lucent. Once fully connected, the cable is expected to increase data-transmission speeds 3,000-fold.[10] Nonetheless, experts say that even when the cable becomes active, the country's internal networks will need to be upgraded if average citizens are to have high-speed access. Many speculate that the first to benefit will be the limited few professional institutions and government offices that have relatively better access today.[11]

Over one year after the cable's reported connection, however, there is no sign of it functioning for public use, nor an official explanation for the delay. Rumors swirl about technical problems or corruption scandals.[12] Some observers speculate that the Cuban

[6] Graham Sowa, "Why Students in Cuba Need Internet," Havana Times, May 23, 2011, http://www.havanatimes.org/?p=44073.
[7] Amaury E. del Valle, "Cuba, la red sigue creciendo" [Cuba, the Network Continues to Grow], Juventud Rebelde, January 6, 2010, http://www.juventudrebelde.cu/suplementos/informatica/2010-01-06/cuba-la-red-sigue-creciendo/.
[8] Larry Press, "Past, Present, and Future of the Internet in Cuba," in *Papers and Proceedings of the Twenty-first Annual Meeting of the Association for the Study of the Cuban Economy (ASCE)* (Miami: ASCE, August 2011), http://www.ascecuba.org/publications/proceedings/volume21/pdfs/press.pdf.
[9] "Cable de fibra óptica une Venezuela, Cuba y Jamaica" [Fiber Optic Cable unites Venezuela, Cuba, and Jamaica], Ministerio de Educación Superior, accessed August 13, 2012, http://www.mes.edu.cu/index.php?option=com_content&view=article&id=82:cable-de-fibra-optica-une-venezuela-cuba-y-jamaica-&catid=1:ultimas-noticias&Itemid=25; "Llega a Cuba el cable submarine de fibra óptica para ofrecer internet de banda ancha" [Underwater Fiber Optic Cable Arrives in Cuba to Offer Broad Band Internet], El País, February 10, 2011, http://internacional.elpais.com/internacional/2011/02/10/actualidad/1297292404_850215.html.
[10] Curt Hopkins, "Cuba's Internet Capacity to Increase 3,000x," ReadWriteWeb (blog), February 13, 2011, http://www.readwriteweb.com/archives/cubas_internet_capacity_increased_by_3000_percent.php; International Telecommunication Union (ITU), "ITU hails connectivity boost for Cuba," news release, February 11, 2011, http://www.itu.int/net/pressoffice/press_releases/2011/CM03.aspx.
[11] Press, "Past, Present, and Future of the Internet in Cuba."
[12] "In Cuba Mystery Shrouds Fate of Internet Cable."

authorities have been spooked by the role of social media in the Arab Spring protests and decided to delay increasing access.[13] Another credible hypothesis is that the Cuban authorities are preparing to replace their current internet control strategy that is based on limiting access with a new model of monitoring, filtering, censored copycats of sites like Facebook, and increased activity by progovernment bloggers. As the latter mechanisms are not yet fully in place, the government is delaying opening up connectivity.[14]

Meanwhile, the government continues to blame the U.S. embargo for the country's connectivity problems, saying it must use a slow, costly satellite connection system and is limited in the space it can buy. However, President Barack Obama eased some aspects of Washington's prolonged trade sanctions in 2009 when he allowed U.S. telecommunications firms to enter into agreements to establish fiber-optic cable and satellite telecommunication facilities linking the United States and Cuba and to enter into roaming agreements with Cuban providers.[15] Cuba's leaders reiterated their demand for a complete end to the embargo, and official media ignored this important change in the U.S. legal framework. The bilateral relationship was affected by another incident in 2009 that touched directly on the lack of open internet access in Cuba. On December 4, the Cuban authorities arrested an American independent contractor, Alan Gross, who was in the country to set up individual satellite-based internet connections as part of a U.S. government–funded project. In March 2011, Gross was sentenced to 15 years in prison for committing an act "against the independence or territorial integrity of the state."[16]

High costs also put internet access beyond the reach of most of the population. A simple computer with a monitor averages around 722 convertible pesos (US$722) in retail outlets, or at least 550 convertible pesos (US$550) on the black market.[17] By comparison, the

[13] Nick Miroff, "In Cuba, Dial-Up Internet Is A Luxury," National Public Radio, December 14, 2011, http://www.npr.org/2011/12/14/143721874/in-cuba-dial-up-internet-is-a-luxury; "In Cuba Mystery Shrouds Fate of Internet Cable."

[14] In May 2012, Venezuela's science and technology minister told media that the cable was operational, but that it was up to the Cuban government how to employ it. Some experts reported that internet speeds had improved in the Ministry of Interior or other government offices, adding to speculation that the government maybe be using the cable, including to provide access for Venezuelan officials to Cuban government databases, while deliberately postponing having the cable benefit average users. "Venezuela: Fiber-optic cable to Cuba is working," Bloomberg Businessweek, May 24, 2012, http://www.businessweek.com/ap/2012-05-24/venezuela-fiber-optic-cable-to-cuba-is-working; Larry Press, "Hard data on the idle ALBA-1 undersea cable," The Internet in Cuba (blog), May 22, 2012, http://laredcubana.blogspot.com.es/2012/05/hard-data-on-idle-alba-1-undersea-cable.html.

[15] "Fact Sheet: Reaching Out to the Cuban People," The White House: Office of the Press Secretary, April 13, 2009, http://www.whitehouse.gov/the_press_office/Fact-Sheet-Reaching-out-to-the-Cuban-people.

[16] Ellery Roberts Biddle, "Cuba: US Contractor Sentenced to 15 Years in Prison," Global Voices, April 4, 2011, http://globalvoicesonline.org/2011/04/04/cuba-us-contractor-sentenced-to-15-years-in-prison/.

[17] Will Weissert, "Cubans Queue for Computers as PC Ban Lifted, But Web Still Outlawed," Irish Examiner, May 5, 2008, http://www.irishexaminer.com/archives/2008/0505/world/cubans-queue-for-computers-as-pc-ban-lifted-but-web-still-outlawed-61940.html.

average monthly Cuban salary is approximately 16 convertible pesos (US$16).[18] Computers are generally distributed by the state-run Copextel Corporation, which imports ICT equipment. Approximately 31 percent of Cubans report having access to a computer, but 85 percent of those said that the computers were located at work or school.[19] An internet connection in a hotel costs between 6 and 12 convertible pesos per hour.

Cuba still has the lowest mobile phone penetration rate in Latin America, but the number is rising fast. According to official reports, as of the end of 2011, 1.3 million Cubans—about 11 percent of the population—had a mobile phone,[20] a dramatic increase since 2009 when that figure was approximately 443,000.[21] The government eased restrictions on mobile phone purchases in March 2008, and during 2011 reduced the sign-up fee by more than half, though it still represents three months' wages for an average worker. Beginning in February 2012, the cost of a text message was halved and receiving phone calls from within Cuba was made free (previously, both caller and receiver paid a charge).[22]

Cuba has roaming agreements with 330 carriers in 135 countries, and 2.2 million people used those services in Cuba in 2010.[23] The island's mobile network reportedly covers 78 percent of Cuban territory, and further expansions are planned.[24] Most mobile phones do not include internet connections, but it is possible to send and receive international text messages and photographs with certain phones. Cuban customs regulations specifically

[18] "Mobile Phone Use Booms in Cuba Following Easing of Restrictions," Agence France-Presse, April 24, 2008.
[19] National Statistics Office (ONE), Republic of Cuba, *Tecnologías de la Información y las Comunicaciones en Cifras: Cuba 2009* [Information and Communication Technologies in Figures: Cuba 2009] (Havana: ONE, May 2010), http://www.one.cu/publicaciones/06turismoycomercio/TIC%20en%20Cifras%20Cuba%202009/TIC%20en%20Cifras%20Cuba%202009.pdf.
[20] Marc Frank, "More Cubans have local intranet, mobile phones," Reuters, June 15, 2012, http://www.reuters.com/article/2012/06/15/net-us-cuba-telecommunications-idUSBRE85D14H20120615; "ETECSA mobile phone users cross million mark," Cubastandard.com, July 14, 2010 http://www.cubastandard.com/2010/07/14/etecsa-mobile-phone-users-cross-million-mark; "Cuban cellphones hit 1 million, Net access lags," Reuters, July 7, 2011, http://www.reuters.com/article/2011/07/07/us-cuba-telecom-idUSTRE76661920110707; Amaury E. del Valle, "Cuba aumenta cantidad de teléfonos fijos y móviles" [Cuba Increases Quantity of Fixed and Mobile Telephones], Juventud Rebelde, December 26, 2011, http://www.juventudrebelde.cu/ciencia-tecnica/2011-12-26/cuba-aumenta-cantidad-de-telefonos-fijos-y-moviles/.
[21] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#. A good analysis of this dramatic increase and its economic benefits (in Spanish) in Emilio Morales, "Cuba: teléfonos celulares y llamadas costosas" [Cuba: cellphones and expensive calls], Café Fuerte, January 17, 2012, http://cafefuerte.com/cuba/noticias-de-cuba/economia-y-negocios/1474-cuba-telefonos-celulares-y-llamadas-costosas.
[22] "Telecoms in Cuba. Talk is cheap," Americas View (blog), The Economist, January 24, 2012, http://www.economist.com/blogs/americasview/2012/01/telecoms-cuba.
[23] "Syniverse holding back $2.5m in Cuban roaming charges," Cubastandard.com, October 21, 2011, http://www.cubastandard.com/2011/10/21/syniverse-holding-back-2-5m-in-cuban-roaming-charges/.
[24] Nick Miroff, "Getting Cell Phones Into Cuban Hands," Global Post, May 17, 2010, http://www.globalpost.com/dispatch/cuba/100514/cell-phone.

prohibit the entry of any phones that use the Global Position System (GPS) or satellite connections.[25]

The government divides access to web technology between the national intranet and the global internet. Most Cubans only have access to the former, which consists of a national email system, a Cuban encyclopedia, a pool of educational materials and open-access journals, Cuban websites, and foreign websites that are supportive of the Cuban government.[26] Cubans can legally access the internet only through government-approved institutions, such as the approximately 600 Joven Clubs de Computación (Youth Computer Clubs) and points of access run by ETECSA.[27] Users are generally required to present identification to use computers at these sites. Some neighborhoods in the main cities of Havana and Santiago advertise "internet" access in ETECSA kiosks, but field research has found that the kiosks often lack computers, instead offering public phones for local and international calls with prepaid phone cards. The government also claims that all schools have computer laboratories, while in practice internet access is usually prohibited for students or limited to email, supervised activities on the national intranet, or very short periods of access. In June 2009, the government adopted a new law (Resolution No. 99/2009) allowing the Cuban Postal Service, which is under the domain of the Ministry of Computers and Communications, to establish cybercafes at its premises and offer internet access to the public.[28] Since then, a small number have been slowly established.

Despite all of these barriers, Cubans still connect to the internet through both authorized and unauthorized points of access. Some are able to break through the infrastructural blockages by building their own antennas, using illegal dial-up connections, or developing blogs on foreign platforms. The underground economy of internet access also includes account sharing, in which authorized users sell access to those without an official account for one or two convertible pesos per hour. Some foreign embassies allow Cubans to use their facilities, but a number of people who have visited embassies for this purpose have reported police harassment. There is a thriving improvisational system of "sneakernets," in which USB keys and data discs are used to distribute material (articles, prohibited photos, satirical cartoons, video clips) that has been downloaded from the internet or stolen from government offices.

There are only two ISPs, CENIAI Internet and ETECSA, and both are owned by the state, though previously Telecom Italia was one of the latter's shareholders. In February 2011, the state-owned company Rafin S.A., a financial firm known for its connections to the military,

[25] See the website of Aduana General de la Republica de Cuba [Cuban Customs]: http://www.aduana.co.cu/turista.htm.
[26] ETECSA: Empressa de Telecomunicaciones de Cuba S.A., accessed August 28, 2010, http://www.etecsa.cu/.
[27] See the club system's website at http://www.cfg.jovenclub.cu/.
[28] Resolution No. 99/2009 was published in the Official Gazette on June 29, 2009.

bought Telecom Italia's 27 percent stake in ETECSA for US$706 million.[29] As a result, the telecom company is now completely owned by six Cuban state entities. Cubacel, a subsidiary of ETECSA, is the only mobile phone carrier. The government has used its control the cell phone network to selectively obstruct citizens' communications at politically sensitive times. Most recently, during the visit to the island of Pope Benedict XVI in March 2012, bloggers and dissidents reported that their cell phones were not working.[30] One independent journalist who investigated the situation found that calls were being automatically redirected to a phone number belonging to the Ministry of Interior.[31]

In 2000, the Ministry of Information Science and Communication was created to serve as the regulatory authority for the internet, and its Cuban Supervision and Control Agency oversees the development of internet-related technologies.[32]

LIMITS ON CONTENT

Rather than engaging in the technically sophisticated blocking and filtering used by other repressive regimes in countries like China, Cuban authorities rely heavily on lack of technology and prohibitive costs to limit users' access to information. The websites of foreign news outlets—including the British Broadcasting Corporation (BBC), *Le Monde*, and *El Nuevo Herald* (a Miami-based Spanish-language daily)—and human rights groups like Amnesty International, Human Rights Watch, and Freedom House remain largely accessible, though slow connection speeds impede access to the content on these sites.[33]

Nevertheless, beginning in 2007, the government systematically blocked core internet portal sites such as Yahoo, MSN, and Hotmail. In addition, until early 2011, the Cuban authorities had blocked access to websites and blogs run by individuals both inside and outside the country that contained independent reporting or views critical of the government. In February 2011, however, most of these blogs and international portals were unblocked for Cuban users accessing the worldwide web rather than the intranet. The group included the Bitácora Cubana blog and the Voces Cubana platform that hosts approximately

[29] Jerrold Colten, "Telecom Italia Sells Etecsa Stake to Rafin SA For $706 Million," Bloomberg, January 31, 2011, http://www.bloomberg.com/news/2011-01-31/telecom-italia-sells-etecsa-stake-to-rafin-sa-for-706-million.html.
[30] "Silenced During Papal Visit, Cuban Bloggers, Dissidents Speak Out (VIDEO)," Hispanically Speaking News, April 7, 2012, http://www.hispanicallyspeakingnews.com/notitas-de-noticias/details/silenced-during-papal-visit-cuban-bloggers-dissidents-speak-out-video/15038/.
[31] Juan O. Tamayo, "Cuba diverts dissidents' phone numbers in pope crackdown," The Miami Herald, March 30, 2012, http://www.miamiherald.com/2012/03/30/2723658/cubas-interior-ministry-left-fingerprint.html.
[32] The ministry's website can be found at http://www.mic.gov.cu/.
[33] Reporters Without Borders, "Free Expression Must Go With Better Communications, Says Reporters Without Borders as Blogs Prove Hard to Access," news release, March 31, 2008, http://en.rsf.org/cuba-free-expression-must-go-with-31-03-2008,26396.html.

40 blogs, including Yoani Sánchez's well-known Generación Y blog, which reportedly draws 26 percent of its readers from within Cuba.[34] No official explanation was offered for the sudden unblocking, but it remained in effect as of May 2012.

Some websites, such as Cubanet (run by an independent journalist in Cuba but hosted on overseas servers), Payolibre (a dissident news website), and the Association for Freedom of the Press remain inaccessible from government-sponsored youth computer centers.[35] In addition, Revolico, a platform for posting classified advertisements, continues to be blocked, despite the apolitical nature of its content.[36] Moreover, Voice over Internet Protocol (VoIP) remains blocked in Cuba, with the exception of unauthorized points of connection in old Havana. Some social-networking platforms such as Facebook and Twitter are accessible from university cybercafes and other locations, although with varying consistency. Most Cuban Twitter users access the microblogging service from a computer rather than a mobile phone and the cost of sending a message is approximately US$1, more than the average daily income.

Resolution 179 from 2008 requires ISPs to censor a range of vaguely defined materials. It specifically authorizes ETECSA to "take the necessary steps to prevent access to sites whose contents are contrary to social interests, ethics and morals, as well as the use of applications that affect the integrity or security of the State." In practice, ETECSA does not proactively police the networks and delete content. However, some bloggers have reportedly removed certain posts criticizing government actions, apparently after receiving threats from officials.[37]

It is a crime to contribute to international media that are not supportive of the government, a fact that has led to widespread self-censorship. Cuban blogs typically feature implicit or explicit instances of self-censorship and anonymity. Many of those working with ICTs are journalists who have been barred from official employment, and the prohibitive costs surrounding the technology represent a major obstacle for them. The majority of their work is done offline by hand, typewriter, or computer, then uploaded and published once or

[34] Nelson Acosta and Esteban Israel, "Cuba unblocks access to controversial blog," Reuters, February 8, 2011, http://ca.reuters.com/article/topNews/idCATRE7175YG20110208; Monica Medel, "Bloggers celebrate as Cuba unblocks their sites," Journalism in the Americas Blog, http://knightcenter.utexas.edu/blog/bloggers-celebrate-cuba-unblocks-their-sites.

[35] Bitácora Cubana can be found at http://cubabit.blogspot.com/; Asociación pro Libertad de Prensa (the Association for Freedom of the Press) can be found at http://prolibertadprensa.blogspot.com/.

[36] Marc Lacey, "A Black Market Finds a Home in the Web's Back Alleys," New York Times, January 3, 2010, http://www.nytimes.com/2010/01/04/world/americas/04havana.html; Peter Orsi, "Cuba's next step on capitalist road: advertising," Boston.com, June 16, 2012, http://www.boston.com/news/world/latinamerica/articles/2012/06/16/cubas_next_step_on_capitalist_road_advertising/.

[37] See for example: http://cafefuerte.com/cuba/noticias-de-cuba/sociedad/2050-malestar-por-cambio-de-edificio-del-partido-comunista-en-camagueey, and http://elyuma.blogspot.com.es/2012/07/ljc-orwellian-memory-hole-google-cache.html.

twice a week using a paid internet access card. For those contributing to international outlets, content can be dictated via costly international phone calls.

There is no exact count of blogs produced in Cuba, but the Cuban Journalists' Union (UPEC) has reported a current total of 174, including sites like Retazos and Convivencia. Independent websites hosted outside the country like La Polemica Digital, Havana Times, or Estado de Sats provide the few able to access the net with a more differentiated and rich selection of news sources than is available from state-run media. Regional radio stations and magazines are also creating online versions, though these are state-run and do not accept contributions from independent journalists. However, in a recent development, some of these official sites have installed commentary tools that allow readers to provide feedback and foster discussion, albeit censored.

In recent years, Yoani Sánchez has become the most visible figure in an independent blogging movement that uses new media to report on daily life and conditions in Cuba that violate basic freedoms. She and other online writers—including Claudia Cadelo, Miriam Celaya, Orlando Luis Pardo, Reinaldo Escobar, Laritza Diversent, and Luis Felipe Rojas—have come together on the Voces Cubanas blogging platform to portray a reality that official media ignore, earning broad support throughout society. They have made it "trendy" to exercise the right to free expression.

Young people are increasingly using the Twitter microblogging service and mobile phones to document repression, voice their opinions, and spread leaks of prohibited information. These have included details exposing government corruption or other abuses. For example, the "Hablalo Sin Miedo" (Speak without Fear) platform enables Cuban residents to call a phone number in the United States and record anonymous messages describing government abuses or other grievances. The messages are then automatically converted into posts shared via Twitter and YouTube.[38] In a rare incident, in November 2011, Yoani Sánchez and other activists had a direct, unfiltered exchange of views with Mariela Castro, the daughter of President Raul Castro, during which the latter referred to the bloggers as "despicable parasites."[39] As of June 2012, Sánchez's followers on Twitter totaled over 260,000, though only a small percentage were from within Cuba.[40]

Unable to completely suppress dissident activity on the internet through legal and infrastructural constraints, the authorities have taken a number of countermeasures. First,

[38] "Acerca de" [About us], Háblalo Sin Miedo, accessed on August, 13, 2012, http://www.hablalosinmiedo.com/p/como-funciona.html.
[39] Jeff Franks, "Castro daughter, dissident blogger clash on Twitter," Reuters, November 8, 2011, http://www.reuters.com/article/2011/11/09/us-cuba-twitter-castro-idUSTRE7A806Y20111109.
[40] Yoani Sanchez's twitter page, accessed August 13, 2012, https://twitter.com/#!/yoanisanchez/.

they have sought to dominate conversations within the medium itself. Government entities maintain a major presence on social networks, and they rely on trusted students at the University of Computer Sciences to help fight the "internet campaigns against Cuba." The authorities have also created official blogs designed to slander and criticize the independent bloggers.[41] According to the Committee to Protect Journalists, the government announced in February 2011 that it had recruited about 1,000 such bloggers.[42] These bloggers often accuse government critics of being financed by the U.S. government or post damaging rumors about their personal lives. In February 2011, an apparently leaked video of a Cuban government expert giving a room of intelligence agents a crash course on social media was uploaded to the internet.[43] In the video, the lecturer emphasizes how these new technologies are being used around the world by activists and warns that bloggers such as Yoani Sánchez have become well-known on Twitter and could organize protests in Havana similar to those that occurred in Iran in 2009. He concludes by saying the government must respond to these threats.

Second, the government has launched its own versions of popular websites, such as Facebook and Wikipedia, though with little success. The online encyclopedia Ecured, unveiled in December 2010, uses similar software and layout as its international counterpart. However, a cursory review indicates that only a small number of people update it, rather than an interactive community, and that it consists of 78,000 articles compared to several million on Wikipedia. Attempts to create an editor profile using a ".edu" or Gmail email account were reportedly rejected.[44] More recently, in December 2011, a social-networking website called Red Social was launched. Its layout uncannily matched Facebook to the point that some observers questioned whether it was a violation of copyright. The site was accessible only from Cuba's intranet, though according to one local blogger, shortly after its launch, it appeared to no longer be functioning, possibly a reflection of the lack of server capacity to maintain it.[45]

[41] A few examples include Cambios en Cuba, http://cambiosencuba.blogspot.com/; Yohandry's blog, http://yohandry.wordpress.com/; and the official bloggers platform CubaSí, http://www.cubasi.cu.
[42] Committee to Protect Journalists (CPJ), *After the Black Spring, Cuba's New Repression* (New York: July 6, 2011), http://cpj.org/reports/CPJ.Cuba.Report.July.2011.pdf.
[43] The video (more than 53,000 views) on Vimeo: "La ciber policia en Cuba" [The cyber police in Cuba], Vimeo video, 53:08, posted by "Coral Negro," January 31, 2011, http://vimeo.com/19402730; English transcription: http://translatingcuba.com/?p=7111; the identification process: "Acuse de recibo: ¿Quién es el ciberpolicía?" [Acknowledgement of Recepit: Who is the Cyber Policeman?], Penúltimos Días, February 5, 2011, http://www.penultimosdias.com/2011/02/05/acuse-de-recibo-18/.
[44] Larry Press, "Ecured is not open like Wikipedia," The Internet in Cuba (blog), December 21, 2011, http://laredcubana.blogspot.com/2011/12/ecured-is-not-open-like-wikipedia.html.
[45] "The Cuban Facebook Imitation Saga – Red Social (Social Facebook)," The Philandrist (blog), December 6, 2011, http://thephilandrist.wordpress.com/2011/12/06/the-cuban-facebook-imitation-saga-redsocial/.

VIOLATIONS OF USER RIGHTS

The legal structure in Cuba is not favorable to internet freedom. The constitution explicitly subordinates freedom of speech to the objectives of a socialist society,[46] and freedom of cultural expression is guaranteed only if the expression is not contrary to the Revolution.[47] The penal code and Law 88 set penalties ranging from a few months to 20 years in prison for any activities that are considered a "potential risk," "disturbing the peace," a "precriminal danger to society," "counterrevolutionary," or "against the national independence or economy."[48]

In 1996, the government passed Decree-Law 209, which states that the internet cannot be used "in violation of Cuban society's moral principles or the country's laws," and that email messages must not "jeopardize national security."[49] In 2007, Resolution 127 on network security banned the spreading via public data-transmission networks of information that is against the social interest, norms of good behavior, the integrity of people, or national security. The decree requires access providers to install controls that will enable them to detect and prevent the proscribed activities, and to report them to the relevant authorities.

Resolution 56/1999 provides that all materials intended for publication or dissemination on the internet must first be approved by the National Registry of Serial Publications. Moreover, Resolution 92/2003 prohibits email and other ICT service providers from granting access to individuals who are not approved by the government, and requires that they enable only domestic chat services, not international ones. Entities that violate these regulations can have their authorization to provide access suspended or revoked.

Despite constitutional provisions that protect various forms of communication, and portions of the penal code that set penalties for the violation of the secrecy of communications, the privacy of users is frequently violated in practice. Tools of content surveillance are pervasive, from public access points and universities to government offices. Resolution 17/2008, which spells out the conditions and procedures to become an ISP, requires ISPs to register and retain the addresses of all traffic for at least a year.[50] The government also routes most connections through proxy servers and is able to obtain all user names and passwords through special monitoring software Avila Link, which is installed at most

[46] Article 53, available at http://www.cubanet.org/ref/dis/const_92_e.htm, accessed July 23, 2010.
[47] Article 39, d), available at http://www.cubanet.org/ref/dis/const_92_e.htm, accessed July 23, 2010.
[48] "International Guarantees and Cuban Law," Committee to Protect Journalists, March 1, 2008, http://cpj.org/reports/2008/03/laws.php.
[49] Reporters Without Borders, "Going online in Cuba: Internet under surveillance," http://www.rsf.org/IMG/pdf/rapport_gb_md_1.pdf.
[50] "Internet En Cuba: Reglamento Para Los Proveedores De Servicos De Acceso A Internet" [Internet in Cuba: Regulations for Internet Service Providers], CubanosUsa.com, December 18, 2008, http://cubanosusa.com/opinion/editorial/42454-internet-en-cuba-reglamento-proveedores-acceso-internet.html.

ETECSA and public access points. In addition, delivery of email messages is consistently delayed, and it is not unusual for a message to arrive without its attachments.

The government continues to repress independent journalism and blogging with detentions, fines, searches, and confiscation of money and equipment. There have been a few cases in which online journalists were imprisoned for their work, most notably two correspondents for Cubanet. One of them was sentenced to four years in prison in April 2007 for "precriminal social danger," and the other was sentenced to seven years in November 2005 for "subversive propaganda." Both were released as part of a broader pardon of prisoners in December 2011.

Under Raul Castro, the Cuban government appears to have shifted its repressive tactics from long-term imprisonment to extralegal detentions, intimidation, and harassment.[51] Bloggers have been summoned for questioning, reprimanded, and had their domestic and international travel rights restricted.[52] In October 2011, Dania Virgen García, a blogger and journalist, was reportedly detained and beaten along with her husband when trying to visit the home of the late Laura Pollán shortly after the founder of the opposition group Ladies in White passed away; the pair was released within a few days.[53] In March 2012, during the Pope's visit to Cuba, dozens of bloggers were placed under house arrest or detained and held throughout the Pope's three-day stay, then released.[54] In February 2011, the Cuban government denied Yoani Sánchez an exit permit for the 19th time in four years.[55] That same month, student Reyner Agüero was expelled from the University of Information Sciences for giving an interview to an anti-Castro blog. The document affirming his three-year expulsion explained that the reason was "unauthorized use of the …information technologies that were provided at no cost by the institution for [students'] studies."[56]

[51] Committee to Protect Journalists (CPJ), *After the Black Spring, Cuba's New Repression*.
[52] Daisy Valera, "This Cuban Woman and Her Online Indiscipline," Havana Times, March 11, 2012, http://www.havanatimes.org/?p=64077; Steven L. Taylor, "Cuba vs. the Bloggers," PoliBlog, December 6, 2008, http://www.poliblogger.com/index.php?s=cuba+bloggers; Marc Cooper, "Cuba's Blogger Crackdown," Mother Jones, December 8, 2008, http://www.motherjones.com/politics/2008/12/cubas-blogger-crackdown.
[53] David Águila Montero, "Golpeada y detenida Dania Virgen" [Beaten and Detained Dania Virgen], Payolibre.com, October 19, 2011, http://www.payolibre.com/noticias/noticias2.php?id=8304; Marc R. Masferrer, "Cuban independent journalist/blogger Dania Virgen Garcia beaten, arrested (UPDATED x 2))," Uncommon Sense (blog), October 21, 2011, http://marcmasferrer.typepad.com/uncommon_sense/2011/10/cuba-independent-journalistblogger-dania-virgen-garcia-beaten-arrested.html.
[54] Silenced During Papal Visit, Cuban Bloggers, Dissidents Speak Out (VIDEO)," Hispanically Speaking News.
[55] "Cuban blogger blocked from travelling to film premiere in Brazil," Amnesty International, February 6, 2012, http://www.amnesty.org/en/news/cuban-blogger-blocked-travelling-film-premiere-brazil-2012-02-06.
[56] Gif of document linked here: http://www.penultimosdias.com/wp-content/uploads/2011/03/documento.gif.

EGYPT

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	12	14
Limits on Content (0-35)	14	12
Violations of User Rights (0-40)	28	33
Total (0-100)	**54**	**59**

* 0=most free, 100=least free

POPULATION: 82 million
INTERNET PENETRATION 2011: 36 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

During the opening months of 2011, the world witnessed a series of demonstrations that soon toppled Hosni Mubarak's 30-year presidency. The Egyptian revolution received widespread media coverage during the Arab Spring not only because of Egypt's position as a main political hub in the Middle East and North Africa, but also because activists were using different forms of media to communicate the events of the movement to the world. While the Egyptian government employed numerous tactics to suppress the uprising's roots online—including by shutting down internet connectivity, cutting off mobile communications, imprisoning dissenters, blocking media websites, confiscating newspapers, and disrupting satellite signals in a desperate measure to limit media coverage—online dissidents were able to evade government pressure and spread their cause through social-networking websites. This led many to label the Egyptian revolution the Facebook or Twitter Revolution.

Since the introduction of the internet in 1993, the Egyptian government has invested in internet infrastructure as part of its strategy to boost the economy and create job opportunities. The Telecommunication Act was passed in 2003 to liberalize the private sector while keeping government supervision and control over information and communication technologies (ICTs) in place. To assure its power, the government used multilayered measures to control ICTs, which have varied from establishing restrictive laws and regulations, to monitoring dissidents and limiting their ability to disseminate political messages online. In several cases, the government used its security arm to intimidate, harass, and detain activists.

These actions, however, did not prevent Egyptians from developing online groups and interacting in virtual communities to discuss issues of common concern. For activists, internet technologies, especially social media websites, have provided not only a tool to access information but also a medium to create a new, virtual world with the powerful ability to influence the real world. Meanwhile, the former regime underestimated the power of the internet, seeing it a space for the opposition to vent.

The current governing authorities in Egypt now have a keener understanding of the revolutionary power of the internet, especially social media. When the Supreme Council of Armed Forces (SCAF) took over the government in February 2011, the military administration maintained many of its predecessor's tactics of control over ICTs, keeping mobile phones, the internet, and social media under vigorous surveillance. Furthermore, new high-tech tools were installed to monitor cyber discussions, and throughout 2011 and early 2012, several activists and bloggers were intimidated, beaten, or tried in military courts for "insulting the military power" or "disturbing social peace."

OBSTACLES TO ACCESS

Recognizing the importance of a strong ICT sector for sustainable economic growth, the Egyptian government long considered the development of the information technology (IT) sector a national priority. In 1999, the government established a Ministry of Communication and Information Technology headed by Ahmed Nazif, who in July 2004 became the last prime minister of Egypt in Mubarak's era.[1] As prime minister, Nazif led a technocrat/business-focused government that believed technology could be controlled and managed if steered by the right policies.[2] Indeed, the Egyptian IT sector developed rapidly over the past decade, with over 2,000 IT companies generating an average of US$7.6 billion for the Egyptian economy per year.[3] Furthermore, the Egyptian ICT industry experienced an annual growth rate of 13 percent between 2004 and 2010 and continued to grow in 2011, despite the economic uncertainty following the events of early 2011.[4]

[1] Sherif Kamel, Dina Rateb, and Mohamed El-Tawil, "The Impact of ICT Investments on Economic Development in Egypt," *The Electronic Journal of Information Systems in Developing Countries* 36 (2009), http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/524/264.
[2] "Technology Innovation and Entrepreneurship Strategy, 2011-2014," Technology Innovation and Entrepreneurship Center, January 2011, http://tiec.gov.eg/backend/Publications%20Files/TIEC_Strategy.pdf.
[3] Ahmed El Gody, *Journalism in a Network: The Role of ICTs in Egyptian Newsrooms* (Örebro: Örebro University Press, 2012).
[4] "Egypt Information Technology Report Q4 2011," Blackmere, March 3, 2012, http://www.transworldnews.com/1024048/c1/egypt-information-technology-report-q4-2011-new-market-research-report.

Internet use in Egypt has increased rapidly, with internet penetration growing from 12.6 percent in 2006 to 35.7 percent in 2011.[5] Further, the number of high-speed internet users reached 18 million households with a 33 percent monthly increase, though there are reports that eight million households using high-speed internet share the connection, often illegally. Meanwhile, Egypt's mobile phone penetration rate stood at nearly 102 percent in 2011, increasing from approximately 24 percent in 2006.[6]

Although these figures are promising, there are a number of obstacles hindering access to ICTs, including a high computer illiteracy rate,[7] poor telecommunications infrastructure, particularly in rural areas and slums, and flagging economic conditions, with nearly a fifth of the population living below the national poverty line.[8] Moreover, ICTs are often viewed with suspicion, and women's access to technology has become a growing concern especially in rural areas.[9]

With Egyptian society becoming increasingly electronic, more people are going online to create a parallel information and communication system to bypass the government's feeble one. Until 2010, the Egyptian government showed a relaxed attitude towards access of ICTs and did not censor websites or use high-end technologies to block online discussions. On the contrary, the government removed many of the obstacles experienced in neighboring Arab countries, for example, by enabling access to the encrypted BlackBerry instant messaging service.[10] However, with the rise of online dissidents, the authorities started to change its attitude towards internet access.

The January 2011 revolution revealed a centralized ICT system with a relatively small number of fiber-optic cables and a few companies that are beholden to strict license rules and government regulations.[11] For example, although Egypt has 214 internet service providers (ISPs), the country's bandwidth is controlled by a handful of providers—Egypt

[5] Ibid.; International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[6] According to official statistics by the Ministry of Communication and Information Technology, the number of mobile phone lines reached 91.3 million, reflecting a penetration rate of 112.3 percent as of January 2012. "ICT Indicators in Brief, February 2012 Monthly Issue," Ministry of Communication and Information Technology, February 2012, http://mcit.gov.eg/Upcont/Documents/Publications_442012000_Eng%20Flyer-Feb2012-3.pdf.

[7] Estimated at 94 percent in 2007. "Computer Literacy & Broadband in Egypt," Ashoka Arab World (blog), December 12, 2007, http://ashokaarabworld.wordpress.com/2007/12/12/computer-literacy-broadband-in-egypt/.

[8] http://data.worldbank.org/indicator/SI.POV.NAHC/countries/EG?display=default

[9] Ahmed El Gody, *New Media New Audience New Topics and New forms of Censorship in the Middle East* (New York: Palgrave, 2008).

[10] "Country profile: Egypt," Africa & Middle East Telecom News, 2012, http://www.africantelecomsnews.com/resources/AfricaOpp_Egypt.shtml; Shorouk El Hariry and Marine Weitzmann, "Egypt's BlackBerry users anxious over regional bans," The Daily News Egypt, August 5, 2010, http://www.thedailynewsegypt.com/people/blackberry-users-anxious-over-possible-ban-dp1.html.

[11] CircleID Reporter, "Egyptian Government Shuts Down Most Internet and Cell Services," CircleID, January 28, 2011, http://www.circleid.com/posts/egyptian_government_shuts_down_most_internet_and_cell_services/.

Telecom, Internet Egypt, Vodafone/Raya Etisalat Misr, and TE Data—which together manage Egypt's internet traffic.[12] Although these ISPs are privately-owned, the Egyptian government maintains tight control through strict rules and regulations as well as by monitoring their performance.[13]

Government control over online access made it easy to block internet traffic in less than an hour on January 27, 2011 following the revolutionary demonstrations. The government shut down almost all of its Border Gateway Protocol routes, which disconnected the country from the global network.[14] Only the Noor service provider (which served the country's cabinet, public banks, and Egypt's airways) was left operating but was denied service couple of days later after several activists began accessing the network from a local office in Alexandria.[15] Similarly, mobile operators were ordered to cut all mobile phone service, including mobile internet and SMS (short message service) text-messaging, under the pretext that "foreign intelligence [was] using communication technologies to plan terrorist actions," according to State Intelligence.[16] In an interview, Mobinil founder Naguib Sawiris stated that under the company's terms of agreement, the government had the right to cancel any or all mobile services when necessary.[17]

During the events of January 2011, the government also shut down the main point of entry for international submarine fiber-optics, the Ramsis Exchange, and its two exchange points, the Cairo Regional Internet Exchange and the Middle East Internet Exchange. To restrict media coverage, the government distorted NileSat's television signals and limited the availability of data bandwidth. The unprecedented restrictions created widespread international condemnation of the Egyptian government,[18] which in part led the authorities to restore internet connectivity on February 2, 2011. In addition, the heavy filtering in place at the height of the revolution ostensibly came to an end, and imprisoned online activists were released. News reports speculated that the authorities unblocked the internet to make

[12] Christopher Williams, "How Egypt shut down the internet," The Telegraph, January 28, 2011, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html.
[13] Ahmed El Gody, *New Media New Audience New Topics and New forms of Censorship in the Middle East*.
[14] Iljitsch van Beijnum, "How Egypt did (and your government could) shut down the Internet," Ars Technica, January 30, 2011, http://arstechnica.com/tech-policy/news/2011/01/how-egypt-or-how-your-government-could-shut-down-the-internet.ars.
[15] Peter Bright, "Amidst chaos and riots, Egypt turns off the Internet," Ars Technica, January 28, 2011, http://arstechnica.com/tech-policy/news/2011/01/amidst-chaos-and-riots-egypt-turns-off-the-internet.ars.
[16] Ameera Fouad, "Saying no to mobile phones," Al-Ahram Weekly Online, Issue No. 1083, February 2-8, 2012, http://weekly.ahram.org.eg/2012/1083/eg402.htm.
[17] Stephanie Baker and Mahmood Kassem, "Billionaire Facing Death Threats Says Egypt Risks Becoming Iran," Bloomberg, October 26, 2011, http://www.bloomberg.com/news/2011-10-26/billionaire-facing-death-threats-says-egypt-risks-becoming-iran.html.
[18] Ryan Singel, "Report: Egypt Turned Off the Net With a Big Switch, Not Phone Calls," Wired, February 10, 2011, http://www.wired.com/threatlevel/2011/02/egypt-off-switch/.

it easier to monitor dissidents' discussions and plans of actions online, since it was more difficult to monitor events as they unfolded on the ground.[19]

In lieu of blocking, the SCAF limited internet connectivity by throttling certain websites in the months following February 2011, especially during major demonstrations like those at Maspiro in October and Mohamed Mahmoud Street in November,[20] where violent clashes arose between the military authorities and protestors. During the 2011 parliamentary elections, several websites and news portals including Al Dostor, Youm7, and Al Shorouk reported slow networks and service time-outs, suspecting foul play by the SCAF. Activists and social media outlets, such as 6th of April, had similar complaints hinting that the ruling military regime was still using old tactics of controlling internet access to suppress dissident activity.

Both mobile service providers and ISPs are regulated by the National Telecommunication Regulatory Authority (NTRA) and governed by the 2003 Telecommunications Regulation Law. As of early 2012, NTRA's board is chaired by the Minister of Communications and Information Technology and includes representatives from the SCAF, national security forces, and Ministries of the Interior, Defense, Intelligence, Finance, and Information.[21] Officially, the NTRA is responsible for establishing telecommunication development plans, such as the eMisr high-speed internet, and building the capacity of mobile operations in Egypt. The NTRA also analyzes the telecommunication market and publishes research to draw investments.[22] However, there have been some reports revealing the NTRA's ties to online access control and surveillance activities, such as controlling the database of mobile subscribers and mobile short messages (especially those of news website services), as well as monitoring social media applications such as WhatsApp.[23]

LIMITS ON CONTENT

During the January 2011 revolution, social-networking websites helped spread ideas of discontent among Egyptians by calling them to join in protest and put pressure on the

[19] Erica Chenoweth, "Backfire in the Arab Spring," Middle East Institute, September 1, 2011, http://www.mei.edu/content/backfire-arab-spring.
[20] Ben Wedeman and Ivan Watson, "Military police try to halt Cairo skirmishes," CNN, November 23, 2011, http://articles.cnn.com/2011-11-23/africa/world_africa_egypt-protests_1_mohamed-hussein-tantawi-riot-police-cairo-s-tahrir-square?_s=PM:AFRICA.
[21] "About Us: Board Members," National Telecommunication Regulatory Agency, accessed July 16, 2012, http://www.tra.gov.eg/english/DPages_DPagesDetails.asp?ID=175&Menu=5.
[22] "Our New National Telecommunication Regulatory Agency" [in Arabic], NTRA, accessed July 16, 2012, http://www.ntra.gov.eg/arabic/News_GetNewsList.asp?ID=39.
[23] Ahmed El Bermawy, "NTRA deny monitoring social media and sms" [in Arabic], Masress, June 20, 2012, http://masress.com/dostor/65762.

Egyptian government. Activists used Twitter to highlight local events, drawing global attention to what was happening on the ground and directly informing Western media coverage. State police admitted that it monitored online dissident discussions, but they underestimated the magnitude of offline protestors.[24] For that reason, in the wake of the demonstrations, the government blocked Twitter, Bambuser, and Facebook websites, and arrested several bloggers, dissidents, activists, and human rights figures in an attempt to control online discussions. Soon, the government censored five of the Muslim Brotherhood websites and disseminated denial-of-service (DoS) messages to media portals including Al Jazeera, BBC Arabic, and Al Arabiya. Other news websites like Al Youm7 and Al Dostor reported slow networks and usual cut-offs.[25]

Losing control over news coverage to social media, the Egyptian government decided to shut down the internet altogether on January 27, 2011. Egypt's netizens, however, found ways to circumvent the government ban. For example, activists began using mobile and satellite mobiles to send short messages for broadcast by Egyptians abroad.[26] Since fixed-phone lines were still working, foreign ISPs in France and Sweden offered modem connections to produce content. Meanwhile, Google and Twitter set up a system of voice tweets whereby people could call a foreign number and leave messages that were instantly posted on Twitter under the hashtag, "#egypt."[27]

The authorities decided to unblock internet access on February 2, 2011, likely because it was harder for Egyptian security forces to control online communications and monitor netizens' plans while Egypt was offline. Once internet and mobile services were restored, the government forced mobile operators to send out messages urging subscribers to participate in pro-government rallies. The government adopted the same tactic with the internet, using public figures to post pro-government messages on their webpages and Facebook accounts. The SCAF created its own group on Facebook to communicate with protestors and to ease the tension between the rebel group in Tahrir Square and the regime. "One of our key weapons was spreading rumors to manipulate the street," stated General Abdel Moneim Qato in a TV interview.[28]

[24] Sam Gustin, "Social Media Sparked, Accelerated Egypt's Revolutionary Fire," Wired, February 11, 2011, http://www.wired.com/epicenter/2011/02/egypts-revolutionary-fire/.
[25] "Egypt Bans Twitter: Access Twitter in Egypt using Proxy Websites and Free VPN," Internet Techies, January 26, 2011, http://www.clickonf5.org/11397/egypt-bans-twitter-access-using-proxy-vpn/.
[26] Calvert Collins, "Social Media Plays Pivotal Role in Egypt's Revolution," 8 News Now, February 14, 2011, http://www.8newsnow.com/story/14029788/social-media-plays-pivotal-role-in-egypts-revolution.
[27] Emma Batha, "TechnoTalk - Google and Twitter help Egyptians bypass Internet closure," AlertNet, February 1, 2011, http://www.trust.org/alertnet/blogs/technotalk/google-and-twitter-help-egyptians-bypass-internet-closure/.
[28] Mohamed El Dahshan, "The Sacking of Dina Abdul Rahman is a threat to the freedom of Media in Egypt," Index on Censorship (Uncut blog), August 5, 2011, http://uncut.indexoncensorship.org/2011/08/the-sacking-of-dina-abdul-rahman-is-a-threat-to-the-freedom-of-media-in-egypt/.

After the revolution ended in February 2011, social networking became the new political playground. All emerging political parties, the Egyptian government, and the military body started actively participating in online forums, engaging with the public in discussions about the current state of the country. Several Facebook groups and Twitter accounts were created to win over Egyptian hearts and minds. The number of Facebook users reached over 10.6 million users by the end of 2011, placing Egypt in the top 20 countries using Facebook.[29] Similarly, the number of YouTube users increased to over eight million, the most in the Arab world. Several activists established websites to monitor government and SCAF activities, especially during the March 2011 referendum and following the parliamentary elections in late 2011.

Online content is still sometimes removed in questionable circumstances. For example, blogger and labor activist Hossam el-Hamalawy had certain photos from his Flickr account deleted in May 2011 by Flickr administrators due to copyright infringement allegations.[30] El-Hamalawy's Flickr account was known for its large collection of photos of Egypt's state security service taken by protestors attending demonstrations since 2008. However, only in March 2011 did Flickr intervene with charges of copyright infringement after el-Hamalawy had posted the profile pictures of security agents found on a disk when activists stormed the state security headquarters. Although the posting of images taken by someone else is indeed against Flickr's terms of use, it appeared as though a sufficient number of pro-government users had alleged copyright infringement, leading to the deletion of the photos even though the content was of public significance. Similar tactics were used previously by the Mubarak government and its sympathizers, who were able to file complaints based on Facebook's official terms of use to temporarily disable two large Facebook groups, one of which played a crucial role in the uprising.

Despite government's efforts to suppress dissenting voices (see "Violations of User Rights"), the internet has continued to grow rapidly as a source of information and news for the country's citizens. Until 2005, Egyptian online content did not exceed a few hundred thousand webpages, but over the following few years, the number of pages surpassed the 20 million mark.[31] To many, this increase has been the result of the rise of independent media, citizen journalism, and bloggers. Regionally, Egyptian news websites are some of the most visited websites in the Middle East, with 45 percent of online news content from of the Arab

[29] "Egypt Facebook Statistics," Socialbakers, accessed July 18, 2012, http://www.socialbakers.com/facebook-statistics/egypt/last-3-months#chart-intervals.
[30] Uri Friedman, "Egyptian Blogger Renews Censorship Charge Against Flickr," The Atlantic News Wire, May 11, 2011, http://www.theatlanticwire.com/global/2011/05/egyptian-blogger-renews-censorship-charge-against-flickr/37559/.
[31] Tim Eaton, "Online activism and revolution in Egypt: Lessons from Tahrir," New Diplomacy Platform, January 25, 2012, http://www.newdiplomacyplatform.com/portfolio/online-activism-and-revolution-in-egypt-lessons-from-tahrir/.

world coming from Egypt.[32] In both 2010 and 2011, Forbes rated the Al Youm7 news portal as the most visited electronic news site in the Middle East.[33]

Online news websites have begun to replace traditional news sources due to their immediate and interactive nature, and because they allow for audience participation and cover topics not tackled by the traditional media. Content from citizen journalism and bloggers' websites have even become raw material for private and independent media. Since 2007, Egyptian bloggers have been collecting and disseminating information about arrests of activists, as well as acts of torture by the regime.[34] Some of these bloggers were arrested in connection with their offline protests and defended by other bloggers who used a variety of digital platforms to support them. Others bloggers have become media celebrities—such as Alaa Abdel Fattah, Wael Abbas, and Asmaa Mahfouz—who have been recognized for their work in pushing the limits of freedom of expression in Egypt. Furthermore, groups like Kifaya, 6th of April, and Shayfenkom have emerged through the use of social-networking websites to communicate with their audiences.[35]

Despite the growing diversity of voices online, the SCAF's security forces in 2011 created its own army of online commentators who are paid to join and steer online discussions in favor of the Egyptian regime, echoing state-controlled media. Prominent government writers such as Abdallah Kamal also set up their own Twitter and Facebook accounts to participate in posts and foster pro-government discussions. Nevertheless, reports[36] have revealed that political parties, especially the Freedom and Justice and Al Nour parties, the Egyptian government, and the SCAF have all established an army of micro-bloggers in their struggle to spread information and set the pace and tone of discussion.

Several independent outlets, including Youm7,[37] El Badil, and social media pages such as RASD on Facebook, have accused the authorities of hacking into their sites and deleting certain content, particularly during times of political unrest. Noting the dangers of working in the journalism business, these outlets have also hinted at the mounting pressures they receive from the authorities to manipulate content, coinciding with user complaints of their online posts and comments being deliberately deleted. In response, journalists from Youm7 and Al Masry Al Youm speaking anonymously stated that they have kept audience

[32] Ahmed El Gody, *Journalism in a Network: The Role of ICTs in Egyptian Newsrooms* (Örebro: Örebro University Press, 2012).
[33] Osama Diab, "New Egypt, new media," The Guardian, March 10, 2011, http://www.guardian.co.uk/commentisfree/2011/mar/10/egypt-media-newspapers-mubarak-propaganda.
[34] Ahmeed El Gody, *Journalism in a Network: The Role of ICTs in Egyptian Newsrooms*.
[35] Naayem Saad Zaghloul, *Electronic Mass Communication in Egypt: Reality and Challenges* (Cairo: Egyptian Cabinet, Information and Decision Support Center, February 2010), 38.
[36] See for example: "Twitter Discussions & Trends," Isqat Al-Nizam, last modified March 5, 2012, accessed June 30, 2012, http://wiki.aucegypt.edu/isqatalnizam/index.php/Twitter_Discussion_%26_Trends.
[37] "Hacking Youm7 News Website," Sacrab News, April 17, 2012, http://www.secarab.com/vb/details-3079.html [in Arabic].

complaints on their sites to serve as recognition of and an indirect apology for the forced deletion of some comments.

There are no clear red lines on what issues journalists and citizens should not tackle, though traditional journalists are typically alert when writing about the presidency, the military, and Muslim-Christian relations. By contrast, online activists and bloggers have grown to be critical of these subjects, pushing the limits of freedom both online and offline by forcing the traditional media to tackle sensitive topics.

With the development of Web 2.0 technologies, more bloggers and civic advocates have begun using social-networking websites to expose government fraud and acts of brutality by the security forces. Activists use ICTs to debate current events, criticize the government, public officials and political parties, share personal experiences, propose solutions to current socio-political problems, and construct various visions of the country's future.[38] The country's netizens have quickly harnessed ICTs, using online news sites, blogs, video blogs, YouTube posts, podcasts, Facebook, Twitter, SMS text messages, and mobile phone web publishing to produce and disseminate news and advocacy that outpaces government control. Surveys between 2010 and 2011 counted 13,500 active citizen news journalism websites in Egypt that provided "politically driven reportage on local events… break[ing] numerous off-limits to the mainstream Egyptian media" and clustering citizens around the idea of democratic change through the use of ICTs.[39]

VIOLATIONS OF USER RIGHTS

The Egyptian constitution and penal code state that the media is free within the limits of society. Such an ambiguous statement gives the government the right to limit freedom of expression under the premise of "keeping public order," and there are no explicit rules that allow the government to censor or monitor citizens' behavior. However, according to local advocates, the constitutional rights for protecting freedom have lost their protective force because of an array of restrictive laws, specifically the 1996 Press Law, the 1971 Law on the Protection of the Nation and Citizens, the 1977 Law on Security of National Unity, the Publications Laws and the Parties Laws, and the Emergency Law.[40]

[38] "Blog Shut Down After Promoting Opposition Candidate," IFEX, September 16, 2010, http://www.ifex.org/egypt/2010/09/16/amrosama.eb2a_blocked/.
[39] Lawrence Pintak, "Arab Media and the Al Jazeera Effect," in *Global Communication: Theories, Stakeholders, and Trends* ed. Thomas L. McPhail (New York: Wiley-Blackwell, 2010), 260.
[40] "Media Sustainability Index – Middle East and North Africa," *Media Sustainability Index 2005* (Washington D.C.: IREX, 2006), http://www.irex.org/system/files/MSI05_MENA_EG.pdf.

In May 2010, the Egyptian government renewed the Emergency Law, which had been in place since 1981, until the end of May 2012. In an effort to reduce controversy, the declaration explicitly limited its use to combating terrorism and drug trafficking and did not grant any powers to impose censorship or shut down media outlets. Nevertheless, both the Mubarak regime and SCAF military administration used the Emergency Law[41] to stifle freedom of expression, restrict citizens' rights to access and publish information,[42] and detain thousands of civilians between 2010 and early 2012, including several online activists.[43] Granting broad powers to the president during emergencies to confiscate, suspend or shutdown all means of communication, the Emergency Law also provided legal justification for the Mubarak regime's unprecedented decision to shut down all internet and mobile connections in January 2011.[44] Although former President Mubarak, the prime minister, and the interior minister were fined a total of US$91 million by a court order for cutting internet and mobile services,[45] the three are appealing the fine, arguing that their actions were within the limits of the law.[46]

The government under the SCAF in 2011 continued to repress online freedom of expression and the free flow of information, which started in 2008 when the Mubarak regime began planning to pass an ambiguous law to control the internet.[47] The bill was soon withdrawn from parliament as a result of mounting pressure from the media and civil society. Shortly after, the government filed a legal case to censor 51 websites mostly belonging to the Muslim Brotherhood, which the court denied, highlighting the importance of freedom of expression. However, in 2009 an Egyptian court issued a ruling that banned access to pornographic websites on grounds that such content was offensive to religion and society's values.[48] The rule was never implemented, likely because the state security forces were more interested in restricting political content. Nevertheless, in March 2012 another court

[41] UPDATE: *Freedom on the Net 2012* covers events in 2011 through May 1, 2012; however, it is important to note that the Emergency Law officially expired on May 31, 2012.
[42] "Egypt: Cosmetic Changes Can't Justify Keeping Emergency Law," Human Rights Watch, May 13, 2010, http://www.hrw.org/news/2010/05/12/egypt-cosmetic-changes-can-t-justify-keeping-emergency-law.
[43] "Egypt: Parliament's Chance to End State of Emergency," Human Rights Watch, May 30, 2012, http://www.hrw.org/news/2012/05/30/egypt-parliament-s-chance-end-state-emergency.
[44] Vittorio Coalo, chief executive of the U.K.'s Vodaphone which is the majority owner of Egypt's largest mobile carrier, and Naguib Sawiris, founder of Mobinil, confirmed in two separate interviews that the shutdown was carried out legally. Coalo said Egyptian officials asked mobile operators to shut off networks and stated this request was "legitimate" under Egyptian law and NTRA's terms of use. See also, Connor Moran, "Egypt's Internet Shutdown: Was it Legal?" Law, Technology & Arts Blog, February 1, 2011, http://wjlta.wordpress.com/2011/02/01/egypts-internet-shutdown-was-it-legal/.
[45] "Mubarak fined for cutting internet and phones," Al Jazeera, May 28, 2011, http://www.aljazeera.com/news/africa/2011/05/201152811555458677.html.
[46] "Egypt court demands details of web, phone blackout," Reuters Africa, August 8, 2011, http://af.reuters.com/article/egyptNews/idAFL6E7J80Z920110808.
[47] David Stanford, "Egypt faces new media censorship," Al Jazeera, August 7, 2008, http://www.aljazeera.com/focus/2008/08/200887919526179 74.html.
[48] "Cairo court rules to block porn sites," Agence France-Presse," May 12, 2009, http://www.google.com/hostednews/afp/article/ALeqM5hnniQuhwRV5EUeG0e_3ABfUjWAYQ.

reaffirmed the 2009 decision,[49] leading to a debate in the currently pro-Islamic parliament on implementing the ban. In the meantime, several ISPs have been reportedly issuing customized filtering services.[50]

Violations against users, especially bloggers, continued to grow between 2010 and 2012, with several bloggers and activists threatened, beaten, or harassed. Prior to the January 2011 revolution, a number of bloggers—including Wael Abbas, Israa Abdel Fattah and Asmaa Mahfouz—were detained to keep them from communicating online under claims that their posts endangered social welfare and/or threatened national security. During the first few days of the 2011 revolution, Egyptian security forces detained a number of activists, bloggers, and Facebook group administrators, including Wael Ghoneim, the founder of the "We are All Khaled Said" group that was created to protest Khaled Said's brutal death by the hands of police forces in July 2010.[51]

After the revolution, the SCAF continued the same policies against bloggers and online activists such as Maikel Sanad, a political activist and blogger who had criticized Egypt's six decades of military rule and actively participated in the revolution. He was arrested on February 4, 2011 by military police and tortured before being released 27 hours later. In March 2011, Sanad was arrested again in his home by military police and sentenced to three years' imprisonment on charges of "insulting the military" in his blog post titled, "The Army and the People Were Never One Hand."[52] On December 14, 2011, the Egyptian supreme military court of appeals reduced his sentence to two years, and after mounting local and global pressure, Sanad was pardoned by the military on January 23, 2012.[53]

In another instance, veteran blogger and human right activist Alaa Abd al-Fattah was detained after refusing to be questioned by military prosecutors over allegations of "inciting violence and sabotage" during deadly clashes between the army and protesters in October 2011. Abd al-Fattah said the army had no grounds for interrogating him and demanded to speak to a civilian official, which prompted his detention. He was released a few months later. Between December 2011 and February 2012, the police and military targeted numerous other activists and human rights advocates, detaining them on allegations of receiving donations and training to spread chaos in the country. As of May 2012, 43 activists

[49] Leon Watson, "Court orders Egypt to ban porn websites to protect its 'society and values,'" Daily Mail, March 30, 2012, http://www.dailymail.co.uk/news/article-2122854/Court-orders-Egypt-ban-porn-websites-protect-society-values.html.
[50] Al-Masry Al-Youm, "Blocking internet pornography a priority for telecom minister," Egypt Independent, March 22, 2012, http://www.egyptindependent.com/news/blocking-internet-pornography-priority-telecom-minister.
[51] See, We are all Khaled Said's Facebook page, accessed August 23, 2012, https://www.facebook.com/elshaheeed.co.uk/info.
[52] Max Strasser, "The Army and the People were Never One Hand," Foreign Policy, January 24, 2012, http://www.foreignpolicy.com/articles/2012/01/24/the_army_and_the_people_were_never_one_hand.
[53] Jack Shenker, "Egypt pardons jailed blogger as generals brace for anniversary protests," The Guardian, January 20, 2012, http://www.guardian.co.uk/world/2012/jan/22/egypt-pardons-blogger-anniversary-protests?newsfeed=true.

are undergoing trial on charges of establishing organizations without proper documentation and receiving foreign donations.[54]

After taking over command of the country in early 2011, it soon became clear that the military forces were continuing the same practices under the Mubarak regime of monitoring internet activity.[55] In addition, the authorities have reportedly invested aggressively in surveillance equipment to monitor online communications. For example, the new Homeland Security Agency established in 2011 (replacing the State Security Investigations Service) has reportedly acquired deep-packet inspection equipment in addition to real time intelligence and content filtering equipment that allows the agency to inspect, track, and target content from internet and mobile networks as it passes through routers.[56]

Restrictions on anonymous communication online have also become a growing issue in Egypt. In 2011, the government enforced an article from the 2003 Telecommunication Act (Law #65) that obliges ISPs and mobile operators to allow government access to customer databases.[57] Several reports highlighted instances of members of the national security forces using ISP databases to obtain information about the activities of specific customers.[58] Mobile operators and ISPs are required to collaborate with the Homeland Security Agency and the military police when asked to release information or provide records of subscribers. In addition, internet cafe customers need to provide their names, email addresses, and mobile numbers to receive a personal identification number (PIN) to access the internet. The country's three mobile operators are also required to register their subscribers as well as keep records of their online activities, and an out-going phone call can be traced by a half-dozen government entities.

Extralegal intimidation against activists and bloggers increased in 2011 and early-2012. In one case, blogger Malek Mostafa lost his right eye to a police rubber bullet during a peaceful protest in November 2011 calling on the SCAF to transfer power to a civilian government.[59] Columnist Mona Eltahawy suffered broken wrists after being brutally beaten and sexually

[54] "Egypt Trial on U.S. democracy activists set for February 26," Reuters, February 18, 2012, http://www.reuters.com/article/2012/02/18/us-egypt-us-hearing-idUSTRE81H0BQ20120218.
[55] Jeremy M. Sharp, "Egypt in Transition," Congressional Research Service, February 8, 2012, http://fpc.state.gov/documents/organization/185937.pdf.
[56] "Will Social Networks Deliver Democracy To Africa And Middle East?" Tek-Tips Forums, January 28, 211, http://tek-tips.nethawk.net/will-social-networks-deliver-democracy-to-africa-and-middle-east/.
[57] Christopher Rhoads and Geoffrey A. Fowler, "Egypt Shuts Down Internet, Cellphone Services," *Wall Street Journal*, January 29, 211, http://online.wsj.com/article/SB10001424052748703956604576110453371369740.html; "New Regulations for customers database" [in Arabic], NTRA, press release, accessed July 16, 2012, http://ntra.gov.eg/arabic/News_NewsDetails.asp?PID=39&ID=168.
[58] Mohamad Al-Assad, "Plan to Control Internet Services in Egypt on January 25 and beyond" [in Arabic], *Al Youm 7*, May 31, 2011, http://www.youm7.com/News.asp?NewsID=425202.
[59] "Tahrir Square Under Attack: 32 Egyptians Killed, 1,750 Injured in Protests Against Military Rule," Democracy Now (video), November 21, 2011, http://www.democracynow.org/2011/11/21/tahrir_square_under_attack_32_egyptians.

assaulted by the military while covering the same protests.[60] In February 2012, the prominent activist Salma Said was left with at least 117 birdshot wounds while filming an armored personnel carrier (APC) after the police responded violently to a peaceful protest in Cairo.[61]

During the 2011 parliamentary elections and preliminary presidential campaigns, several Facebook news accounts such as "RASD" (Arabic for "observe") were hacked. The page started as a Facebook alert service to report on fraud and offences during the 2010 parliamentary elections and became a popular news alternative to mainstream media when the revolution broke out in January 2011.[62] Known for its Facebook campaign, "Monitor, capture, and blog," that successfully reported on military and government offences during the parliamentary election, RASD began experiencing systematic attempts, allegedly orchestrated by the military and government, to hack its website. The hacking resulted in the deletion of news items about protests against the government and the subsequent dissemination of pro-government/SCAF messages, which forced the group to change its Facebook account.[63]

[60] Peter Beaumot and Bel Trew, "Journalist Mona Eltahawy tells of sex assault in Cairo ministry," The Guardian, November 24, 2011, http://www.guardian.co.uk/world/2011/nov/24/journalist-mona-eltahawy-sex-assault-cairo.

[61] Salma Shukrallah and Bel Trew, "Egypt's Interior Minister proven a liar: overwhelming evidence police fired birdshot at protesters," Ahram Online, February 7, 2012, http://english.ahram.org.eg/News/33950.aspx.

[62] Wikipedia, "About RASD News," accessed September 10, 2012, http://ar.wikipedia.org/wiki/%D8%B4%D8%A8%D9%83%D8%A9_%D8%B1%D8%B5%D8%AF_%D8%A7%D9%84%D8%A5%D8%AE%D8%A8%D8%A7%D8%B1%D9%8A%D8%A9.

[63] Hassan Hassan, "Penetrating Rasd Server," Alekhteraq.com, June 17, 2012, http://www.alekhteraq.com/2012/06/17/%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D8%B3%D9%8A%D8%B1%D9%81%D8%B1%D8%A7%D8%AA-%D8%B4%D8%A8%D9%83%D8%A9-%D8%B1%D8%B5%D8%AF-%D8%A7%D9%84%D8%A5%D8%AE%D8%A8%D8%A7%D8%B1%D9%8A%D8%A9/#.

ESTONIA

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	2	2
Limits on Content (0-35)	2	3
Violations of User Rights (0-40)	6	5
Total (0-100)	**10**	**10**

* 0=most free, 100=least free

POPULATION: 1.3 million
INTERNET PENETRATION 2011: 77 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Estonia ranks among the most wired and technologically-advanced countries in the world. With a high internet penetration rate and widespread e-commerce and e-government services embedded into the daily lives of individuals and organizations, Estonia has become a model for free internet access as a development engine for society. When the country regained independence in 1991 after nearly 50 years of Soviet rule, its infrastructure was in disastrous condition. The country's new leadership, however, perceived the expansion of information and communication technologies (ICTs) as a key to economic growth and invested heavily in their development.

The first internet connections in the country were introduced in 1992 at academic facilities in Tallinn and Tartu. The government subsequently worked with private and academic entities to initiate in 1996 a program called Tiger Leap, which aimed to computerize and establish internet connections in all Estonian schools by 2000. This program helped to build general competence and awareness of ICTs. Today, with a high level of computer literacy and connectivity already established, the program's focus has shifted from basic concerns such as access, quality, and cost of internet services to discussions about security, anonymity, the protection of private information, and citizens' rights on the internet. Children's safety on the internet is a high priority, and the special program "Targalt Internetis" (Wiser Internet) is dedicated to country-wide training and awareness-building

activities on internet safety issues for parents and children. In addition, a majority of users conduct business and e-government transactions over the internet.[1]

Over the past two years, the issue of copyright protection on the internet has become a widely debated topic in Estonia and various organizations that represent the interests of authors and other copyright holders have come at the forefront of the effort to remove copyright-protected content from popular services such as YouTube. Moreover, the issue of legal liability of online forums for the comments posted by anonymous users continues to be watched by free expression advocates with an important ruling by the European Court of Human Rights expected in late 2012.

OBSTACLES TO ACCESS

The number of internet and mobile telephone users in Estonia has grown rapidly in the past 20 years. According to 2011 statistics from the International Telecommunication Union (ITU), internet penetration in Estonia is 77 percent (approximately 993,000 people).[2] There are also nearly 1.9 million mobile phone subscriptions as of 2011, translating into a mobile phone penetration rate of 139 percent. This outsized figure is commonly attributed to the growing popularity of machine-to-machine (M2M) services, widespread use of mobile internet access devices, use of more than one mobile phone by individual Estonians, and the growing number of visitors who use local subscriptions while in the country.

The first public WiFi area was launched in 2001, and since then the country has developed a system of mobile data networks that enable widespread wireless broadband access. In 2011, the country had over 2,400 free, certified WiFi areas meant for public use, including at cafes, hotels, hospitals, schools, and even gas stations, and the government has continued to invest in public WiFi.[3] In addition, a countrywide wireless internet service based on CDMA technology has been deployed and priced to compete with fixed broadband access. Three mobile operators cover the country with mobile 3G and 3.5G services, and penetration of 4G networks is increasingly attracting subscribers. Municipalities in rural areas have been subsidizing local wireless internet deployment efforts, and the country's regulatory framework presents low barriers to market entry, enabling local start-ups to proliferate.

Estonians use a large variety of internet applications, including search engines (85 percent of

[1] Kristina Randver, "Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega" [Citizens' Satisfaction with the Provision of Public E-Services], TNS Emor, May 11, 2010, available at http://www.riso.ee/et/files/Randver_infohommik_11.05.2010.pdf.
[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[3] Public WiFi Hotspot database in Estonia: http://kaardistajad.wifi.ee/avalik.php.

users), email (83 percent), local online media, news portals, social-networking sites, instant messaging, and internet-based voice services.[4] In addition, 83 percent of the population uses the internet for online banking—the second highest percentage in the European Union (EU).[5] Estonian Public Broadcasting delivers all radio channels and its own TV production services including news in real time over the internet; it also offers archives of its radio and television programs at no charge to users. YouTube, Facebook, LinkedIn and many other international video-sharing and social-networking sites are widely available and popular. Moreover, 21 percent of Estonians use the internet for uploading and sharing original content such as photographs, music, and text—the highest level of shared public communication in Europe.[6]

The Estonian Electronic Communications Act was passed in late 2004 and a number of amendments have further been added to help develop and promote a free market and fair competition in electronic communications services.[7] Today, there are over 200 operators offering such services, including six mobile phone companies and numerous internet service providers (ISPs). ISPs and other communications companies are required to register with the Estonian Technical Surveillance Authority (ETSA), a branch of the Ministry of Economic Affairs and Communications, though there is no registration fee.[8]

In 2009, the Estonian Internet Foundation was established to manage Estonia's top level domain, ".ee."[9] With its multi-stakeholder foundation, the organization represents the Estonian internet community internationally and has succeeded in overseeing various internet governance issues such as the domain name registration process. However, due to concerns over the foundation's domain registration pricing policy[10] and management capabilities,[11] the foundation's substantive work has been paralyzed in 2012, and the Estonian government is currently seeking consultation with other stakeholders to help

[4] Pille Pruulmann-Vengerfeldt, Margit Keller, and Kristina Reinsalu, "1.1.4 Quality of Life and Civic Involvement in Information Society," *Information Society Yearbook 2009* (Tallinn: Ministry of Economic Affairs and Communications, 2010), http://www.riso.ee/en/pub/2009it/#p=1-1-4.

[5] "Estonians tend to avoid e-shopping—survey," Baltic News Service, February 8, 2008, http://www.estemb.org/news/aid-1247.

[6] "Individuals Using the Internet for Uploading Self-Created Content to Any Website to Be Shared," Eurostat, accessed June 10, 2010, http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00119.

[7] "Electronic Communications Act," Ministry of Economic Affairs and Communications, accessed March 26, 2009, http://www.mkm.ee/index.php?id=9576.

[8] Estonian Technical Surveillance Authority (ETSA), "Commencement of Provision of Communications Service," accessed February 21, 2011, http://www.tja.ee/index.php?id=11703.

[9] Estonian Internet Foundation: http://www.internet.ee/eng.

[10] The activities of the Estonian Internet Foundation are not subsidized from the state budget and the fee is established so that it is possible to cover infrastructure investments, operating costs and the reserve from it.

[11] Members of the Management Board resigned early 2012 and new competition to fill Management Board will be held in autumn 2012. "Marek-Andres Kauts resigns as board member," Eesti Internet, March 23, 2012, http://www.internet.ee/eng/news/marek-andres-kauts-resigns-as-board-member/_year/2012.

recover the progress of the foundation, including meetings with the Internet Users Advisory Board.

LIMITS ON CONTENT

Restrictions on internet content and communications in Estonia are among the lightest in the world. Nevertheless, due in part to Estonia's strong privacy laws, there are some instances of content removal. Most of these cases involve civil court orders to remove inappropriate or off-topic reader comments from news sites. Comments are similarly removed from online discussion forums and other sites. Generally, users are informed about a given website's privacy policy and rules for commenting, which they are expected to follow. Most of the popular online services have established policies that outline a code of conduct for the responsible and ethical use of their services and have enforcement policies in place.

In 2008, a debate over self-censorship and pre-publication censorship took center stage when the victim of unflattering and largely anonymous comments on a news story filed suit, claiming that web portals must be held responsible for reader comments and screen them before they become public.[12] Website owners argued that they did not have the capacity to monitor and edit all comments made on their sites. Nonetheless, the Estonian courts ruled in favor of the plaintiff, making web portals responsible for all comments posted. The ruling was appealed to the European Court of Human Rights and is expected to have its decision made by late 2012.

In January 2010, a new law on online gambling came into force, requiring all domestic and foreign gambling sites to obtain a special license or face access restrictions. As of June 2012, the Estonian Tax and Customs Board had placed 636 websites on its list of illegal online gambling sites, requiring Estonian ISPs to block them.[13]

In 2011, the removal of online content related to possible copyright infringement on YouTube increased, facilitated greatly by requests of copyright enforcement organizations representing Estonian authors. Hundreds of videos have been removed from YouTube for copyright violations even though some of the videos were posted by the authors themselves

[12] Kaja Koovit, "Big Businessman Goes to War Against Web Portals," Baltic Business News, March 18, 2008, http://www.balticbusinessnews.com/?PublicationId=48694078-50cc-4fe1-b3e4-6e10bc6a5ec1.

[13] The list of restricted websites can be found on the Estonian Tax and Customs Board website: "Ebaseadusliku kaughasartmängu serverite domeeninimed" [Illegal gaming servers, domain names], Tax and Customs Board, accessed June 10, 2010, http://www.emta.ee/index.php?id=27399.

who were apparently not aware of the activities of copyright enforcement organizations representing their rights.[14]

There are over 70,000 active Estonian-language blogs on the internet, including an increasing number of group, project, and corporate blogs. The vibrancy and activities of the blogosphere are frequently covered by traditional media, particularly when blog discussions center on civic issues. The fact that so many Estonians are both computer literate and connected to the internet has created unique opportunities for the Estonian government. In addition to hosting virtual trade fairs and an online embassy, the Estonian president's office has its own Twitter, Facebook and YouTube channel, and releases messages exclusively on YouTube.[15]

Estonia has the largest functioning public-key infrastructure[16] in Europe, based on the use of electronic certificates maintained on the national identification (ID) card.[17] More than 1.2 million active ID cards are in use, which enable both electronic authentication and digital signing.[18] The Digital Signature Act, adopted in 2000,[19] gives an individual's digital signature the same weight as a handwritten one and requires public authorities to accept digitally-signed documents. Estonian ID cards were used to facilitate electronic voting during the parliamentary elections in 2007 and were used again in the 2009 municipal and European Parliament elections. During the 2011 national parliamentary elections, 140,846 votes were cast over the internet, representing over 20 percent of all votes. In 2011, 94 percent of citizens filed their taxes online, making the web services offered by the tax department the most popular public e-service. Over 63 percent of internet users regularly use e-government services, and 77 percent have indicated their satisfaction with such services.[20]

In early 2012, Estonian daily newspapers and TV raised public awareness on the progress of the Anti-Counterfeiting Trade Agreement (ACTA) and its developments in the European Union. As in many other countries, the Estonian government's initial position on ACTA's

[14] "Autorite ühing laseb YouYube'ist videoed eemaldada," ERR News, February 2, 2011, http://uudised.err.ee/index.php?06223519.

[15] "Estonia Launches Embassy in Virtual World Second Life," Sydney Morning Herald, December 5, 2007, http://www.smh.com.au/news/Technology/Estonia-launches-embassy-in-virtual-world-Second-Life/2007/12/05/1196530704693.html; "Estonian President Launches YouTube Video Blog," TopNews.in, December 9, 2008, http://www.topnews.in/estonian-president-launches-youtube-video-blog-297028.

[16] A *public-key infrastructure (PKI)* is a system for the creation, storage, and distribution of *digital certificates* which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed.

[17] See the web portal for the ID-card system at http://id.ee/?lang=en.

[18] Ibid., accessed July 15, 2010.

[19] "Digitaalallkirja seadus" [Digital Signature Act], Riigi Teataja, accessed August 21, 2012, https://www.riigiteataja.ee/akt/694375.

[20] Kristina Randver, *Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega, Jaanuary 2010* [Citizens' Satisfaction with the Provision of Public E-Services, January 2010] (Tallinn: TNS Emor, 2010), http://www.riso.ee/et/files/kodanike_rahulolu_avalike_eteenustega_2010.pdf.

possible negative implications on user privacy was formal, stating that nothing would change if ACTA was ratified.[21] From February 8-20, 2012, the discussion on ACTA escalated in public media and political debates, which were crucially influenced by the internet user community and experts. On February 11th, demonstrations against ACTA were held in Tallinn and Tartu, gathering more than 2,000 participants.[22] As a result, open debates in the Estonian Parliament rephrased the government's initial support with a more careful approach to be informed by further consultations and analysis. Overall, the ACTA controversy in Estonia demonstrated the increasing awareness of and civic participation in internet freedom issues and intellectual property regulation.

VIOLATIONS OF USER RIGHTS

Freedom of speech and freedom of expression are protected by Estonia's constitution and by the country's obligations as an EU member state. Anonymity is unrestricted, and there have been extensive public discussions on anonymity and the respectful use of the internet. Internet access at public access points can be obtained without prior registration. The Personal Data Protection Act (PDPA), first passed in 1996, restricts the collection and public dissemination of an individual's personal data. No personal information that is considered sensitive—such as political opinions, religious or philosophical beliefs, ethnic or racial origin, sexual behavior, health, or criminal convictions—can be processed without the consent of the individual. The Data Protection Inspectorate (DPI) is the supervisory authority for the PDPA, tasked with "state supervision of the processing of personal data, management of databases and access to public information."[23] The current version of the PDPA came into force in 2008.[24]

The Electronic Communications Act was launched on January 1, 2005, aligning itself with EU legislation and replacing the Telecommunications Act. Since January 2008, electronic communications companies have been required to preserve traffic and location data as defined by the EU Data Retention Directive (2006/24/EC) for one year. Companies have been required to retain data on internet access, telephony, and email since March 2009, and must only retain such data that becomes known to them in the course of providing

[21] "Ministeeriumid lubavad, et ACTA midagi ei muuda" [Ministries promise that ACTA will not change anything], ERR News, January 25, 2012, http://uudised.err.ee/index.php?06244282.
[22] Arni Alandi, "ACTA vastu seisti mitmel pool maailmas" [ACTA is a required standing around the world], ERR News, February 11, 2012, http://uudised.err.ee/index.php?06245704.
[23] Electronic Privacy Information Center (EPIC) and Privacy International, "Republic of Estonia," in *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (Washington: EPIC, 2007), http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-8.html.
[24] See the homepage of the Estonian Data Protection Inspectorate at http://www.aki.ee/eng.

communications services. They must also only provide the surveillance agency or security authority with the information at their disposal when presented with a court order.[25]

There have been no physical attacks against bloggers or online journalists in Estonia, though online discussions are sometimes inflammatory. Following instances of online bullying and sexual harassment and the misuse of social media in 2009-2010, discussions and public awareness campaigns were recently launched to raise parental involvement in increasing the protection of children on the internet.

Awareness of the importance of ICT security in both private and business use has increased significantly since the cyberattacks that occurred in spring 2007. To protect the country from future attacks, the government adopted a five-year Cyber Security Strategy in 2008 that focuses on the development and implementation of new security measures, increasing competence in cyber security, improving the legal framework, bolstering international cooperation, and raising public awareness.[26] Estonia's cyber security strategy is built on strong private-public collaboration[27] and a unique voluntary structure through the National Cyber Defense League.[28] With more than 150 experts participating, the League has simulated different security threat scenarios over the past few years as defense exercises that have served to improve the technical resilience of Estonia's telecommunication networks and other critical infrastructure. Also in 2008, the North Atlantic Treaty Organization (NATO) established a joint cyberdefense center in Estonia to improve cyberdefense interoperability and provide security support for all NATO members. Since its founding, the center has supported awareness campaigns and academic research on the topic and hosted several high-profile conferences, among other activities.[29]

[25] Electronic Communications Act, translation to English, at http://www.legaltext.ee/text/en/X90001K2.htm.
[26] Cyber Security Strategy Committee, *Cyber Security Strategy* (Tallinn: Ministry of Defence, 2008), http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.
[27] See, *Cyber Security Strategy*.
[28] "Küberkaitseliit," Wikipedia, accessed August 21, 2012, http://en.wikipedia.org/wiki/Küberkaitseliit.
[29] "Conference on Cyber Conflict," Cooperative Cyber Defense Centre of Excellence (CCD COE), accessed July 15, 2010, http://www.ccdcoe.org/conference2010/.

ETHIOPIA

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	21	22
Limits on Content (0-35)	26	27
Violations of User Rights (0-40)	22	26
Total (0-100)	**69**	**75**

* 0=most free, 100=least free

POPULATION: 87 million
INTERNET PENETRATION 2011: 1 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Ethiopia is the second most populous country in Africa, but poor infrastructure and a government monopoly over the telecommunications sector have notably hindered the growth of information and communication technologies (ICTs). Consequently, Ethiopia has one of the lowest rates of internet and mobile telephone penetration on the continent. Despite low access, the government maintains a strict system of controls and is the only country in Sub-Saharan Africa to implement nationwide internet filtering.

In 2011, in the wake of the Arab Spring protests in the Middle East and several online calls for similar demonstrations in Ethiopia,[1] the government reacted by strengthening internet censorship and carrying out a systematic crackdown on independent journalists, including at least one blogger. Beginning in June 2011, over ten journalists were sentenced to long prison terms,[2] mostly on questionable charges of terrorism. Among them was the editor of an exiled online news website who was sentenced in abstentia to life imprisonment. A prominent dissident blogger based in Ethiopia was also arrested in September 2011 and sentenced to 18 years in prison in July 2012.[3] The latest crackdown is part of a broader

1 René Lefort, ""Beka!" ("enough")." Will Ethiopia be next?" openDemocracy.net, May 26, 2011, http://www.opendemocracy.net/ren%C3%A9-lefort/beka-enough-will-ethiopia-be-next.
2 Yukio Strachan, "Prisoners of Conscience: Swedish Journalists Jailed in Ethiopia," Digital Journal, December 29, 2011, http://digitaljournal.com/article/316820.
3 William Easterly et al., "The Case of Eskinder Nega," *The New York Review of Books*, January 12, 2012, http://www.nybooks.com/articles/archives/2012/jan/12/case-eskinder-nega/?pagination=false; "Ethiopia sentences Eskinder, 5 others on terror charges," Committee to Protect Journalists, July 13, 2012, http://cpj.org/2012/07/ethiopia-sentences-eskinder-six-others-on-terror-c.php.

trend of growing repression against independent media since the 2005 parliamentary elections, in which opposition parties mustered a relatively strong showing.[4]

Internet and mobile phone services were introduced in Ethiopia in 1997 and 1999, respectively.[5] In recent years, the government has attempted to increase access through the establishment of fiber-optic cables, satellite links, and mobile broadband services. It has refused to end exclusive control over the market by the state-owned Ethiopian Telecommunication Corporation (ETC). However, in December 2010 France Telecom took over management of ETC for a two-year period, renaming it Ethio Telecom in the process.[6] China has also emerged as a key investor and contractor in Ethiopia's telecommunications sector.[7] Given allegations that the Chinese authorities have provided the Ethiopian government with technologies that can be used for political repression, such as surveillance cameras and satellite jamming equipment,[8] some observers fear that the Chinese may assist the authorities in developing more robust internet and mobile phone censorship and surveillance capacities in the coming years.

OBSTACLES TO ACCESS

Ethiopia's telecommunications infrastructure is among the least developed in Africa and is almost entirely absent from rural areas, where about 85 percent of the population resides. In 2011, only 829,000 fixed telephone lines were in actual operation (a decrease from 908,000 lines in 2010[9]), serving a population of 83 million for a penetration rate of less than 1 percent, according to the International Telecommunication Union (ITU).[10] Similarly, as of

[4] Julia Crawford, "Ethiopia: Poison, Politics and the Press," Committee to Protect Journalists, April 28, 2006, http://cpj.org/reports/2006/04/ethiopia-da-spring-06.php.

[5] The first use of internet-like electronic communication was in 1993, when the United Nations Economic Commission for Africa (UNECA) launched the Pan African Documentation and Information Service Network (PADISNET) project, establishing electronic communication nodes in several countries, including Ethiopia. PADISNET provided the first store-and-forward email and electronic-bulletin board services in Ethiopia. It was used by a few hundred people, primarily academics, and staff of international agencies or nongovernmental organizations.

[6] William Davison, "France Telecom Takes Over Management of Ethiopia's Monopoly," Bloomberg, December 3, 2010, http://www.bloomberg.com/news/2010-12-03/france-telecom-starts-two-year-management-contract-at-ethiopia-s-utility.html.

[7] Isaac Idun-Arkhurst and James Laing, *The Impact of the Chinese Presence in Africa* (London: africapractice, 2007), http://www.davidandassociates.co.uk/davidandblog/newwork/China_in_Africa_5.pdf.

[8] Hilina Alemu, "INSA Installing Street Surveillance Cameras," *Addis Fortune*, March 21, 2010, http://www.addisfortune.com/Vol%2010%20No%20516%20Archive/INSA%20Installing%20Street%20Surrviellance%20Cameras.htm; "China Involved in ESAT Jamming," *Addis Neger*, June 22, 2010, http://addisnegeronline.com/2010/06/china-involved-in-esat-jamming/.

[9] International Telecommunication Union (ITU),"Fixed-telephone subscriptions," 2010, accessed July 18, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[10] International Telecommunication Union (ITU),"Fixed-telephone subscriptions," 2011, accessed July 18, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

the end of 2011, internet penetration stood at 1.1 percent, up from 0.75 percent in 2010.[11] Mobile phone penetration in 2011 was higher at roughly 17 percent with a little over 14 million subscriptions, up from an 8 percent penetration rate in 2010.[12] While all of the above reflect very slight improvements in access compared to 2010 (except for fixed-telephone lines), such penetration rates represent extremely limited access to ICTs by global comparison.

The combined cost of purchasing a computer, initiating an internet connection, and paying usage charges places internet access beyond the reach of most Ethiopians. A 2010 study by the ITU found that Ethiopia's broadband internet connections were among the most expensive in the world when compared with monthly income, second only to the Central African Republic,[13] and merely 27,000 broadband subscriptions were recorded in 2011.[14] Prices are set by Ethio Telecom and kept artificially high. In April 2011, Ethio Telecom announced a new set of pricing packages,[15] reducing the subscription charge from US$80 to US$13 and the monthly fee from over US$200 per for unlimited usage to fees of between US$17 and US$41 for between 1 GB and 4 GB of use. By comparison, the annual gross national income (GNI) per capita at purchasing power parity was US$1,110 (or US$92.50 per month) in 2011.[16] Although the new tariffs have rendered the service slightly more affordable—though still relatively expensive—for individual users, cybercafe owners have complained that the lack of an unlimited usage option could hurt the financial viability of their business.[17] Furthermore, an adult literacy rate of 30 percent means that the majority of Ethiopians would be unable to take full advantage of online resources even if they had access to the technology.[18] Radio remains the principal mass medium through which most Ethiopians obtain information.

The majority of internet users rely on cybercafes to access the web, though connections there are often slow and unreliable. Internet access via mobile phones has grown over the

[11] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[12] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[13] Jonathan Fildes, "UN Reveals Global Disparity in Broadband Access," BBC News, September 2, 2010, http://www.bbc.co.uk/news/technology-11162656.

[14] Ibid.

[15] "Residential Tariff," Ethio Telecom, accessed July 16, 2012, http://www.ethiotelecom.et/products/residential-tariff.php.

[16] World Bank, "Gross national income per capital 2011, Atlas method and PPP," World Bank Databank, 2011, accessed July 18, 2012, http://databank.worldbank.org/databank/download/GNIPC.pdf.

[17] Elias Gebreselassie, "Ethio-Telecom Limits EVDO Internet Access<" Addis Fortine, April 3, 2011, http://addisfortune.com/Vol_10_No_570_Archive/Ethio-Telecom%20Limits%20EVDO%20Internet%20Access.htm; "Ethio-Telecom unveils wide-ranging tariff changes across all services," TeleGeography, April 5, 2011, http://www.telegeography.com/products/commsupdate/articles/2011/04/05/Ethio Telecom-unveils-wide-ranging-tariff-changes-across-all-services.

[18] UNICEF, "Ethiopia: Statistics," accessed July 16, 2012, http://www.unicef.org/infobycountry/ethiopia_statistics.html#67.

past year, particularly in semi-urban areas, but slow speeds are a constant problem. A 2010 study commissioned by Manchester University's School of Education found that accessing an online email account and opening one message took six minutes in a typical Addis Ababa cybercafe with a broadband connection.[19] The number of cybercafes has grown in recent years and continues to expand in large cities, after a brief period in 2001–02 during which the government declared them illegal and forced some to shut down. Since July 2002, the Ethiopian Telecommunications Agency (ETA) has been authorized to issue licenses for new cybercafes.

The authorities have placed some restrictions on advanced internet applications. In particular, the use or provision of Voice over Internet Protocol (VoIP) services or internet-based fax services—including at cybercafes—is prohibited,[20] with potential punishments including fines and up to five years in prison.[21] The government instituted the ban on VoIP in 2002 after it gained popularity as a less expensive means of communicating and began to drain revenue from the traditional telephone business belonging to the state-owned Ethiopian Telecommunication Corporation (ETC), or Ethio Telecom.[22] Despite the restriction on paper, many cybercafes offer the service with few repercussions.

Social-networking sites such as Facebook, the video-sharing site YouTube, and the Twitter microblogging service are available, though very slow internet speeds make it impossible to access video content. International blog-hosting websites such as Blogger have been frequently blocked since the disputed parliamentary elections of 2005, during which the opposition used online communication to organize and disseminate information that was critical of the ruling Ethiopian People's Revolutionary Democratic Front (EPRDF).[23] In addition, for two years following the 2005 elections, the ETC blocked text-messaging via mobile phones after the ruling party accused the opposition of using the technology to

[19] Andinet Teshome, *Internet Access in the Capital of Africa* (School of Education, University of Manchester, 2009); EthioTube video, 8:56, posted by "Kebena," accessed August 06, 2010, http://www.ethiotube.net/video/9655/Internet-Access-in-the-Capital-of-Africa-Addis-Ababa.

[20] Ethiopian Telecommunication Agency (ETA), "Telecommunication Proclamation No. 281/2002, Article 2(11) and 2(12)," July 2, 2002, accessed July 25, 2012, http://www.eta.gov.et/Scan/Telecom%20Proc%20281_2002%20(amendment)%20NG.pdf. As an amendment to article 24 of the Proclamation, the Sub-Article (3) specifically states, "The use or provision of voice communication or fax services through the internet are prohibited" (page 1782).

[21] ETA, "Telecommunication Proclamation No. 49/1996, Articles 24 and 25," November 28, 1996, accessed July 25, 2012, http://www.eta.gov.et/Scan/Telecom%20Proc%2049_1996%20NG1.pdf.

[22] Groum Abate, "Internet Cafes Start Registering Users," *Capital*, December 25, 2006, http://www.capitalethiopia.com/index.php?option=com_content&view=article&id=259:internet-cafes-start-registering-users-&catid=12:local-news&Itemid=4.

[23] Bogdan Popa, "Google Blocked in Ethiopia," Softpedia, May 3, 2007, http://news.softpedia.com/news/Google-Blocked-In-Ethiopia-53799.shtml.

organize antigovernment protests. Text-messaging services did not resume until September 2007.[24]

Around May 26, 2011, on the eve of a planned opposition demonstration inspired by anti-government protests in the Middle East and celebrations for the anniversary of the ruling party coming to power, the internet was cut off for at least half a day.[25] It remained unclear whether the cause of the shutdown was a deliberate government attempt to restrict communication at a sensitive time, a technical problem, or sabotage of a fiber-optic cable. Separately, when high-profile international events, such as a meeting of the African Union, have taken place in Addis Ababa and other major cities, the government has redirected much of the country's bandwidth to the venues hosting visitors, leaving ordinary users with even slower connections than usual.

Ethiopia is connected to the international internet via satellite, a fiber-optic cable that passes through Sudan and connects to its international gateway, and another cable that connects through Djibouti to an international undersea cable.[26] In an effort to expand connectivity, the government has reportedly installed several thousand kilometers of fiber-optic cable throughout the country in recent years.[27] There are also plans in place to connect Ethiopia to a global undersea cable network through the East African Submarine Cable System (EASSy) project. The EASSy project itself was completed and launched in July 2010, but its effects on Ethiopia have yet to be seen.[28] The government has sought to increase access via satellite links for government offices and schools in rural areas. WoredaNet, for instance, connects over 500 *woredas*, or local districts, to regional and central government offices, providing services such as video conferencing and internet access. Similarly, SchoolNet connects over 500 high schools across the country to a gateway that provides video- and audio-streamed educational programming.[29] The impact of such projects has been limited, however, as internet speeds across these networks remain almost prohibitively slow and outages are common.

The ETC, or Ethio Telecom, retains a monopoly on all telecommunications services, including internet access and both mobile and fixed-line telephony. Connection to the

[24] Human Rights Watch, "Ethiopia: Repression Rising Ahead of May Elections," news release, March 24, 2010, http://www.hrw.org/en/news/2010/03/24/ethiopia-repression-rising-ahead-may-elections.
[25] "Internet is down through out Ethiopia – update," Ethiopian Review, May 26, 2011, http://www.ethiopianreview.com/content/33165.
[26] Hailu Teklehaimanot, "Unraveling ZTE's Network," *Addis Fortune*, August 22, 2010, http://www.addisfortune.com/Interview-Unraveling%20ZTEs%20Network.htm.
[27] Samuel Kinde, "Internet in Ethiopia: Is Ethiopia Off-Line or Wired to the Rim?" MediaETHIOPIA, November 2007, http://www.mediaethiopia.com/Engineering/Internet_in_Ethiopia_November2007.htm.
[28] Brian Adero, "WIOCC-EASSy Cable Ready for Business," *IT News Africa*, July 23, 2010, http://www.itnewsafrica.com/?p=8419.
[29] Kinde, "Internet in Ethiopia."

international internet is centralized via Ethio Telecom, from which cybercafes must purchase their bandwidth. The Ethiopian Telecommunications Agency (ETA) is the primary regulatory body overseeing the telecommunications sector.[30] Although it was established as an autonomous federal agency, in practice the ETA is tightly controlled by the government.

The space for independent initiatives, entrepreneurial or otherwise, is extremely limited.[31] In October 2011, the government announced[32] that earlier in the year, it had begun granting permission to private companies that run internet-dependent operations to acquire and use VSAT links, connections previously restricted only to governmental and international organizations per special authorization.[33] Under the new directive, which has yet to be made public as of May 2012, companies are reportedly permitted to use the technology for their own operations but are barred from providing services to third parties, thereby maintaining Ethio Telecom's monopoly on public internet access.

Liberalization of the telecommunications sector is expected to greatly increase internet and mobile phone penetration, but the prospects for such loosening remain uncertain. Despite repeated international pressure to do so, the Ethiopian government has been reluctant to ease its grip on the sector.[34] While some observers consider the December 2010 entry of France Telecom as manager of Ethio Telecom to be a potential move toward liberalization, others are skeptical of the government's commitment to allowing greater public access to information and communication technologies (ICTs). The foreign partnership may simply be an effort to improve service delivery while maintaining the state monopoly. Even so, under the new management, users continue to complain that speeds delivered are lower than advertised, service is regularly interrupted, and the quality of customer assistance has declined, possibly due to loss of morale following layoffs.[35]

[30] ETA, "Telecommunication Proclamation No. 49/1996, Part Two," November 28, 1996, accessed August 24, 2010http://www.eta.gov.et/Scan/Telecom%20Proc%2049_1996%20NG1.pdf.
[31] Al Shiferaw, "Connecting Telecentres: An Ethiopian Perspective," *Telecentre Magazine*, September 2008, http://www.telecentremagazine.net/articles/article-details.asp?Title=Connecting-Telecentres:-An-Ethiopian-Perspective&articleid=163&typ=Features.
[32] "Private VSAT Permit Directive Number 2/2003" as noted in: "Ethiopia to liberalise VSAT market," Screen Africa, November 16, 2011, http://www.screenafrica.com/page/news/industry/1097820-Ethiopia-to-liberalise-VSAT-market.
[33] Yelibenwork Ayele, "Companies in Ethiopia Permitted to Use VSAT," 2Merkato.com, October 3, 2011, http://www.2merkato.com/20111003380/companies-in-ethiopia-permitted-to-use-vsat.
[34] "US urge Ethiopia to liberalise telecom sector," Voices of Africa, March 10, 2010, http://voicesofafrica.africanews.com/site/list_message/26217; Technology Strategies International, "ICT Investment Opportunities in Ethiopia—2010," March 1, 2010, http://www.marketresearch.com/Technology-Strategies-International-v3460/ICT-Investment-Opportunities-Ethiopia-2663628/.
[35] Meron Tekleberhan, "Internet Connection a Persistent Problem in Ethiopia," Ezega.com, December 26, 2011, http://www.ezega.com/news/NewsDetails.aspx?Page=heads&NewsID=3169.

LIMITS ON CONTENT

Ethiopian authorities persistently deny engaging in online censorship,[36] but the results of the most recent independent tests conducted by the OpenNet Initiative (ONI) in 2009 and checked again by Freedom House at the end of 2011, indicate otherwise. Both sets of tests indicated that the Ethiopian government imposes nationwide, politically motivated internet filtering.[37] The blocking of websites is somewhat sporadic, tending to tighten ahead of sensitive political events. This on again, off again dynamic continued in 2011, though there were also indications that the technical sophistication of the government's blocking had increased and that periods of openness were shrinking.

The government's approach to internet filtering has generally entailed hindering access to a list of specific internet protocol (IP) addresses or domain names at the level of the international gateway. One blogger reported in January 2011, however, that since mid-2010, the government had been introducing more sophisticated equipment capable of blocking a webpage based on a keyword in the URL path. The observable evidence he cited included the blocking of the individual Facebook page of the exiled news outlet *Addis Neger*, as well as the fact that blocked content could no longer be accessed via Google cache as was previously possible.[38] In July 2011, Ethio Telecom released a tender calling for bids to develop deep-packet inspection (DPI) to be implemented by mid-2012,[39] which would make the existing censorship apparatus more sophisticated.

Testing by ONI found that the filtering focuses primarily on independent online news media, political blogs, and Ethiopian human rights groups' websites.[40] International news outlets such as the U.S.-based Cable News Network (CNN) and nongovernmental organizations such as Human Rights Watch, Amnesty International, and Reporters Without Borders—all of which have criticized the Ethiopian government's human rights record—were available as of early 2009. However, tests conducted by Freedom House found that in 2010 and 2011, the websites of Freedom House, Human Rights Watch, and Amnesty International were inaccessible.

[36] "Ethiopia: Authorities Urged to Unblock Websites," Integrated Regional Information Networks (IRIN), May 25, 2006, http://www.irinnews.org/report.aspx?reportid=59115.
[37] OpenNet Initiative, "Regional Overview: Sub-Saharan Africa," accessed May 28, 2010, http://opennet.net/research/regions/ssafrica.
[38] Daniel Berhane, "Ethiopia's web filtering: Advanced technology, hypocritical criticisms, bleeding constitution," Danielberhane's Blog, January 16, 2011, http://danielberhane.wordpress.com/2011/01/16/ethiopias-web-filtering-advanced-technology-hypocritical-criticisms-bleeding-constitution/.
[39] Azi Ronen, "Ethio Telecom Issued a Tender for DPI," Broadband Traffic Management (blog), July 7, 2011, http://broabandtrafficmanagement.blogspot.com/2011/07/ethio-telecom-issued-tender-for-dpi.html.
[40] OpenNet Initiative, "Regional Overview: Sub-Saharan Africa," http://opennet.net/research/regions/ssafrica.

Ethiopian websites and blogs that are typically blocked but that suddenly became available in early 2009 included CyberEthiopia, Ethiopian Review, Ethiopian Media Forum, Quatero, and Ethiomedia. Several observers suggested that the loosening came in response to the 2008 U.S. State Department human rights report on Ethiopia released in February 2009,[41] which accused the government of restricting internet access by blocking politically oriented websites.[42] CyberEthiopia, a prodemocracy website, commented in March 2009 that the erratic nature of internet filtering may be a deliberate tactic by the authorities to create confusion and buttress government claims that there is no systematic or pervasive filtering in the country.

By mid-2010, all newly available websites and several others—including the online version of *Addis Neger*, a leading independent newspaper that was forced to close in December 2009[43]—were temporarily inaccessible again, apparently as part of the government's broader election-related restrictions on the free flow of information.[44] These websites were blocked for much of 2011, but were briefly unblocked in May 2011, coinciding with a UNESCO event for International Press Freedom Day and the release of a report by the Committee to Protect Journalists criticizing internet censorship in Ethiopia; the timing again reflected the government's possible efforts to loosen online censorship when under international scrutiny, only to impose it again when the spotlight is removed.[45] By late May, many of the above websites, and some new ones, were blocked again after activists created a Facebook page titled "Beka!" (Enough!)[46] calling for anti-government protests inspired by the Arab Spring uprisings to take place on May 28, 2011.[47] As of early 2012, the above-mentioned websites, as well as those of Ethsat (an independent exile television station) and Dilethiopia (an opposition website) were inaccessible. Further, an independent test conducted by Freedom House in early 2012 found that 65 websites related to news and views, 14 websites belonging to different Ethiopian political parties, 37 blogs, 7 audio-video websites, and 37 Facebook pages were not accessible in Ethiopia.

[41] Bureau of Democracy, Human Rights, and Labor, "Ethiopia," in *2008 Country Reports on Human Rights Practices* (Washington, DC: U.S. Department of State, February 2009), http://www.state.gov/g/drl/rls/hrrpt/2008/af/119001.htm.
[42] Mohamed Keita, "Ethiopia Lifts Filtering of Critical Web Sites—At Least for Now," Committee to Protect Journalists (blog), March 4, 2009, http://cpj.org/blog/2009/03/ethiopia-lifts-filtering-of-critical-web-sites--at.php.
[43] Reporters Without Borders, "Weekly Forced to Stop Publishing, Its Journalists Flee Abroad," news release, December 4, 2009, http://en.rsf.org/ethiopia-weekly-forced-to-stop-publishing-04-12-2009,35258.html.
[44] Oromsis Adula, "Election 2010, Blogging, Medrek, and the Future of Ethiopia," Gadaa.com, May 25, 2010, http://gadaa.com/oduu/3799/2010/05/25/the-2010-election-blogging-medrek-and-the-future-of-ethiopia/.
[45] Haleta Yirga and Merga Yonas, "Ethiopia: Freedom of expression being suppressed," The Reporter Ethiopia, May 7, 2011, http://www.thereporterethiopia.com/Politics-and-Law/ethiopia-freedom-of-expression-being-suppressed.html; Jillioan C. York, "Africa's cascade of Internet censorship," AlJazeera, May 12, 2011, http://www.aljazeera.com/indepth/opinion/2011/05/2011512134039497302.html.
[46] René Lefort, ""Beka!" ("enough")." Will Ethiopia be next?"
[47] David Smith, "Ethiopia's 'day of rage' hopes to oust Meles Zenawi from power," The Guardian, May 27, 2011, http://www.guardian.co.uk/world/2011/may/27/ethiopia-day-of-rage-protest.

In addition to website blocking, some restrictions are also placed on mobile phone text-messaging. In particular, mobile phone users, businesses, and civil society groups are unable to send a message to more than ten recipients without prior approval of its content from Ethio Telecom.[48]

Procedures for determining which websites should be blocked and when are extremely opaque. There is no published list of blocked websites or publicly available criteria for how such decisions are made, and users are met with an error message when trying to access a blocked website. This lack of transparency is exacerbated by the government's continued denial of its censorship efforts. The decision-making process does not appear to be centrally controlled. Thus, various governmental entities, along with the Information Network Security Agency (INSA) and Ethio Telecom, seem to be implementing their own lists, contributing to the phenomenon of inconsistent blocking.

The increased repression in 2011 against journalists working in traditional media as well as against a number of bloggers has generated a chilling effect in the online sphere. Few Ethiopian journalists work for both domestic print media and as correspondents for overseas online outlets, as this could draw negative repercussions. Many bloggers publish anonymously to avoid reprisals.

In addition to censorship, the authorities use regime apologists, paid commentators, and pro-government websites to proactively manipulate the online news and information landscape. Acrimonious exchanges between a small number of apologist websites and a wide array of diaspora critics and opposition forces have become common in online political debates. Lack of adequate funding represents another challenge for independent online media, as fear of government pressure dissuades Ethiopian businesses from advertising with politically critical websites.

Regime critics and opposition forces in the diaspora increasingly use the internet as a platform for political debate and an indirect avenue for providing information to local newspapers. However, given the low internet penetration rate, the domestic Ethiopian blogosphere is still in its infancy. Blogging initially blossomed during the period surrounding the 2005 parliamentary elections and the subsequent clampdown on independent newspapers. This growth has slowed somewhat since 2007, when the government instituted a blanket block on the domain names of two popular blog-hosting websites, Blogger and Nazret.com. Some political commentators use proxy servers and anonymizing tools to hide their identities when publishing online and to circumvent filtering. Among general internet

[48] Based on an interview with individuals working in the telecom sector who requested to remain anonymous, as well as a test conducted by a Freedom House consultant who found it was not possible for an ordinary user to send out a bulk text message.

users, however, circumvention tools are rarely employed, and most people simply forego accessing websites that are blocked.[49]

Over the past two years, the use of social-networking sites, most notably Facebook, as platforms for political deliberation, social justice campaigns, and information sharing has gained momentum. For example, in March 2012 some activists used social media to launch campaigns on behalf of Ethiopian female domestic workers working in the Middle East who were being abused.[50] Nevertheless, many civil society groups based in the country are wary of mobilizing against the government. In February 2011, opposition activists launched the Facebook group "Beka!" (Enough!) calling for a "day of rage" and anti-government protests to be held on May 28. The intention was to have a counter demonstration the same day as a government-sponsored rally celebrating the anniversary of Prime Minister Meles Zenawi's rule. No protest materialized, however.[51] This appeared to be because the calls for protest were mostly coming from the Ethiopian diaspora rather than from within the country, as those inside Ethiopia still harbored fear from the bloody crackdown on opposition demonstrations after the 2005 elections and from the most recent round of opposition activist arrests in April 2011 (see "Violations of User Rights").[52]

VIOLATIONS OF USER RIGHTS

Over the course of 2011 and through mid-2012, the Ethiopian government's already poor treatment of journalists and internet users deteriorated dramatically. A systematic crackdown and series of prosecutions, including over eight Ethiopian journalists and two Swedish reporters, caused many journalists to flee into exile, stripping the country of its last remaining independent voices.[53] In 2011, such repression spread for the first time against bloggers and internet users, with several arrests and at least one prosecution reported.

[49] Interview with an Ethiopian blogger and political commentator, August 8, 2010.

[50] Endalk, "Ethiopia: Netizens Take Campaign for Shweya Mullah Online," Global Voices, October 13, 2011, http://globalvoicesonline.org/2011/10/13/ethiopia-netizens-take-campaign-for-shweyga-mullah-online/; Endalk, "Ethiopia: Outrage Over Abuse of Ethiopian Domestic Worker in Lebanon," Global Voices, March 12, 2012, http://globalvoicesonline.org/2012/03/12/ethiopia-outrage-over-abuse-of-ethiopian-domestic-worker-in-lebanon/.

[51] "What happens on facebook remains on facebook: The "Beka" revolution evangelists on facebook revisited," Endalks' Blog, June 24, 2011, http://endalk.wordpress.com/2011/06/24/what-happens-on-facebook-remains-on-facebook-the-%E2%80%9Cbeka%E2%80%9D-revolution-evangelists-on-facebook-revisited.

[52] Jawar Mohammed, "Nonviolent Struggle: Ethiopian Exceptionalism?" Democracy: Liberty, Security, & Prosperity (blog), February 27, 2011, http://dhummuugaa.wordpress.com/2011/02/27/nonviolent-struggle-ethiopian-exceptionalism-2/; David Smith, "Ethiopia 'day of rage' hopes to oust Meles Zenawi from power"; Eskinder Nega, "Understanding the absence of Ethiopia's 'day of rage,'" Gasha for Ethiopians, June 3, 2011, http://www.ethiopiangasha.org/tmp/EskinderNega3June2011.html; David Shinn, "Revolutionary Winds from North to South of the Sahara: Wishful Thinking?" East Africa Forum, June 13, 2011, http://www.eastafricaforum.net/2011/06/13/prof-david-shinn-revolutionary-winds-from-north-to-south-of-the-sahara-wishful-thinking/.

[53] "Ethiopia: Crackdown 'A Threat to Democracy,'" AllAfrica.com, December 1, 2011, http://allafrica.com/stories/201112020788.html.

Constitutional provisions guarantee freedom of expression and media freedom.[54] Nevertheless, in recent years the government has adopted laws—namely the Mass Media and Freedom of Information Proclamation and the Anti-Terrorism Proclamation—that restrict free expression.[55] According to Human Rights Watch, the 2008 Mass Media and Freedom of Information Proclamation has some positive aspects, such as a ban on the pretrial detention of journalists. However, it also introduced crippling fines, licensing restrictions for establishing a media outlet, a clause permitting only Ethiopian nationals to establish mass media outlets, and powers allowing the government to impound periodical publications.[56] A criminal code that came into force in May 2005 provides for "special criminal liability of the author, originator or publisher" when writings are deemed to be linked to offenses such as treason, espionage, or incitement; in such instances, the penalty may be life imprisonment or death.[57] Also under the criminal code, publication of a "false rumor" is punishable by up to three years in prison.[58]

In 2009, the government enacted the Anti-Terrorism Proclamation, which includes an overly broad definition of terrorism that gives the authorities wide discretion when suppressing nonviolent dissent. Under the legislation, publication of a statement that is likely to be understood as a direct or indirect encouragement of terrorism is punishable by up to 20 years in prison.[59] In 2011, the authorities made extensive use of this law to prosecute a number of individuals who had criticized the government both online and offline, or who had reported on the activities of Ginbot 7, a banned opposition political party that the government has declared a terrorist group. The crackdown generated a notable chilling effect and international condemnation. In September 2011, the well-known dissident blogger Eskinder Nega[60] was arrested on terrorism charges shortly after publishing an online column calling for greater political freedom and criticizing the use of the Anti-Terrorism Proclamation to silence political dissent.[61] Nega was put on trial in March 2012,

[54] "Constitution of the Federal Democratic Republic of Ethiopia, Article 29," Parliament of the Federal Democratic Republic of Ethiopia, accessed August 24, 2010, http://www.ethiopar.net/.

[55] Human Rights Watch, *Analysis of Ethiopia's Draft Anti-Terrorism Law* (New York: Human Rights Watch, 2009), http://www.hrw.org/en/news/2009/06/30/analysis-ethiopia-s-draft-anti-terrorism-law.

[56] "Freedom of the Mass Media and Access to Information Proclamation No. 590/2008," *Federal Negarit Gazeta* No. 64, December 4, 2008.

[57] International Labour Organization, "The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation No. 414/2004, Article 44," accessed August 24, 2010, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/70993/75092/F1429731028/ETH70993.pdf.

[58] International Labour Organization, "The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation No. 414/2004, Articles 485 and 486," accessed August 24, 2010, http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/70993/75092/F1429731028/ETH70993.pdf.

[59] "Anti-Terrorism Proclamation No. 652/2009," *Federal Negarit Gazeta* No. 57, August 28, 2009.

[60] Nega is also the 2011 recipient of the PEN/Barbara Goldsmith Freedom to Write Award. Sarah Hoffman, "That Bravest and Most Admirable of Writers: PEN Salutes Eskinder Nega," PEN American Center (blog), April 13, 2012, http://www.pen.org/blog/?p=11198.

[61] Endalk, "Ethiopia: Freedom of Expression in Jeopardy," Global Voices, February 3, 2012, http://advocacy.globalvoicesonline.org/2012/02/03/ethiopia-freedom-of-expression-in-jeopardy/.

found guilty of terrorism in July, and sentenced to 18 years in prison.[62] In January 2012, Elias Kifle, editor of the U.S. based Ethiopian Review website known for its fierce criticism of Prime Minister Zenawi, was sentenced in abstentia to life imprisonment.[63] In a lower-profile case, two youth were arrested on charges of terrorism in August 2011 while using the internet in an Addis Ababa cybercafe, likely to visit opposition websites; according to unconfirmed reports, they were later released.[64]

Government surveillance of online and mobile phone communications is a concern in Ethiopia, though there is a lack of concrete evidence as to the scale of such practices. In a series of trials of journalists and bloggers throughout 2011 and early 2012, government prosecutors have presented intercepted emails and phone calls between the journalists as evidence.[65] Upon purchasing a mobile phone, individuals are asked to register their SIM card with their full name, address, and government-issued identification number. Internet subscription account holders also are required to register their personal details, including their home addresses, with the government.

For a period following the 2005 elections, cybercafe owners were required to keep a register of their clients, but this requirement has not been implemented since mid-2010. Nevertheless, there are strong suspicions that cybercafes are required to install software to monitor user activity, which arose after a few incidents were reported of users getting arrested while leaving internet cafes in 2011. The arrests were followed by government warnings that "visiting anti-peace websites using proxy serves is a crime."[66] The use of such monitoring software remains unconfirmed.

The key government body involved in surveillance is the Information Network Security Agency (INSA),[67] which is suspected of engaging in internet filtering and email monitoring.[68] There have also been reports of the government using technology obtained from the Chinese authorities to monitor phone lines and various types of online

[62] Markos Lemma, "Ethiopia: Online Reactions to Prison Sentence for Dissident Blogger," Global Voices, July 15, 2012, http://globalvoicesonline.org/2012/07/15/ethiopia-online-reactions-to-prison-sentence-for-dissident-blogger/.
[63] "Ethiopia Sentences 3 Journalists to Long Prison Terms," Voice of America News, January 26, 2012, http://www.voanews.com/english/news/africa/Ethiopia-Sentences-3-Journalists-to-Long-Prison-Terms-138214754.html.
[64] "Ethiopia: Crackdown in Addis Ababa Internet Cafes, Two arrested on Tuesday," *Addis Neger*, August 12, 2011, http://addisnegeronline.com/2011/08/crackdown-in-addis-ababa-internet-cafes-two-arrested-on-tuesday/.
[65] "Ethiopian blogger, journalists convicted of terrorism," Committee to Protect Journalists, January 19, 2012, http://cpj.org/2012/01/three-journalists-convicted-on-terrorism-charges-i.php.
[66] "TPLF regime Arresting Internet Café Users in Addis Ababa," Ethiopian Review, August 12, 2011, http://www.ethiopianreview.com/forum/viewtopic.php?f=2&t=30136.
[67] "Mission Statement," Information Network Security Agency of Ethiopia, accessed June 2, 2010, http://www.insa.gov.et/INSA/faces/welcomeJSF.jsp.
[68] Chris Forrester, "…While Ethiopia Starts Jamming," Rapid TV News, June 23, 2010, http://www.rapidtvnews.com/index.php/201006236926/while-ethiopia-starts-jamming.html.

communication.[69] According to internal sources working in the industry, INSA is currently testing tools that will enable its officials to mask their identities to acquire user information such as usernames and passwords, which could lead to full-fledged phishing attacks against government opponents in the future.[70] To date, cyberattacks and other forms of technical violence have not been a serious problem in Ethiopia, partly due to the limited number of users.

While it has been common for traditional media journalists in Ethiopia to face considerable harassment and intimidation, leading several to flee the country, prior to 2011 such threats did not affect online activists and bloggers. With the 2011 crackdown against online journalists such as Eskinder Nega, however, dissident bloggers and netizens are beginning to experience increasing levels of intimidation for their work.

[69] Helen Epstein, "Cruel Ethiopia," *New York Review of Books*, May 13, 2010, http://www.nybooks.com/articles/archives/2010/may/13/cruel-ethiopia/.

[70] Interview with individuals working in the technology and security sector in Ethiopia, who requested to remain anonymous, January 2012.

GEORGIA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Free**
Obstacles to Access (0-25)	12	9
Limits on Content (0-35)	10	10
Violations of User Rights (0-40)	13	11
Total (0-100)	**35**	**30**

* 0=most free, 100=least free

POPULATION: 4.5 million
INTERNET PENETRATION 2011: 37 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Internet access and use continues to grow rapidly in Georgia, particularly as interest in connecting with friends through social-networking sites has increased in recent years. State bodies and several key politicians have also increased their use of the internet and modern social media tools to share information with citizens and attract attention from the potential electorate.[1] The Ministry of Economy and Sustainable Development continues its cooperation with bloggers, encouraging blogger's projects and engaging in discussions about information technology (IT) development trends. While government restrictions on internet access and content are rare, there was one case of blocking in 2011 involving the distribution of the Hollywood film "5 Days of War" on torrent and peer-to-peer (P2P) file-sharing websites.

The internet was first introduced in Georgia at the end of 1990s, and after a boom in new services such as broadband at the beginning of 2004, connections became available for almost everyone with a telephone line in Tbilisi, the capital. Internet subscriptions have also proliferated in other large cities. Online news media are still developing slowly, while a growing number of journals and newspapers are launching websites, and major newspapers and news agencies are sharing content through applications such as Facebook, Twitter, and YouTube. Meanwhile, many journalists working in the traditional media sphere are looking forward to advancing their knowledge about internet technology and web tools.

[1] The website of the President of Georgia features links to all of the named social media sites: http://president.gov.ge/.

OBSTACLES TO ACCESS

The number of internet and mobile telephone users in Georgia is growing, but high prices for services and inadequate infrastructure remain obstacles to access, particularly for those in rural areas or with low incomes. In 2011, 36.6 percent of the population had access to the internet according to the International Telecommunication Union (ITU), up from 7.5 percent in 2006,[2] while a survey by the Caucasus Research Resource Centers (CRRC) found that 4 percent of Georgians are unfamiliar with the internet altogether.[3] The same survey found that 20 percent of the Georgian population surfs the internet during their free time,[4] 5 percent uses the internet as a main source of information,[5] and 14 percent uses it as a second source.[6] Additionally, 23 percent of Georgians access the internet every day, while 56 percent of the population have never used internet.[7]

In 2011, the most frequent activity among users was the use of social media tools (70 percent of users), while 45 percent of users used the net to search for information and 20 percent browsed the news.[8] With over half of the total number of internet users on Facebook, social networks serve as an important platform for discussion and information exchange among the more liberal segments of Georgian society.[9] State bodies have also stepped up their use of the internet. For example, departments in the Ministry of Justice, the Ministry of Finance's Tax Inspection, and others have developed online services that allow citizens to register and receive services, apply for identification cards, or file tax documentation.

Internet service providers (ISPs) offer dial-up, DSL broadband, fiber-optic, EVDO and CDMA connections. The average cost for an internet connection is US$20 a month, and the lowest price for a 1 Mbps DSL connection is about US$9.[10] Many users complain about the quality of connections and suffer from frequent outages. Nevertheless, there were over

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[3] Tinatin Zurabishvili, *Media Survey 2011, Georgia*, Caucasus Research Resource Centers, 2011, http://www.crrc.ge/oda/.

[4] "What do you do in your free time? – Surf the Internet (%)," *Media Survey 2011, Georgia*, Caucasus Research Resource Centers, 2011, http://www.crrc.ge/oda/?dataset=7&row=18.

[5] "Main source of information about current events in Georgia (%)," *Media Survey 2011, Georgia*, Caucasus Research Resource Centers, 2011, http://www.crrc.ge/oda/?dataset=7&row=22.

[6] "Second source of information about current events in Georgia (%)," *Media Survey 2011, Georgia*, Caucasus Research Resource Centers, 2011, http://www.crrc.ge/oda/?dataset=7&row=23.

[7] "Frequency of Internet usage (%)," *Media Survey 2011, Georgia*, Caucasus Research Resource Centers, 2011, http://www.crrc.ge/oda/?dataset=7&row=391.

[8] Elza Ketsbaia, "Internet usage in Georgia," Net Prophet, January 30, 2012, http://netprophet.tol.org/2012/01/30/internet-usage-in-georgia/.

[9] "Georgia Facebook Statistics," Socialbakers, accessed January 22, 2012, http://www.socialbakers.com/facebook-statistics/georgia.

[10] Comparative data from two major ISP's prices (SilkNet and Caucasus Online).

329,000 fixed-line (broadband) internet connections in 2011 for a broadband penetration rate of 7.6 percent, up from 0.6 percent in 2006.[11]

Mobile phone penetration is greater than that of the internet and has continued to grow from 38.4 percent in 2006 to 102.4 percent in 2011.[12] Mobile phones significantly outnumber landlines, and reception is available throughout the country, including rural areas. The use of mobile devices to connect to the internet has been limited by high costs, but providers are offering new and somewhat less expensive services, including CDMA and EVDO technologies.

The Georgian National Communications Commission (GNCC) introduced mobile number portability in February 2011[13] and fixed-line number portability in December 2011,[14] giving users more freedom to switch between service providers and choose between price plans.[15] According to a new national numbering plan as of January 2012**,** all phone numbers have changed to align with international standards.[16]

The web presence and internet usage of large companies and small businesses grew rapidly in 2011, particularly as a result of social media tools. Many established brands and companies such as banks, financial institutions, artists, public figures, and electronics stores have begun to use social media to promote their businesses and build customer support,[17] and more money is being invested into online projects.[18]

Cybercafes provide internet access at reasonable prices, but they are located mainly in large cities, and there are too few to meet the needs of the population. Most cafes have less than a dozen computers, and customers often have to wait as long as an hour for access. Many restaurants, cafes, bars, cinemas, and other gathering places provide WiFi access, allowing customers to use the internet on their personal laptops.

[11] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions."
[12] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[13] "Ported Subscriber Numbers Statistics," Georgian National Communication Commission, May 25, 2011, http://www.gncc.ge/index.php?lang_id=ENG&sec_id=110&info_id=9071.
[14] "Porting of Subscriber Number of Fixed Network Started From Today," Georgian National Communication Commission, December 1, 2011, http://www.gncc.ge/index.php?lang_id=ENG&sec_id=110&info_id=9812.
[15] Mobile price plan calculator: http://online.gncc.ge/MobileCalc/MobileCalc2.aspx The Calculator gives users the ability to choose best plan and pricing options between mobile operators.
[16] Phone numbers now all begin with *0* and *00* prefixes.
[17] Georgian-language Facebook page statistics service, http://like.ge/ [in Georgian].
[18] According to a leading marketing specialist David Birman: "2011 was the year of discovery of social networks for Georgian Businesses." Source: Commersant.ge, January 25, 2012, http://www.commersant.ge/?id=6504 [in Georgian].

There are 20 ISPs in Georgia, all of which are privately-owned, though two ISPs serve more than two-thirds of the market: SilkNet with more than 44.5 percent and Caucasus Online with a 32 percent share. Three of the 20 ISPs are also mobile operators.[19] While mobile operators have no direct connections to the government, there is no available information on the ownership structure of ISPs, possibly because governmental interests are in play.

The telecommunications infrastructure in Georgia is still weak, and users may experience disconnections from the international internet up to two or three times per month, allowing them to access only Georgian websites. In general, the connection speed for accessing content hosted in Georgia is greater than for international content. There are many factors influencing this, including the major underground fiber-optic cable that is often threatened by landslides, heavy rain, or construction works along the road. In April 2011, for example, an older Georgian woman accidentally cut off an underground cable while looking for scrap metal, causing a large outage of nearly the entire Georgian internet sector that provides service to Armenia, leaving Armenia without an international connection for five hours.[20]

YouTube, Facebook, and international blog-hosting services are freely available. Indeed, Facebook is now the most popular site on the Georgian internet, with bloggers and journalists increasingly using it to share or promote their content, gain readers, and start discussions on current events.

The Georgian National Communications Commission (GNCC) is the main media and communications regulatory body, and although there have yet to be many test cases, it seems to be fair in dealing with internet companies. The GNCC mostly deals with mobile operators as well as television and radio broadcasting licenses. However, there is no significant difference between GNCC procedures for handling traditional media and those pertinent to telecommunications and internet issues, thus criticism surrounding the commission's alleged lack of transparency and flawed licensing procedures for traditional media may reappear in the context of internet regulation. Nevertheless, the GNCC has begun to involve the public in discussions and committee hearings, signaling that it is slowly turning toward openness and transparency.

LIMITS ON CONTENT

There was one reported instance of online content being blocked in Georgia in 2011, involving the block of torrent sites and P2P file-sharing services for several days in June

[19] Data obtained in January 2012. For current data, see Top.ge at http://top.ge/all_report.php [in Georgian].
[20] Tom Parfitt, "Georgian woman cuts off web access to whole of Armenia," The Guardian, April 6, 2011, http://www.guardian.co.uk/world/2011/apr/06/georgian-woman-cuts-web-access.

2011. The block was requested by the Georgian Copyright Association and enforced by the GNCC to prevent the illegal downloading of "5 Days of War,"[21] a Hollywood action drama film about the 2008 Russian-Georgian war.[22] In an effort to encourage Georgians to see the film in theaters instead of illegally downloading it—presumably because the film portrayed Georgian President Mikheil Saakashvili in a positive light—Georgian officials acted rapidly to block torrent sites and forced users to remove the film from other standalone websites.[23] Several blog posts about the movie were also removed. Most alarmingly, the list of websites restricted by the GNCC reportedly included those that had nothing to do with the film but were blocked as a preventive measure.[24]

Aside from the single incident in 2011, government censorship is not a major hindrance to internet freedom in Georgia. Users can freely visit any website around the world, upload or download any content, and contact other users via forums, social-networking sites, and instant messaging applications. In fact, content is so accessible that numerous sites offer illegal material such as pirated software, music, and movies, and the government has not enacted appropriate legal measures to combat the problem. However, as a result of the blocking of the "5 Days of War" film described above, the GNCC announced that they have started working on the issue. ISPs still host websites with a great deal of pirated material,[25] but visits to such sites have decreased and given way to social-networking, video-sharing, blogging, and news sites.[26] Within some state institutions and private companies, there is a small degree of censorship designed to improve worker productivity and limit internet traffic, for example by blocking access to Facebook and YouTube. At the same time, as previously mentioned, both governmental bodies and private employers are increasingly using social media for recruitment and public relations purposes.

There are no laws that specifically govern the internet, regulate online censorship, or ban inappropriate content such as pornography or violent material. The Law of Georgia on the Protection of Minors from Harmful Influence addresses gambling and violence, but it does not refer to online activities.[27] Nevertheless, all legal regulations (especially copyright or criminal law) apply directly to internet activities via the so-called legal analogy, and this

[21] "5 Days of War," IMDB, 2011, http://www.imdb.com/title/tt1486193/.
[22] "Cracking Down on Pirated August War Movie," Georgian America, 2011, http://georgianamerica.com/eng/news/cracking_down_on_pirated_august_war_movie_3179.
[23] "Almighty Mouse and Internet Censorship," Tabula, September 4, 2011, http://en.tabula.ge/article-5322.html.
[24] Attack regarding 5 days of war: http://www.liberali.ge/ge/liberali/articles/106775/ [in Georgian]; "Torrentless worries," Qilipa (blog), June 16, 2011, http://qilipa.wordpress.com/2011/06/16/უ-ტორენტობა-გამოწვევა/ [in Georgian].
[25] See, for example, http://gol.ge/; http://avoe.ge/movies/.
[26] "Top Sites in Georgia," Alexa, accessed August 30, 2012, http://www.alexa.com/topsites/countries/GE.
[27] The law is available in English on the GNCC website at: http://www.gncc.ge/index.php?lang_id=ENG&sec_id=7050&info_id=6521.

legal ambiguity could be exploited to impose significant internet content restrictions in the future.

Self-censorship among Georgian internet users is active to some extent but primarily on issues related to Georgian traditions, social norms, taboos, or religion. For example, the satirical online news agency Ni2.ge (for Niori, or "Garlic," as an allusion to the American satirical newspaper, The Onion), known for its humorous commentary on the Georgian Church and its leader, was shut down in mid-2012 due to pressure the owners received from society.[28] However, a new group of individuals is trying to reanimate the satire news genre in Georgia at the website, Chiti.ge.[29]

There have been some anecdotal reports of the Georgian authorities attempting to manipulate online content, including cases of government employees being forced to "like" Facebook pages of governmental bodies or politicians. Similarly, school children have recounted incidents in which unidentified officials have attended computer classes and asked students to "like" and share specific pages on Facebook. Nevertheless, government manipulation of online content is neither systematic nor pervasive.

Inadequate revenues in the online news business, combined with a lack of technological knowledge, have hampered the expansion of traditional media outlets to the internet. The government's apparent interest in blogging and social media could help spur traditional outlets to establish a greater internet presence, but this would also require more private investment in online advertising. Currently, it is estimated that annual spending on online advertising does not exceed US$1 million,[30] which is only approximately 1 percent of the total amount spent in the Georgian Advertising Market. At present, most online media outlets face difficulty in attracting advertisers, but the problem seems to be more acute for sites that are critical of the government.[31] Some media owners reported instances in which advertisers decided to withdraw ads from websites after those outlets published news articles that were overly critical of the government or the ruling party.

[28] Ni2 News Facebook page, accessed August 30, 2012, https://www.facebook.com/ni2news.
[29] "ctrp415 Satire and News in Georgia," Citizenreporter.org, March 26, 2012, http://citizenreporter.org/2012/03/ctrp415-satire-and-news-in-georgia/.
[30] "The Georgian Advertising Market," Transparency International Georgia, December 2011, http://transparency.ge/sites/default/files/post_attachments/TI%20Georgia%20-%20The%20Georgian%20Advertising%20Market_0.pdf
[31] "Report on the Media and Advertising Industry Research in Georgia," Georgia Management Consulting Group, October 24, 2011, http://irex.ge/wp-content/uploads/Executive-Summary-Georgian-Media-industry-research-INNOVA.pdf.

The Georgian blogosphere grew impressively from 100 blogs in 2010 to over 3,000 blogs in 2011.[32] Minorities are not restricted from internet use, but they are represented online through only a small number of forums and blogs. Similarly, there is little representation of other vulnerable groups, such as internally displaced persons from conflict regions. Although most Georgians use the internet as a source of entertainment, various Web 2.0 applications have become an important platform for discussion and information exchange. Many different political and civil society groups post calls for action on Facebook and use social media marketing tools for communicating with their supporters. Nevertheless, most forms of online activism to date have remained online and have not had a significant impact in real life.

VIOLATIONS OF USER RIGHTS

Civil rights, including the right to access information and freedom of expression, are guaranteed by the Georgian constitution[33] and are generally respected in practice. The Law on Freedom of Speech and Expression "makes it clear that other 'generally accepted rights' related to freedom of expression are also protected even if they are not specifically mentioned."[34] Furthermore, Article 20 of the constitution and Article 8 of the Law of Georgia on Electronic Communications include privacy guarantees for users and their information, but they simultaneously allow privacy rights to be restricted by the courts or other legislation.[35] Internet activities can be prosecuted under these laws—mainly in cases of alleged defamation, which was decriminalized in 2004—or under any applicable criminal law. Furthermore, a huge discussion on the independence of the judiciary has been taking place in Georgian society. International organizations such as Transparency International and Georgian NGO's such as the Georgian Young Lawyers Association have reported that despite recent reforms and changes in the judiciary system, its independence is still tenuous and "suffers from undue influence exerted by the Prosecutor's Office and the executive authority."[36]

Nevertheless, there were no cases of charges against online users for libel or other internet activities in 2011. There were also no known instances of detention or prosecution, and

[32] Zakaria Babutsidze, et al., "The Structure of Georgian Blogosphere and Implications for Information Diffusion," European Consortium for Political Research, August 5, 2011, http://www.ecprnet.eu/MyECPR/proposals/reykjavik/uploads/papers/1676.pdf.
[33] The constitution is available in English at: http://www.parliament.ge/index.php?lang_id=ENG&sec_id=68.
[34] Article 19, *Guide to the Law of Georgia on Freedom of Speech and Expression* (London: Article 19, April 2005), http://www.article19.org/pdfs/analysis/georgia-foe-guide-april-2005.pdf.
[35] The law is available in English on the GNCC website at: http://www.gncc.ge/index.php?lang_id=ENG&sec_id=7050&info_id=3555.
[36] Erekle Urushadze, "Judiciary," in *National Integrity System – Georgia*, ed. Caitlin Ryan (Transparency International – Georgia, 2011), http://transparency.ge/nis/2011/judiciary.

compared to previous years, there were no occurrences of extralegal intimidation or violence against users reported.

The Georgian Law on Operative-Investigative Activity (passed in 1999) grants the police and security services significant discretion in conducting surveillance. Police can generally begin surveillance without a court's approval, though they must obtain it within 24 hours. There are some official requirements for launching such monitoring, but in reality it is sufficient to label the targeted individual a suspect or assert that he may have criminal connections. New amendments to the law promulgated in September 2010 require that websites, mail servers, internet service providers, and other relevant companies make private communications such as emails and chats available to law enforcement authorities when court approval is obtained.[37] There were no known cases of this occurring in 2011.

Additionally, ISPs and mobile phone companies are obligated to deliver statistical data on user activities concerning site visits, traffic, and other topics when asked by the government. Cybercafes, on the other hand, are not obliged to comply with government monitoring, as they do not register or otherwise gather data about customers. Furthermore, individuals are not required to register when they buy a mobile phone, but registration is needed to buy a SIM card and obtain a number.

Cyberattacks against opposition websites have not been a significant issue in Georgia, with the last major attacks occurring in 2008 and 2009 in relation to political tensions between Georgia and Russia. However, in March 2012, the company ESET Antivirus conducted an analysis of a suspicious piece of malware targeting Georgian nationals that specialized in stealing information from an infected system, discovering that the virus had been communicating with the "gov.ge" domain belonging to the Georgian government. According to an ESET Antivirus researcher, "This does not automatically mean that the Georgian government is involved."[38] Rather, the company's analysis concluded that the virus, known as Win32/Georbot, was most likely "created by a group of cyber criminals trying to find sensitive information in order to sell it to other organizations… [and were] 'lucky' enough to gain control of a government website… to use as part of their operation."[39]

[37]Tamar Chkheidze, "Internet Control in Georgia," Humanrights.ge, November 17, 2010, http://www.humanrights.ge/index.php?a=main&pid=12564&lang=eng.

[38] Richard Zwienenberg, "From Georgia With Love: Win32/Georbot information stealing Trojan and botnet," ESET Threat Blog, March 28, 2012, http://blog.eset.com/2012/03/21/win32georbot-information-stealing-trojan-botnet-from-georgia-with-love.

[39] "From Georgia, with Love, Win32/Georbot: Is someone trying to spy on Georgians?" ESET Threat Blog, March 2012, http://blog.eset.com/wp-content/media_files/ESET_win32georbot_analysis_final.pdf.

GERMANY

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	4	4
Limits on Content (0-35)	5	3
Violations of User Rights (0-40)	7	8
Total (0-100)	**16**	**15**

* 0=most free, 100=least free

POPULATION: 82 million
INTERNET PENETRATION 2011: 83 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Germany has a high level of internet and mobile penetration. Media and internet freedom are generally well-respected but have been challenged in recent years by legislative initiatives on blocking of harmful content, as well as surveillance measures by secret services and the police. Nevertheless, 2011 and early 2012 were characterized by a remarkable mainstreaming of internet issues. Topics such as copyright protection, net activism, access blocking, and online surveillance experienced significant attention in federal and state parliaments, major newspapers, and on television.

The growing political relevance of internet-related topics is partly due to an active, articulate, and well-networked civil society, which successfully framed issues such as access blocking in terms of threats to freedom of expression or as incompetence of established political actors in internet regulation. Consequently, in December 2011 the Federal Parliament repealed the Access Restriction Act, which called for blocking of child pornography websites, and instead, most political parties now support the system of take down notices and criminal prosecutions of those who post such content. Internet freedom was also a subject of several important court judgments including a decision to protect as free speech the posting of links that may lead to copyright infringing websites.

Nevertheless, several recent measures, taken by secret services and police in the context of surveillance, violated users' rights and potentially overstepped the existing laws. In October 2011, it became publicly known that the police in several German states used a Trojan-like piece of software in order to spy on criminal suspects. Also, the police systematically used

traffic data obtained by means of radio cell queries to investigate a series of car burnings in Berlin and demonstrations in Dresden

OBSTACLES TO ACCESS

Germany has a very well-developed information and communication technology (ICT) infrastructure, and 73 percent of the population has internet access at home, representing an increase by 6 percentage points between 2010 and 2011.[1] According to the International Telecommunication Union (ITU), overall internet penetration in Germany stood at 83 percent in 2011,[2] and the vast majority of users (86 percent) access the internet through DSL-technology. Alternative connections such as cable and LTE are slowly gaining market share (rising from 10 percent in 2009 to 13 percent in 2011), while 16 percent of the population still relies on dial-up connections.[3] A recent survey by Eurostat shows broadband adoption by Germany households at 78 percent, 10 percentage points above the European Union (EU) average.[4] With regard to high-speed broadband connections above 50 Mbps, there is currently a striking gap between supply and demand. While more than 40 percent of German households have access to high-speed internet connections thanks to well-developed cable networks, the subscriber rate is only 2 percent. Current broadband internet flat rates range from 15€ to 40€ per month (US$20 to $55) depending on the bandwidth of connection.

Most schools in Germany provide computers and internet access to their students mainly in dedicated computer rooms. Only 25 percent of German schools have classrooms equipped with computers.[5] According to an international survey by the World Economic Forum,

[1] Birgit van Eimeren and Beate Frees, *Ergebnisse der ARD/ZDF-Onlinestudie 2011* [Findings of the ARD/ZDF Online Survey 2011], 2011, p. 335, http://www.ard-zdf-onlinestudie.de/ (accessed March 20, 2012).
[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[3] Bundesministerium für Wirtschaft und Technologie [BMWi, Federal Ministry of Economics and Technology], *Breitbandatlas 2011* [Broadband Atlas 2011], 2011a, p. 5, http://www.zukunft-breitband.de/Dateien/BBA/PDF/breitbandatlas-bericht-mitte-2011-teil-1,property=pdf,bereich=bba,sprache=de,rwb=true.pdf; Bundesnetzagentur [Federal Network Agency], *Tätigkeitsbericht 2010/2011 Telekommunikation* [Report 2010/2011 Telecommunications], 2011, p. 34, http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf?__blob=publicationFile; Initiative D21, (N)Onliner Atlas 2011, 2011, p. 61, http://www.initiative21.de/wp-content/uploads/2011/07/NOnliner2011.pdf.
[4] BITKOM, "Breitband-Anschlüsse: Deutschland in der Spitzengruppe" [Broadband connections: Germany in the leading group], Press Release, January 31, 2012, http://www.bitkom.org/de/markt_statistik/64042_71099.aspx. The Federal Network Agency provides different numbers based on provider subscription data it reports 27 million households with a broadband connection (Bundesnetzagentur, 2011, p. 34). For the sake of comparison, the data provided by Eurostat have been chosen.
[5] Initiative D21, "Bildungsstudie: Digitale Medien in der Schule" [Digital Media in Schools], 2011, p. 8-9, http://www.initiative21.de/wp-content/uploads/2011/05/NOA_Bildungsstudie_140211.pdf (accessed 20 March 2012).

Germany ranks tenth among the 15 most developed ICT countries in terms of internet access in schools.[6] Meanwhile, the difference between urban and rural internet access is decreasing with rural areas having higher growth rates. For example, Berlin and Bremen have an 80 percent broadband penetration, while rural Mecklenburg-Vorpommern has 67 percent.[7]

While the gender difference in younger demographics of internet users is disappearing, it persists in the population above 50 and especially among the elderly over 70.[8] Men also significantly outnumber women in the adoption of mobile internet access (26 percent vs. 13 percent). Levels of formal educational remain a crucial factor influencing the use of the internet, as 90 percent of people with higher education access the internet regularly compared to 60 percent of Germans with basic education. However, these gaps are beginning to close as internet penetration increases. In contrast, income-related differences in internet use have persisted: only 53 percent of households with a monthly income below €1,000 (US$1,280) access the internet from home compared to 92 percent of households with an income higher than €3,000 (US$3,835).[9]

Mobile phone penetration in Germany is almost universal, with a penetration rate of over 132 percent at the end of 2011.[10] Only Finland, Italy and Great Britain have higher penetration rates.[11] However, the adoption of mobile internet is below the EU average, with only 28 percent of Germans accessing the internet by phone (compared to 34 percent in the EU).[12] Germany's 3G coverage of 89 percent is also slightly below the EU average.[13]

The telecommunications sector was privatized in the 1990s with the aim of fostering competition. Over the past decade, market consolidation has led to a competitive environment dominated by large companies both in fixed-line as well as mobile internet access; consequently, several smaller internet service providers (ISPs) have been forced out of business. The incumbent Deutsche Telekom's share of the broadband market is 46

[6] Bundesministerium für Wirtschaft und Technologie [BMWi, Federal Ministry of Economics and Technology], *Monitoring-Report Deutschland Digital 2011*, 2011b, p. 75, http://www.bmwi.de/Dateien/BMWi/PDF/IT-Gipfel/ikt-monitoring,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.
[7] BMWi, 2011a, Breitband-Atlas 2011.
[8] Eimeren and Frees 2011, p. 337; Initiative D21, 2011, (N)Onliner 2011, p. 42.
[9] Initiative D21, 2011, (N)Onliner 2011, p. 16.
[10] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[11] Bundesnetzagentur, 2011, p. 50; BMWi 2011b, Monitoring, p. 101.
[12] BMWi, 2011b, Monitoring, p. 119.
[13] European Commission, "3G coverage (as a % of total population)," Digital Agenda Scoreboard Survey 2011, accessed March 20, 2012, http://cl.ly/FL2U.

percent. Other relevant ISPs are 1&1 (United Internet), Arcor (Vodafone), Telefónica, and Kabel Deutschland.[14]

There are four general carriers for mobile internet access: market leader Vodafone (33 percent), incumbent T-Mobile (31 percent), E-Plus (19.8 percent), and Telefonica (16.2 percent). The latter two are more recent market entrants with higher growth rates that have resulted in a redistribution of market shares.[15] In effect, the mobile market is seen as one of the most competitive in the EU,[16] though competition in downstream markets of mobile services such as Voice over Internet Protocol (VoIP) or instant messaging is limited, since all German mobile providers contractually prohibit or limit these services. Nevertheless, these prohibitions have yet to be enforced systematically by the carriers.[17]

Management of network traffic and bandwidth availability is very common.[18] The online platform RespectMyNet.eu,[19] initiated in 2011 by La Quadrature Du Net and Bits of Freedom to collect and publish information on violations of net neutrality in Europe, shows that German users most frequently report the (temporary) throttling of YouTube data, the blocking of peer-to-peer (P2P) websites, and the contractual blocking of internet protocol (IP) telephony servers for mobile internet. Although practically all ISPs support net neutrality in theory, they nonetheless include in their general terms and conditions constraints on internet access. Typical services subject to exclusion or restrictions are tethering (the use of smart phones as a router for providing internet accessing to other devices), VoIP, and limitations of the monthly data volume included in flat rates.

Internet access, both broadband and mobile, is regulated by the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway (Bundesnetzagentur, or BNetzA) operating under the supervision of the Federal Ministry of Economics and Technology. The president and vice president of the agency are appointed for five-year terms by the federal German government following recommendations from an Advisory Council consisting of 16 members of the lower house of parliament and 16 representatives of the upper house. The German Monopoly Commission and the European Commission (EC) have both criticized

[14] European Commission, "New entrants' share in fixed broadband lines," Digital Agenda Scoreboard 2011, accessed March 20, 2012, http://cl.ly/FK1q.
[15] Bundesnetzagentur, 2011, p. 51.
[16] EU Digital Agenda Scoreboard 2011. Electronic Communications Market Indicators, p.10, accessed March 20, 2012. Cf. also the study by Haucaup et al. documenting a fairly competitive market: Haucap/Heimeshoff/Stühmeier, 2010, Wettbewerb im Deutschen Mobilfunkmarkt: Ordnungspolitische Perspektiven Nr. 4.
[17] Call Magazin, "Brüssel will das Blocken von VoIP-Diensten stoppen," April 21, 2011, http://www.call-magazin.de/handy-mobilfunk/handy-mobilfunk-nachrichten/bruessel-will-das-blocken-von-voip-diensten-stoppen_29988.html.
[18] See the report of the Parliamentary Inquiry Commission Internet and Digital Society on net neutrality: p. 12, www.bundestag.de/internetenquete/dokumentation/Netzneutralitaet/Netzneutralitaet_Zwischenbericht_1708536.pdf.
[19] Respect My Net website: http://respectmynet.eu/.

this highly political setting and the concentration of important regulatory decisions in the presidential chamber of the Federal Network Agency.[20] The appointment of President Jochen Homann, the former state secretary in the supervising federal ministry who took over the post from Matthias Kurth after he was surprisingly dismissed in February 2012, seems to affirm the concern over a lack of independence. Similarly, the European Court of Justice (ECJ) and the EC noted that the regulation of data protection and privacy by agencies under state supervision does not comply with the EU Data Protection Directive 95/46/EC.[21]

In addition to such institutional concerns, regulatory decisions by the BNetzA have been criticized for providing a competitive advantage to Deutsche Telekom, the former state-owned monopoly.[22] The most recent example of preferential treatment has been the setting of the price the incumbent is allowed to charge competitors for the "last mile,"[23] yielding one of the highest prices in Europe.[24] The industry associations Eco and BITKOM represent the political and economic interests of ISPs and regularly participate in debates concerning provider liability, copyright enforcement, and access blocking.

LIMITS ON CONTENT

While the blocking of websites rarely takes place in Germany, court orders mandating the deletion of websites have been a common occurrence. Due to substantial criticism by activists and NGOs that provoked an intense political debate, the 2010 law on blocking websites containing child pornography, the Access Restriction Act (Zugangserschwerungsgesetz),[25] never came into effect and was finally repealed by the

[20] Monopolkommission [Monopoly Commission], *Telekommunication 2009: Klaren Wettbewerbskurs halten* (Berlin: Monopolkommission, 2009), 75, http://www.monopolkommission.de/sg_56/s56_volltext.pdf [in German]; European Commission, *Progress Report on the Single European Electronic Communications Market, 15th Report* {COM(2010) 253}, 196, http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/15threport/15report_part1.pdf.

[21] European Commission, "Data Protection: European Commission requests Germany to ensure independence of data supervisory authority," press release, Brussels, April 6, 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/407&format=HTML&aged=0&language=EN&guiLanguage=en.

[22] European Commission, *Progress Report*, 196.

[23] The final leg of delivering connectivity from a communications provider to a customer, see http://en.wikipedia.org/wiki/Last_mile.

[24] For an overview on European prices, cf. the international tariff comparison by the BNetzA, accessed March 20, 2012, http://cl.ly/FW13. For the criticism of the competitors cf. "Telekom muss Miete für die letzte Meile kaum senken," golem.de, March 31, 2011, http://www.golem.de/1103/82473.html.

[25] Law on the reduction of access to child pornography in communication networks (Access Impediment law), February 17, 2010, http://beck-online.beck.de/default.aspx?typ=reference&y=100&g=ZugErschwG.

German parliament in December 2011.[26] The law would have required ISPs to block access to pages containing child pornography and authorized the Federal Criminal Office (BKA) to maintain continuously updated lists of sites to be blocked. All parliamentary parties have now agreed on the position put forward by the Working Group Against Internet Blocking and Censorship (AK Zensur)[27] supporting take down notices and prosecution rather than blocking as an appropriate remedy. Furthermore, attempts by the district council Düsseldorf, North Rhine-Westphalia, to block illegal gambling sites were rejected by various administrative courts.[28]

In response to an initiative by the European Commission on introducing access blocking at the EU level, German diplomats under the auspices of the German Department of Justice joined NGOs and members of the European Parliament in vetoing the proposed directive. In effect, the European Parliament and the European Commission agreed on a considerably weakened directive that no longer includes mandatory EU-wide blocking but rather stipulates that EU member states focus on the removal of webpages containing actionable content (such as child pornography) in and outside their territory.[29]

Evidence suggests that ISPs across Europe regularly use deep packet inspection for the purposes of traffic management but also to throttle peer-to-peer traffic.[30] In Germany, there is a clear lack of transparency regarding the scope of traffic management, in general, and the use of deep packet inspection, in particular, since ISPs are not required to make such information public.

There is no censorship prior to publication of internet content. However, figures released by the Google Transparency Report concerning requests by public authorities for post-

[26] EDRI, "German web blocking law repealed," EDRi-gram Newsletter, No. 9.24, December 14, 2011, http://www.edri.org/edrigram/number9.24/german-internet-blocking-law-repealed.

[27] Ak-Zensur website: http://ak-zensur.de/.

[28] Thomas Stadler, "Auch das VG Köln spricht sich gegen Netzsperren bei Glücksspielen aus" [Also, the Cologne Administrative Court is opposed to Internet blocking in games], Internet-Law (blog), January 12, 2012, http://www.internet-law.de/2012/01/auch-das-vg-koln-spricht-sich-gegen-netzsperren-bei-gluecksspielen-aus.html.

[29] Directive 2011/92/EU of the European Parliament and of the Council of December 13, 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, accessed March 20, 2012, http://eurlex.europa.eu/JOHtml.do?uri=OJ:L:2011:335:SOM:EN:HTML. For more information on the development of this directive, cf. "Provisional conclusion of negotiations on blocking," European Digital Rights Initiative (EDRi), accessed March 20, 2012, http://www.edri.org/blocking_negotiations, and the procedure file of the European Parliament, http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?id=584949.

[30] "BEREC preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely," Body of European Regulators for Electronic Communications, press release, 2012, http://www.erg.eu.int/doc/2012/TMI_press_release.pdf. See also the preliminary report on net neutrality by the multi-stakeholder Commission of Inquiry (Enquete Kommission) on the Internet and Digital Society, set up by the German Federal Parliament in 2010: p. 12, http://www.bundestag.de/internetenquete/dokumentation/Netzneutralitaet/Netzneutralitaet_Zwischenbericht_1708536.pdf .

publication content removal indicate that this strategy is used extensively. During the first six months of 2011, Germany ranked second behind Brazil among 62 listed countries with 125 government requests for the removal of 2,405 items.[31] In the last six months of 2011, Germany ranked third behind Brazil and the United States with 103 government requests to remove 1,722 items.[32] The most common reasons for court order requests were defamation, privacy, and security matters.

The protection of minors constitutes another important legal framework for the regulation of content. Youth protection on the internet is principally addressed by states through the Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting (JMStV), which bans content similar to that outlawed by the criminal code such as the glorification of violence and sedition.[33] A controversial provision of the JMStV reflecting the regulation of broadcasting media mandates that adult-only content on the internet, including adult pornography, must be made available in a way that verifies the age of the user. Compliance with the interstate agreement is overseen by the Commission for Youth Protection Relating to Media. Importantly, the JMStV opens up the prospect of content being blocked if other actions against offenders fail and if the blocking of content is expected to be effective. Owners of offending websites residing outside of Germany are put on blacklists that are made available for privately-developed filtering software. Members of the self-regulatory body, Voluntary Self-control for Multimedia Service Providers (FSM), have committed to removing blacklisted websites from their search results.

In late 2010, the JMStV's planned amendment to introduce age rating for online content failed due to both procedural issues, particularly the lack of public consultation, and substantive issues. According to critics, the amendment did not sufficiently take into account the categorical differences between content made available by broadcasting media and the distributed mode of content production on the internet.

Although access providers are not responsible for the content they transmit, there is a certain tension between the underlying principles of liability privilege and that of secondary

[31] Google complied fully or partially with 86 percent of these requests. Google, "Germany," Google Transparency Report, January to June 2011, accessed August 2, 20122http://www.google.com/transparencyreport/removals/government/countries/?p=2011-06.

[32] Google complied fully or partially with 77 percent of these requests. Google, "Germany," Google Transparency Report, July to December 2011, accessed August 2, 20122, http://www.google.com/transparencyreport/removals/government/DE/?p=2011-12.

[33] Cf. the respective paragraphs 130 and 131 in the Crimical Code: http://dejure.org/gesetze/StGB/130.html; http://dejure.org/gesetze/StGB/131.html.

liability (breach of duty of care).[34] The Telemedia Act §8, based on Articles 12 to 14 of the European E-Commerce Directive, explicitly states that access providers are not legally responsible for the content they transmit over the internet unless they violate reasonable audit requirements or collaborate with users in unlawful behavior. Recent court rulings both on the national and the European level have confirmed the liability privilege for information intermediaries following several years of contradictory rulings. The liability privilege also applies to host providers who are not required to monitor content or install filtering devices. As the European Court of Justice ruled in the 2011 case "Scarlet Extended," "a measure ordering an ISP to install a system for filtering and blocking electronic communications in order to protect intellectual property rights in principle infringes fundamental rights."[35]

Another important ruling refers to liability for URLs. In the 2011 "AnyDVD" case, the German Federal Constitutional Court confirmed a lower court's decision that URLs belonging to copyright infringing websites are protected by freedom of expression and freedom of opinion.[36] Likewise, host providers are not liable for blog entries; they just have to act upon objections.[37] An important exception concerns wireless networks. In 2010, the German Federal High Court sentenced the private owner of a wireless router on the grounds that his or her open network allowed its use for illegal activities.[38] Because of the adverse effects of this judgment on the operators of open networks, the Berlin state legislature is planning to modify the secondary liability in question.[39]

The principle of proportionality has constitutional status in Germany to which public authorities must comply. There is no specific supervisory body in place to oversee the implementation of this principle. Yet, the interplay between the Ministry of Justice, national data protection officer, association of internet service providers (Eco), and internet community effectively hold the bodies involved to account.

[34] Liability privilege means that information intermediaries on the internet such as ISPs are not responsible for the content their customers transmit. Secondary or indirect liability applies when intermediaries contribute to or facilitate wrongdoings of their customers.

[35] Court of Justice of the European Union, PRESS RELEASE No 37/11, Luxumbourg, April 14, 2011, http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037en.pdf.

[36] "German Constitutional Court confirms BGH's 'AnyDVD' copyright decision," The IPKate (blog), February 21, 2012, http://ipkitten.blogspot.de/2012/02/german-constitutional-court-confirms.html. For the concrete reasons given for the judgment, cf. the court's ruling: http://www.bundesverfassungsgericht.de/entscheidungen/rk20111215_1bvr124811.

[37] Cf. the opinion of the court: http://www.telemedicus.info/urteile/Internetrecht/1317-BGH-Az-VI-ZR-9310-Pruefpflichten-fuer-Hostprovider-Blogspot.html.

[38] Christopher Burgess, "Three Good Reasons to Lock Down Your Wireless Network," The Huffington Post (blog), June 8, 2010, http://www.huffingtonpost.com/christopher-burgess/three-good-reasons-to-loc_b_599945.html.

[39] "Berliner Initiative für offene WLANs" [Initiative for free WLAN in Berlin], heise.de, April 7th 2012, http://www.heise.de/newsticker/meldung/Berliner-Initiative-fuer-offene-WLANs-1517403.html.

Court proceedings are generally public, and there are no so-called gag orders that would restrict media coverage of ongoing law suits. While there is no comprehensive list of all content blocking or deletion orders, there is general media coverage of such measures. One important exception in reporting concerns the index of the Commission for the Protection of Minors in the Media (KJM) and the Federal Review Board for Media Harmful to Young People (BpJM), which are kept secret.

There is no systematic self-censorship in the German press; however, there are more or less unspoken rules codified in the publishing principles of the German press.[40] The code, which has the status of a voluntary commitment, specifies the ethical principles of journalism and seeks to strike a balance between the public interest and the protection of personal rights and privacy. Since 2009, these principles have applied to online journalism. The penalty code and JMStV prohibit content in a well-defined manner (e.g. child pornography, racial hatred, and the glorification of violence). The JMStV also regulates adult content that is potentially harmful to minors, stipulating that content unsuitable for certain age groups must be protected to prevent access by children or young individuals (see discussion on deletion of content).

In line with the European Commission's regulatory approach toward net neutrality, the German Federal Network Agency principally supports net neutrality but rejects its legal codification. At the same time, the national regulator has shown sympathy for the ISPs' practice of traffic management. The regulator is also open to new business models based on price discrimination and differentiated classes of service as long as ISPs are transparent about their policies and give customers a choice.[41] Yet, the latest amendment of the Law on Telecommunications (Telekommunikationsgesetz, TKG) adopted in December 2011 authorizes the government to define basic requirements for non-discriminatory data transfer and minimum quality of service standards in order to prevent a deterioration of internet services.[42]

The use of proxy servers is common in Germany but for the purpose of circumventing copyright provisions than to avoid censorship. There are no figures available about the extent of use.

[40] Cf. the codex of the German Press Council: http://www.presserat.info/uploads/media/Novellierter_Kodex_03.pdf.
[41] See the minutes of the Expert Meeting on net neutrality of the Parliamentary Inquiry Commission, October 8th, 2010, http://www.bundestag.de/internetenquete/dokumentation/Netzneutralitaet/Gespraechsprotokoll_-_6_Sitzung_BNetzA_2010-11-08.pdf.
[42] See the report of the parliamentary board of economy and technology, October 26th, 2011: http://dipbt.bundestag.de/dip21/btd/17/075/1707521.pdf.

Germany is home to a vibrant internet community and blogosphere with growing political influence on public and private regulatory action. Policies affecting internet regulation, data protection, or surveillance are enjoying increasing public attention and media coverage. The disproportionate number of young males in the internet community is striking, however. The recent success of the Pirate Party (with 8.9 percent of the vote) and the Saarland (with 7.4 percent)—parties that are known for their strong positions in favor of the free sharing of knowledge and substantial reforms in copyright law—in state elections in Berlin confirms both the growing popularity of internet-related topics and the predominantly male composition of the internet community.

The multi-stakeholder Commission of Inquiry (Enquete Kommission) on the Internet and Digital Society, set up by the German Federal Parliament in 2010, has significantly contributed to the mainstreaming of internet issues.[43] All political parties by now have internet experts and feel the need to express and justify opinions on internet-related topics. Also, there are regular public interactions between politicians and the internet community on Twitter and blogs and at public events. An example of the growing discursive power of the internet community concerns the forced resignation of the defense minister in 2011 due to plagiarism exposed in detail on a dedicated website.[44] Another example involved the widespread demonstrations in roughly 60 German cities against the Anti-Counterfeiting Trade Agreement (ACTA) in early 2012, which led the minister of justice to make a political U-turn and put the signing of ACTA on hold.

VIOLATIONS OF USER RIGHTS

German Basic Law guarantees freedom of expression and freedom of the media (Article 5) as well as the privacy of letters, posts, and telecommunications (Article 10). These articles generally safeguard offline as well as online communication. In addition, a groundbreaking 2008 ruling by the Federal Constitutional Court established a new fundamental right warranting the "confidentiality and integrity of information technology systems" that is grounded in the general right of personality guaranteed by Article 2 of the Basic Law.[45]

[43] Cf. the website of the commission: http://www.bundestag.de/internetenquete/

[44] Cf. the website "GuttenPlag": http://de.guttenplag.wikia.com/wiki/GuttenPlag_Wiki.

[45] Bundesverfassungsgericht [Federal Constitutional Court], Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the Internet null and void, Judgment of 27 February 2008, 1 BvR 370/07; 1 BvR 595/07, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007en.html; See also, Press release no. 22/2008, http://www.bundesverfassungsgericht.de/en/press/bvg08-022en.html. For more background cf. W Abel and B Schafer, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822," (2009) 6:1 *SCRIPTed* 106, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.

These rights were contested in the political aftermath of the September 2001 terrorist attacks in the United States (cf. the 2001 Act for Limiting the Secrecy of Letters, the Post, and Telecommunications).[46] However, after several cases concerning the infringement of journalists' rights, a Federal Constitutional Court ruling in February 2007 set a strong precedent for the protection of journalists' sources.[47] Following this ruling, the federal parliament issued in 2012 the Act on Strengthening Press Freedom (Gesetzes zur Stärkung der Pressefreiheit im Straf- und Strafprozessrecht, PrStG), which protects journalistic sources and establishes high barriers for searching and seizing journalists' properties.[48] In addition to the aforementioned rulings on the liability privilege of providers, these developments constitute a trend of strengthening media freedom in Germany. The rulings of the Federal Constitutional Court continue to promote freedom of expression in particular.

Online journalists are generally accorded the same rights and protections as journalists in print or broadcast. Although the functional boundary between journalists and bloggers is becoming blurry, the German federation of journalists maintains professional boundaries by handing out press cards only to full-time journalists. Similarly, the German Code of Criminal Procedure grants the right to refuse testimony solely to individuals who have "professionally" participated in the production or dissemination of journalistic materials."[49]

Incidents of confiscated video material covering demonstrations, for example, have led to a debate about extending the right to refuse testimony to a larger group. In August 2011, the Pirate Party filed a petition to the Federal Parliament asking to discard the term "professionally" in the relevant paragraph of the German Code of Criminal Procedure, but this issue has not gained a lot of attention.[50]

[46] This Act enables secret services to intercept, monitor, and record private communications, including the surveillance of journalists under specific conditions. It also restricts journalistic privileges such as the right to refuse to give evidence. "Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses" [Law on the restriction of correspondence, posts and telecommunications secrecy], Bundesministerium der Justiz, accessed March 20, 2012, http://www.gesetze-im-internet.de/g10_2001/index.html.

[47] Bundesverfassungsgericht [Federal Constitutional Court], "Cicero-Urteil," Decision 1 BvR 538/06, accessed March 20, 2012, http://www.bverfg.de/entscheidungen/rs20070227_1bvr053806.html. For the European context, see David Banisar, *Speaking of Terror: A Survey of the Effects of Counter-terrorism Legislation on Freedom of the Media in Europe* (Strasbourg: Council of Europe, 2008), accessed March 20, 2012, http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf.

[48] Cf. the press release of the Federal Ministry of Justice, accessed March 20, 2012: http://cl.ly/FVeK.

[49] Strafprossordnung (StPO) [Code of Criminal Procedure], Paragraph 53 (1) 5, accessed March 20, 2012, http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0198.

[50] File of the petition in the parliamentary epetition-system, accessed March 20, 2012, https://epetitionen.bundestag.de/index.php?action=petition;sa=details;petition=19350.

The German penal code (StGB) includes a paragraph on "incitement to hatred" (StGB §130), which penalizes calls for violent measures against minority groups and assaults on human dignity.[51] This provision is generally regarded as legitimate by the German population not least because it is mostly applied in the context of holocaust denials.

The anonymous use of email services, online platforms, wireless internet access points, and public telephone booths are legal. Although the federal minister of the interior and other members of the conservative parties have repeatedly expressed their disapproval of anonymity on the net,[52] this situation is not likely to change. With explicit references to the constitution, several courts have repeatedly affirmed the right to anonymity and its necessity for the exercise of the constitutional right to freedom of expression.[53] At the same time, the Telemedia Act (Telemediengesetz, TMG) and the Interstate Treaty on Broadcasting (Rundfunkstaatsvertrag, RFStV) mandate a legal notice that includes contact data for most websites and blogs.

Under Sections 112 and 113 of the Telecommunications Act, law enforcement agencies and prosecutors can obtain users' contractual data without a judge's order. For traffic and content data, however, judicial approval is required. The Federal Network Agency serves as the data collecting intermediary between telecommunications companies and law enforcement bodies. The agency reported six million requests from public authorities and 36 million queries directed to telecommunications service providers in 2010.[54] A small number of government entities are authorized, for narrowly circumscribed purposes, to request sensitive data under Section 113 of the Telecommunications Act (TKG). This data may include personal identity numbers (PINs), personal unblocking keys (PUKs), and passwords that allow access to devices or online services. Such inquiries may only be used to identify the person who generated a certain communication or connection at a certain point in time.[55]

---

[51] For an English translation of the German penal code see: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P130, accessed March 20, 2012.

[52] See for example, "Innenminister Friedrich will Blogger-Anonymität aufheben" [Federal Minister of Interior wants to abolish anonymity of bloggers], Tagesspiel online, August 7, 2011, http://www.tagesspiegel.de/politik/internet-innenminister-friedrich-will-blogger-anonymitaet-aufheben/4473060.html.

[53] Eg. Oberlandesgericht (OLG) Hamm [German Federal Court of Appeals Hamm], File I-3 U 196/10, August 3, 2011, http://www.justiz.nrw.de/nrwe/olgs/hamm/j2011/I_3_U_196_10beschluss20110803.html.

[54] The period from 2001 to 2010 shows a steady increase on both counts, from an initial 1.5 million requests from security authorities and 3.2 million queries by the Federal Network Agency in 2001, cf. Bundesnetzagentur, *Annual Report 2010*, 125, accessed March 20, 2012, http://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/ReportsPublications/2011/AnnualReport2010pdf.pdf.

[55] This procedure was ruled as partly unconstitutional by the Federal Constitutional Court in January 2012. The legislative is asked to revise the paragraph until 30 June 2013. Federal Constitutional Court, Decision 1 BvR 1299/05, January 24, 2012, http://www.bundesverfassungsgericht.de/entscheidungen/rs20120124_1bvr129905.html.

Telecommunications interception by state authorities is regulated by the code of criminal procedure (StPO) and is understood as a serious interference with basic rights. It may only be employed for the prevention or prosecution of serious crimes for which specific evidence exists and when other less intrusive investigative methods are likely to fail. According to recent statistics published by the Federal Office of Justice, there were a total of 20,398 orders for telecommunications interception in 2010, of which 997 concerned internet communications. This is an increase of about 25 percent compared to 2008.[56] There were also a total of 12,576 orders asking for internet traffic data in 2010.[57]
Surveillance measures conducted by the secret services under the Act for Limiting the Secrecy of Letters, the Post, and Telecommunications exceed these figures. The competent Parliamentary Control Panel reported for 2011 a total of 37 million emails scanned, of which only 239 were considered relevant.[58]

Excessive interceptions by secret services formed the basis of a 2008 Federal Constitutional Court ruling, which established a new fundamental right warranting the "confidentiality and integrity of information technology systems." The court held that preventive covert online searches are only permitted "if factual indications exist of a concrete danger" that threatens "the life, limb, and freedom of the individual" or "the basis or continued existence of the state or the basis of human existence." The court also established that any covert infiltration of information technology systems requires a court order and that statutes permitting such infiltrations must "contain precautions in order to protect the core area of private life."[59] Based on this Constitutional Court ruling, the Federal Parliament passed an act in 2009 authorizing the Federal Bureau of Criminal Investigation (BKA) to conduct covert online

[56] Bundesamt für Justiz [Federal Office for Justice], "Übersicht Telekommunikationsüberwachung (Maßnahmen nach §100a StPO) für 2010," July 29, 2011, http://www.bundesjustizamt.de/cln_115/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Uebersicht__TKUE__2010,templateId=raw,property=publicationFile.pdf/Uebersicht_TKUE_2010.pdf [in German].
[57] Bundesamt für Justiz, "Übersicht Verkehrsdatenerhebung (Maßnahmen nach § 100g StPO) für 2010," July 29, 2011, http://www.bundesjustizamt.de/cln_115/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Uebersicht__Verkehrsdaten__2010,templateId=raw,property=publicationFile.pdf/Uebersicht_Verkehrsdaten_2010.pdf [in German].
[58] Cf. the report of the Parliamentary Control Panel: Deutscher Bundestag, Drucksache 17/8639, February 10, 2012, http://dipbt.bundestag.de/dip21/btd/17/086/1708639.pdf. The Parliamentary Control Panel periodically reports to the parliament and nominates the members of the G 10 Commission. The G 10 Commission controls surveillance measures and is also responsible for overseeing telecommunications measures undertaken on the basis of the Counterterrorism Act of 2002 and the Amendment Act of 2007. See also: http://www.bundestag.de/htdocs_e/bundestag/committees/bodies/scrutiny/index.html [in German].
[59] Bundesverfassungsgericht [Federal Constitutional Court], Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the Internet null and void, Judgment of 27 February 2008, 1 BvR 370/07; 1 BvR 595/07, See also, http://www.bundesverfassungsgericht.de/en/press/bvg08-022en.html, accessed March 20, 2012. For more background cf. W Abel and B Schafer, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822," (2009) 6:1 *SCRIPTed* 106, accessed March 20, 2012, http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.

searches to prevent terrorist attacks on the basis of a warrant.[60] In addition to online searches, the act authorizes the BKA to employ methods of covert data collection including dragnet investigations, surveillance of private residences, and the installation of a program on a suspect's computer that intercepts communications at their source.

In October 2011, the Chaos Communication Club (CCC), a German hacker organization, uncovered the use of a Trojan-like piece of software by the police for crime investigation purposes in several German states. The CCC's analysis of the software showed that the Trojan not only enables the police to (legally) eavesdrop on encrypted conversations but also allows for a far wider range of actions, which are illegal to deploy for both police and secret services. Among these encroachments include the searching of digital devices, logging of keystrokes, and even planting of "backdoors" that allow for the remote installment of additional software or insertion of false evidence. Five German states admitted the use of the "Bundestrojaner" (Federal Trojan) as such but denied the use of any illegal functions.[61]

Together with evidence that the police made use of radio cell queries in the context of the car burnings investigations in Berlin in late 2009 and demonstrations in Dresden in 2011 and 2012,[62] the proportionality of the surveillance measures must be questioned. However, the rulings of the Federal Constitutional Court form a strong counterweight to massive violations of user rights.

Following the EU Data Retention Directive, the 2007 Law on the Revision of Telecommunications Monitoring and other Covert Investigation Measures and the Implementation of Directive 2006/24/EC require ISPs and mobile phone companies to retain traffic data for six to seven months to facilitate criminal investigations. A constitutional complaint filed by nearly 35,000 individuals, including the justice minister herself, with the Federal Constitutional Court led to the repeal of the national data retention provisions in 2010.[63] A revision of the data retention law, as required by the European Commission, is still pending as of mid-2012. Under discussion is the option of a "quick freeze" procedure for traffic data which would allow for data to be stored only upon concrete preservation orders from law enforcement agencies. A legal opinion commissioned

[60] "Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten," http://www.gesetze-im-internet.de/bkag_1997/ (accessed March 20, 2012). Cf. Dirk Heckmann, "Anmerkungen zur Novellierung des BKA-Gesetzes: Sicherheit braucht (valide) Informationen," Internationales Magazin für Sicherheit nr. 1 (2009), http://www.ims-magazin.de/index.php?p=artikel&id=1255446180,1,gastautor [in German].
[61] Deutsche Welle, "Several German states admit to use of controversial spy software," October 11, 2011, http://www.dw.de/dw/article/0,,15449054,00.html.
[62] André Meister, "Massenhafte Funkzellenabfrage jetzt auch in Berlin: Was Vorratsdatenspeicherung wirklich bedeutet," Netzpolitik.org (blog), January 19, 2012, http://cl.ly/FjXb [in German].
[63] "Leitsätze zum Urteil des Ersten Senats vom2. März 2010" [Guidelines to the judgment of the First Senate of March 2, 2010], Bundesverfassungsgericht, accessed August 20, 2012, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

by the federal government expressed strong doubts about the compatibility of the data retention directive with the European Charter of Fundamental Rights.

As part of the data retention law, the government also revised the duty of identification, obliging ISPs to store contractual data of their customers. The obligatory identification concerns phone lines, SIM cards for mobile phones, and DSL connections. Email, WLAN services, and internet cafes are exempted from this obligation.

Building on the Safer Social Networking Principles for the EU,[64] the minister of interior suggested in 2011 that providers of social networks and search engines agree upon a code of conduct in order to support the protection of minors and that of consumers.[65] This initiative also follows a national code of conduct developed under the auspices of the organization for Voluntary Self-Monitoring of Multimedia Service Providers (FSM), which focuses on data protection for minors.[66]

As part of its cyber security strategy,[67] the federal government established in 2011 a cyber-defense center operating under the auspices of the Federal Office for Information Security, itself a subordinate body of the Federal Ministry of the Interior. In the face of an increasing number of cyberattacks, the German government has attached growing importance to the protection of "critical infrastructure."[68] Within the first months of its activity, the cyber-defense center apparently dealt with three to five cases of cybercrime a day.[69] Considering the potential impact of cybercrime and its conspicuous rise since 2009, the founding of a cyber-defense center is viewed as a useful if somewhat belated step.

[64] European Commission, "Safer Social Networking Principles for the EU," February 10, 2009, http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

[65] Innenministerium setzt auf Datenschutz-Selbstkontrolle von Facebook [German Government favors self-regulation by Facebook], heise.de, September 8, 2011. http://www.heise.de/newsticker/meldung/Innenministerium-setzt-auf-Datenschutz-Selbstkontrolle-von-Facebook-1339410.html.

[66] Cf. the code of conduct on the website of the FSM: http://fsm.de/de/Web_2_0.

[67] Cf. the policy paper on Cybersecurity of the Federal Ministry of Interior: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile.

[68] Cf. the press release of the Federal Ministry of Interior: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/mitMarginalspalte/06/cyber.html.

[69] "Täglich bis zu fünf Fälle für das Cyber-Abwehrzentrum" [Cyber-defense center handles five cases each day], FOCUS Online, June 8, 2011, http://www.focus.de/digital/computer/computer-taeglich-bis-zu-fuenf-faelle-fuer-das-cyber-abwehrzentrum_aid_635369.html.

HUNGARY

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Free**
Obstacles to Access (0-25)	n/a	5
Limits on Content (0-35)	n/a	6
Violations of User Rights (0-40)	n/a	8
Total (0-100)	**n/a**	**19**

* 0=most free, 100=least free

POPULATION: 9.9 million
INTERNET PENETRATION 2011: 59 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

When Hungary transitioned from a one-party state to a parliamentary democracy in 1989-1990, very few people were using the internet in the country. In the following years, dial-up connections spread and the number of users expanded, particularly in the 2000s when the price of internet started to decrease while the availability of broadband connections increased. Today, a majority of the population is online. Information and communication technologies (ICTs) are being used not only for social activities and newsgathering, but also increasingly for political activism.

In the 2010 parliamentary elections, the conservative Hungarian Civic Union (Fidesz) and its ally, the Christian Democratic People's Party (KDNP), won a landslide victory gaining more than two-thirds of the seats, which enabled them to draft and accept a set of laws in late 2010 regulating the media,[1] including online media outlets and news portals. A new regulatory authority, the National Media and Infocommunications Authority (NMHH), was also established to oversee the mass communications industry with the power to penalize or suspend outlets that violate stipulations of the media regulation. While the 2010 media laws threaten to have a chilling effect on journalism, the Hungarian Constitutional Court annulled a few of the laws' provisions in December 2011, finding them to be an infringement on freedom of expression and leaving the legislators until May 31, 2012 to modify them.

Hungary adopted a new constitution, the Fundamental Law of Hungary, in April 2011 that

[1] Act CIV of 9 November 2010, On the freedom of the press and the fundamental rules on media content, and Act CLXXXV of 30 December 2010, On media services and on the mass media.

includes a provision concerning the supervision of the mass communications industry and media as a whole.[2] The new constitution also created the National Agency for Data Protection whose independence has been called into question due to the political appointment process of the agency's leadership.

OBSTACLES TO ACCESS

According to the International Telecommunications Union (ITU), internet penetration in Hungary stood at 59 percent in 2011,[3] up from 47 percent in 2006, while the National Media and Infocommunications Authority of Hungary (NMHH) reported in late 2011 that 54.5 percent of households have a broadband internet subscription.[4] Dial-up internet service is not widely used. The ITU and NMHH also recorded a mobile phone penetration rate of 117.3 percent and 2,155,000 mobile internet subscriptions, while nearly 70 percent of residential areas had 3G coverage in 2011.[5] Nevertheless, 28 percent of the population had never used the internet.[6]

There are geographical, socioeconomic, and ethnic differences in Hungary's internet penetration, with low access rates found in rural areas[7] and among the Roma community, the country's largest ethnic minority.[8] Most internet users access the internet from home, work, and school, while access at internet cafes and telecottages (local community centers) is less common.[9] Cybercafes do not need prior approval to open or operate.

[2] The Fundamental Law of Hungary, Art. VIII, par. 3, http://tasz.hu/files/tasz/imce/alternative_translation_of_the_draft_constituion.pdf.

[3] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[4] "Flash report on wireline service," National Media and Infocommunications Authority (NMHH), November 2011, http://www.nmhh.hu/dokumentum.php?cid=29609&letolt.

[5] "Flash report on mobile internet," NMHH, December 2011, http://www.nmhh.hu/dokumentum.php?cid=29784&letolt; Hungary's population was 9,962,000 by the end of 2011. See, "Population, vital events," Hungarian Central Statistical Office (KSH), accessed August 15, 2012, http://portal.ksh.hu/pls/ksh/docs/eng/xstadat/xstadat_infra/e_wdsd001a.html.

[6] "Individuals who have never used the internet. Percentage of individuals aged 16 to 74," Eurostat, accessed January 23, 2012, http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00093.

[7] Anna Galácz, Ithaka Kht, eds., "A digitális jövő térképe. A magyar társadalom és az internet. Jelentés a World Internet projekt 2007. évi magyarországi kutatásának eredményeiről" [The map of the digital future. The Hungarian society and the internet. Report on the results of the 2007 World Internet Project's Hungarian research], (Budapest: 2007), p. 20.

[8] Statistically speaking, someone who is younger, studying, working or has a degree, and living in the capital or in a city is more likely to use internet than the elderly, unemployed or pensioner, with lower educational background, living in a village. See, World Internet Project (WIP), *Report on the Hungarian Research for the World Internet Project 2007* (Budapest: Ithaka, 2008), pg. 26, http://worldinternetproject.com/_files/_Published/_oldis/Hungary_Report_2007.pdf; "Internet-riport 2011/Q3" [Internet-report 2011/Q3], Nrc.hu, January 13, 2012, http://nrc.hu/index.php?name=OE-eLibrary&file=download&keret=N&showheader=N&id=215.

[9] World Internet Project, "Map of the Digital Future: Hungarian Society and the Internet," 2007, http://www.worldinternetproject.net/_files/_Published/_oldis/Hungary_Report_2007.pdf.

The Budapest Internet eXchange (BIX) is a network system that maintains the Hungarian internet traffic between domestic internet service providers (ISPs) and is overseen by the Council of Hungarian Internet Service Providers (ISZT)[10] without any governmental interference.[11] Shutting down the BIX would only slow down the internet in Hungary, and as BIX includes a domain name system (DNS) server that translates ".hu" domains, interfering with it would cause further difficulties.[12] The government does not restrict bandwidth, routers, or switches,[13] and backbone connections are owned by telecommunications companies.[14] Legally, however, the internet and other telecommunications services can be paused or limited in instances of unexpected attacks, for preemptive defense, or in states of emergency or national crisis.[15]

YouTube, Facebook, Twitter, international blog-hosting services, instant messaging, person-to-person communication, and other Web 2.0 applications are freely available. An increasing number of widely used software and websites are available in Hungarian, and there are several Hungarian blog-hosting sites.[16] By the end of 2011, there were more than 600,000 registered ".hu" domains[17] recorded at some 130 companies.[18]

Ten ISPs share 94 percent of the total fixed broadband market,[19] and there are three mobile phone providers, all privately owned by foreign companies.[20] Additional actors began entering the mobile phone market in 2012, including a virtual mobile company operated by British Tesco and a mobile frequency tender that was won by a consortium of state-owned companies.[21]

Following the passage of the 2010 media laws, the NMHH was established to oversee the

[10] "BIX Charter," Budapest Internet Exchange (BIX), April 21, 2009, http://bix.hu/?lang=en&page=charter.
[11] Zoltán Kalmár, Council of Hungarian Internet Service Providers, email communication, January 24, 2012.
[12] "Le lehetne kapcsolni a magyar internetet is?" [Could the Hungarian internet be shut down too?], Index.hu, February 11, 2011, http://index.hu/tech/net/2011/02/11/le_lehetne_kapcsolni_a_magyar_internetet_is/.
[13] Zoltán Kalmár, Council of Hungarian Internet Service Providers, email communication, January 24, 2012.
[14] "Magyarország internetes infrastruktúrája" [Hungary's internet infrastructure], Rentit.hu, January 29, 2010, http://www.rentit.hu/cikk/83/magyarorszag-internetes-infrastrukturaja.aspx.
[15] Act CXIII of 2011 on home defense, Military of Hungary, and the implementable measures under special legal order, Art. 68, par. 5.
[16] The largest Hungarian blog hosting site is Blog.hu with over 100,000 blogs, of which 17,000 are updated regularly. See, Cemp Sales House, "Médiaajánlatok" [Media offers], accessed January 27, 2012, http://ajanlat.index.hu/ajanlatok/.
[17] "The number of domains under the .hu public domains," Council of Hungarian Internet Providers, accessed January 23, 2012, http://www.nic.hu/English/statisztika/.
[18] "List of registrars," Official .hu domain registry, accessed January 24, 2012, http://www.domain.hu/domain/English/.
[19] Major ISPs are: T-Home with a 62 percent market share, Invitel 13 percent, and UPC 10 percent. See, "Flash report on wireline service," NMHH, November 2011.
[20] The three mobile phone companies are: T-Mobile with a 45 percent market share, Telenor 32 percent, and Vodafone 23 percent. See, "Flash report on mobile phone," NMHH, December 2011.
[21] "State-run consortium bags biggest frequency block at auction," Bbj.hu, January 31, 2012, http://www.bbj.hu/business/update---state-run-consortium-bags-biggest-frequency-block-at-auction--_62585.

mass communications industry. Its activities range from mobile phone frequency allocation to telecommunications market surveillance.[22] The NMHH also maintains an administrative register of media service providers that includes online media services and news portals.[23]

The Media Council is the NMHH's decision-making body related to media outlets, and its responsibilities include allocating television and radio frequencies and penalizing violations of media regulations. The members of the Media Council are nominated and elected by the governing two-thirds parliamentary majority.[24] The current president of NMHH, a former Fidesz member of parliament, is also the president of the Media Council and appointed directly by the prime minister for a nine-year term, indicating the council's lack of independence.[25] As the media authority was established in 2010, it is too early to assess the extent of politicization in its decision-making. Nevertheless, a 2011 decision on a regional radio's frequency is considered to be controversial,[26] and in January 2012, the NMHH accepted only one new registration application for a mobile phone frequency tender from a consortium of state-run companies, rejecting all other applicants based on "formal deficiencies."[27]

In the new Hungarian constitution adopted in April 2011, the governing parties prematurely ended the six-year term of the well-functioning Data Protection Commissioner, replacing the former office with the National Agency for Data Protection. The head of the new agency is appointed by the prime minister for a nine-year term and can be dismissed by the president or prime minister on arbitrary grounds,[28] calling into question the independence of the agency.

LIMITS ON CONTENT

The government does not mandate any type of technical filtering of websites, blogs, or text messages.[29] Anyone can launch a blog or a website to freely express his or her opinion.

[22] Act CLXXXV of 2010, On media services and mass media, Art. 110, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/hungarian_media_law/hungarian_media_lawen.pdf.
[23] Ibid, Art 41-46.
[24] Act CLXXXV of 2010, Art. 124.
[25] Act CLXXXV of 2010, Art. 111, par. 3.
[26] "Memorandum to the European Union on Media Freedom in Hungary," Human Rights Watch, February 16, 2012, http://www.hrw.org/news/2012/02/16/memorandum-european-union-media-freedom-hungary.
[27] "State-run consortium bags biggest frequency block at auction," Bbj.hu, January 31, 2012.
[28] Act CXII of 2011, On data protection and freedom of information, Section 40, par. 1, 3; Section 45, par. 4–5, http://www.naih.hu/files/ActCXIIof2011_mod_2012_05_09.pdf.
[29] Even though Hungary signed the Anti-Counterfeiting Trade Agreement (ACTA)–which still needs to be ratified by the parliament–it does not impose any stricter rules related to intellectual property than the operating Hungarian laws, according to the National Board Against Counterfeiting. See, "Kérdések és válaszok a Hamisítás Elleni Kereskedelmi Megállapodásról (ACTA)"

Nevertheless, the 2010 media laws contain several general content regulation provisions concerning online media outlets, particularly if they provide services for a profit. For example, online media outlets bear editorial responsibility if their aim is to distribute content to the public for "information, entertainment or training purposes."[30] A member of the Media Council claimed that a blog qualified as such if it was produced for a living.[31]

The 2010 media laws also stipulate that media content—both online and offline—may not offend, discriminate or "incite hatred against persons, nations, communities, national, ethnic, linguistic and other minorities or any majority as well as any church or religious groups."[32] Further, human dignity, constitutional order, and human rights must be respected, and privacy and public morals cannot be violated.[33] However, the law does not define the meaning of "any majority" or "public morals." If a media outlet does not comply with the law, the Media Council may oblige it to "discontinue its unlawful conduct,"[34] publish a notice of the resolution on its front page, and/or pay a fine of up to 25 million forints (US$124,415). If a site repeatedly violates the stipulations of the media regulation, the intermediary service provider can be obligated to suspend the site's given domain, and as a last resort, the media authority can delete the site from the administrative registry.[35] Any such action can be appealed in court.

Critics of the 2010 media laws contend that the Media Council operates with unclear provisions and imposes high fines and sanctions on media outlets,[36] which might give rise to uncertainty and fear, lead to self-censorship, and have a chilling effect on journalism as a whole. Nonetheless, as of May 2012, no online media outlet had been penalized for violating the 2010 media laws, and in December 2011, the Constitutional Court struck down several provisions applicable to print and online outlets.[37]

Intermediary service providers are not legally responsible for transmitted content if they did not initiate or select the receiver of the transmission, or select or modify the transmitted

[Questions and Answers on the Anti-counterfeiting Trade Agreement (ACTA)], February 3, 2012, http://www.hamisitasellen.hu/hu/hirek/2012/kerdesek-es-valaszok-a-hamisitas-elleni-kereskedelmi-megallapodasrol-acta.

[30] Act CIV of 2010, On the freedom of the press and the fundamental rules on media content, Art. 1, par. 6, http://hunmedialaw.org/dokumentum/152/Smtv_110803_EN_final.pdf.

[31] "Tanácsnokok és bloggerek" [Members and bloggers], Mediatanacs.blog.hu, January 11, 2011, http://mediatanacs.blog.hu/2011/01/11/tanacsnokok_es_bloggerek.

[32] Act CIV of 2010, Art. 17.

[33] Act CIV of 2010, Art. 14, 16, 18, and 4, par. 3.

[34] Ibid.

[35] Act CLXXXV of 2010, Art. 186, par. 1., 187, par. 3, 189, par. 4.

[36] "Hungarian media laws Q&A," Article 19, August 2011, http://www.article19.org/data/files/medialibrary/2714/11-09-01-REPORT-hungary.pdf.

[37] Judit Bayer, "Hungarian Constitutional Court repeals parts of Media Constitution and Media Law," Media Laws, December 29, 2011, http://www.medialaws.eu/hungarian-constitutional-court-repeals-parts-of-media-constitution-and-media-law/.

information.[38] Further, ISPs are also not obliged to verify the content they "transmit, store or make available," nor do they need to search for unlawful activity.[39]

The NMHH operates an internet hotline where disturbing or allegedly unlawful content such as child pornography can be reported. In cases of a "presumably illegal website," the authority asks the content provider to delete the offending content and notifies the police. It is highlighted that the hotline is "not an authority procedure, but an activity undertaken by the NMHH in the name of corporate social responsibility," and it cannot force deletion; rather, it can only "request the removal of the contested content."[40] Cases of copyright infringement are usually considered under civil law and can result in the "destruction of the device or material."[41] However, copyright infringement cases that cause financial injury can be punishable by imprisonment under the Criminal Code.[42]

There is only anecdotal evidence on the extent of online self-censorship in Hungary, which is not due to direct state interference but to political or economic pressure. As one investigative journalist put it, "the threat of a lawsuit is often enough for Hungarian media companies to publish demanded corrections immediately, without trying to defend their work in court," and the interests of media owners can lead to "excessive self-censorship."[43] A 2006 journalist survey indicated that for online news sites, attempts to apply political or economic pressure were low compared the traditional media sphere.[44] However, recent cases suggest that some kind of pressure provoking self-censorship does exist in state-run media.[45]

Since 2011, the state-owned Hungarian News Agency (MTI) has had a virtual monopoly on the news market, as most of its news items are available free of charge. Consequently, media outlets that have been impacted by the economic crisis tend to publish MTI news items. Csaba Belénessy, head of the MTI, said in an interview that "a public service media outlet has to be loyal to the government and fair to the opposition."[46] The 2010 media laws oblige the MTI to produce news bulletins for public service broadcasters and edit their joint news

[38] Act CVIII of 2001, Act on E-Commerce, Art. 8, par. 1.
[39] Act CVIII of 2001, Art. 7. par. 3.
[40] "Operation of the Internet Hotline," Internethotline.hu, accessed June 27, 2012, http://internethotline.hu/tart/index/51/Operation_of_the_Internet_Hotline.
[41] Act LXXVI of 1999, On Copyright, Art. 94, http://www.oapi.wipo.net/wipolex/en/text.jsp?file_id=127828#P530_98754.
[42] Act IV of 1978, On the Criminal Code, Art. 329/A, http://www.wipo.int/wipolex/en/details.jsp?id=2199.
[43] Tamás Bodoky, "Hungarian media law doomed," Reportingproject.net, accessed August 15, 2012, http://www.reportingproject.net/occrp/index.php/press-box/882-hungarian-media-law-doomed.
[44] Mária Vásárhelyi, "Foglalkozása: újságíró" [Profession: journalist], Magyar Újságírók Országos Szövetsége, Budapest, 2007, p. 84.
[45] "Journalists protest manipulation with hunger strike," Spiegel.de, December 16, 2011, http://www.spiegel.de/international/europe/0,1518,804299,00.html.
[46] Ágnes Lampé, "Kormányfelügyelet a médián: »Most tesszük le a magyar BBC alapjait«" [Government control over the media: "We establish the basis of the Hungarian BBC"], 168ora.hu, December 13, 2010, http://www.168ora.hu/itthon/kovetkezik-a-hirado-kapcsoljuk-az-mti-t-66216.html.

portal.[47]

The information landscape of online content in Hungary is relatively diverse. The two main news portals in Hungary are Index.hu and Origo.hu, both of which have around 750,000 individual visitors daily.[48] Most civil society organizations have websites, and an increasing number of them have a presence on Facebook. There are some media outlets, including online portals, for the minority Roma community;[49] the LGBT community and religious groups have their online sources and forums as well. Nevertheless, Hungarian society is politically divided, as is the press, and partisan journalism is widespread.[50] Blogs are generally considered an opinion genre and do not typically express independent or balanced news. According to one study, 46.5 percent of blog readers consume blogs on politics and current affairs, and one of the reasons why people read blogs is because they represent strong opinions.[51] There are also blogs analyzing governmental policies, the activities of public figures, and corruption.[52] Trolling is usually moderated where it is possible to comment on articles, typically to prevent negative discussions. However, political trolling has become widespread using fake IDs on Facebook,[53] which has nearly four million users in Hungary as of early 2012.[54]

Facebook has grown increasingly popular in Hungary, especially after the 2010 parliamentary elections.[55] In 2011 and early 2012, many Facebook groups were formed, and several large demonstrations mobilizing tens of thousands of people both for[56] and against the government[57] were organized through Facebook[58] and disseminated on other social-

[47] Act CLXXXV of 2010, Art. 101, par. 4.
[48] "Daily average for December 2011," Medián webaudit, accessed January 30, 2012, http://webaudit.hu/.
[49] Borbála Tóth, "Minorities in the Hungarian media. Campaigns, projects and programmes for integration," Center for Independent Journalism, Budapest, 2011, p. 19.
[50] If a media outlet does not have a leaning to a political/ideological side, then it is apolitical, dedicated to human interest stories, crimes, and catastrophes.
[51] Tamás Bodoky, "Támad a civilmédia: minden ötödik Index-olvasó blogol" [The civil media is attacking: every fifth Index-reader is blogging], in Médiakutató (Media researcher), 2008 summer, http://www.mediakutato.hu/cikk/2008_02_nyar/06_civilmedia_index_blog/.
[52] To name a few: Mandiner.hu, Szuveren.hu, Velemenyvezer.blog.hu, K-monitor.hu, Atlatszo.hu, and the sites of Human Civil Liberties Union (Tasz.hu) and Eötvös Károly Institute (Ekint.org).
[53] Thomas Bauer, "Tükröt tartva a magyar valóságnak: trollok és familiárisok" [Holding a mirror to the Hungarian reality: trolls and familials], February 16, 2011, http://thomasbauer.b02.hu/blog/?p=397; "Baloldali trollok támadása" [Attack of left-wing trolls], Atvhamisit.blog.hu, January 11, 2012, http://atvhamisit.blog.hu/2012/01/11/btt; "Fantom trollok védik a Fidesz-kormányt Facebookon" [Phantom trolls protect the Fidesz government on Facebook], Piroslapok.blog.hu, January 21, 2011, http://piroslapok.blog.hu/2011/01/21/fantom_trollok_vedik_a_fidesz_kormanyt_facebookon.
[54] Socialbakers, "Hungary Facebook Statistics," accessed January 26, 2012, http://www.socialbakers.com/facebook-statistics/hungary.
[55] Walter Mayr, "Facebook generation fights Hungarian media law," Spiegel.de, January 4, 2011, http://www.spiegel.de/international/europe/0,1518,737455,00.html.
[56] "100,000 march in Hungary pro-government rally against EU criticism," Washington Post, January 21, 2012, http://159.226.12.170/pkmg/viewShot.do?type=record&id=000000003339dcce0135025aace71e02.
[57] "Hungarians protest against new Fidesz constitution," BBC, January 3, 2012, http://www.bbc.co.uk/news/world-europe-16387117.

networking sites. Protests for social issues were also organized,[59] and there was at least one unannounced protest organized partly via mobile phones.[60] However, the extent of mobile phone use in organizing protests is unknown.

VIOLATIONS OF USER RIGHTS

The Fundamental Law of Hungary—passed in April 2011 and effective as of January 1, 2012—acknowledges the right to freedom of expression and defends "freedom and diversity of the press,"[61] though, there are no laws that specifically protect online modes of expression. In January 2012, the European Commission launched infringement proceedings against Hungary, partly regarding the independence of the National Agency for Data Protection and the judiciary, which is threatened by the mandatory early retirement of judges over 62 years old (lowered from 70 years) and the concentration of Fidesz party members.[62]

The Civil Code recognizes civil rights and poses a ban on insulting an individual's honor.[63] Libel cases demonstrate that the courts generally protect freedom of expression, except when there is a conflict with another basic right. Defamation cases have decreased since a 1994 Constitutional Court decision, which claimed that a public figure's tolerance of criticism should be higher than an ordinary citizen's.[64] Nevertheless, Hungarian law does not distinguish between traditional and online media outlets in libel or defamation cases. The Criminal Code bans defamation, slander, the humiliation of national symbols (the anthem, flag, and coat of arms), the dissemination of totalitarian symbols (the swastika and red

[58] "LIVE BLOG: »Don't like the system? – Protest!« Demonstration; Budapest," Thecontrarianhungarian.wordpress.com(blog), October 23, 2011, https://thecontrarianhungarian.wordpress.com/2011/10/23/live-blog-dont-like-the-system-protest-demonstration-budapest/.

[59] "Civil sphere and grassroots protest in Hungary: December, 2011," Thecontrarianhungarian.wordpress.com (blog), January 2, 2012, http://thecontrarianhungarian.wordpress.com/2012/01/02/civil-sphere-and-grassroots-protests-in-hungary-december-2011/; "28 arrested in sit-in against criminalization of homelessness in Budapest, Hungary," Thecontrarianhungarian.wordpress.com (blog), November 13, 2011, http://thecontrarianhungarian.wordpress.com/2011/11/13/28-arrested-in-sit-in-against-criminalization-of-homelessness-in-budapest-hungary/.

[60] "December 16. 17:00-tól: köztérfoglalás!" [16 December from 5 p.m.: public space occupation!], Belvaros.blogspot.com (blog), December 16, 2011, http://belvaros.blogspot.com/2011/12/kozteruletfoglalas-8-keruleti-vig.html. The protest, organized against the criminalization of homelessness, was said to be successful, as the office established for the penalization of the homeless closed for that evening and none of the participants were taken into custody. "Köztérfoglalás beszámoló" [Public space occupation report], accessed January 30, 2012, http://kozterfoglalas.nfshost.com/thanks.php.

[61] The Fundamental Law of Hungary (25 April 2011) Art. VIII., 1–2, http://tasz.hu/files/tasz/imce/alternative_translation_of_the_draft_constituion.pdf.

[62] "European Commission launches accelerated infringement proceedings against Hungary," European Commission, January 17, 2012, http://ec.europa.eu/economy_finance/articles/governance/2012-01-18-hungary_en.htm.

[63] Act IV of 1959 on the Civil Code, Art. 75–85.

[64] Péter Bajomi-Lázár and Krisztina Kertész, "Media Self-Regulation Practices and Decriminalization of Defamation in Hungary," pp. 177–183, in *Freedom of Speech in South East Europe: Media Independence and Self-Regulation*, 2007, ed. Kashumov, Alexander (Sofia: Media Development Center pp. 162–193),

pentagram), the denial of the sins of national socialism or communism, and public scare-mongering through the media.[65]

The Criminal Code has been used "sporadically" in cases of defamation or slander.[66] The most recent incident occurred in 2008 when the Hungarian Supreme Court found a journalist guilty of libel for describing the famous Hungarian Tokaj wine as "shit" in an article published in both the print and online versions of a daily newspaper; the decision was reversed at the European Court of Human Rights in 2011.[67] Otherwise, no individual has been detained, prosecuted, or sanctioned by the law for disseminating or accessing information on political or social issues through ICTs.

Generally, users who wish to comment on a web article need to register with the website by providing an email address and nickname. The operator of a website might be asked to provide the commenter's internet protocol (IP) address, email or other data in case of an investigation.[68] The 2010 media laws "blurred the responsibility of the media outlet and the commenter."[69] Consequently, at least one website decided to disable the commenting option in 2011.[70] In July 2011, an inquiry was launched against the online version of the daily *Népszava* because of a comment that was considered offensive,[71] even though the Media Council has stated that comments are not subject to regulation.[72]

There are no restrictions on anonymous communication, and encryption software is freely available without government interference. Pretty Good Privacy (PGP), a data encryption program, is often used by investigative journalists.[73] Nevertheless, to sign a contract with the mobile phone company, users must provide personal data upon purchase of a SIM card.[74]

National security services can collect traffic data (such as caller and recipient phone numbers, SIM cards personal data, the geographic location of the two SIM cards, and the browsing data of certain IP addresses) from telecommunication systems and other data

[65] Act IV of 1978 on the Criminal Code, Art. 179, 180, 269/A, 269/B, 269/C, Art. 270, 270/A.
[66] Bajomi-Lázár and Kertész 2007, p. 179.
[67] "European Court of Human Rights acquits Hungarian journalist of libel," Politics.hu, July 20, 2011, http://www.politics.hu/20110720/european-court-of-human-rights-acquits-hungarian-journalist-of-libel/.
[68] Act XIX of 1998 on criminal proceedings, Art. 178/A, par. 1.
[69] Anonymous internet expert, email communication, February 7, 2012.
[70] "Ha eljön a hajnal, menni muszáj – búcsú a kommentektől" [We must leave when dawn is coming – farewell from comments], Velvet.hu, June 30, 2011, http://velvet.hu/trend/2011/06/30/ha_eljon_a_hajnal_menni_muszaj_-_bucsu_a_kommentektol/.
[71] "Kormánytag kezdeményezett eljárást lapunk ellen – egy komment miatt" [Member of government initiated an inquiry against us – because of a comment], Nepszava.hu, July 1, 2011, http://www.nepszava.hu/articles/article.php?id=445426.
[72] "A kommentekre nem vonatkozik a médiatörvény" [The media law does not concern comments], Index.hu, July 3, 2011, http://index.hu/belfold/2011/07/03/a_kommentekre_nem_vonatkozik_a_mediatorveny/.
[73] Borbála Toth, "Mapping Digital Media: Hungary," Open Society Foundations, February 2012, p. 50, http://www.opensocietyfoundations.org/reports/mapping-digital-media-hungary.
[74] Act C of 2003, On Electronic Communications, Art. 129, http://www.ictregulationtoolkit.org/en/Publication.2347.html.

storage devices without a warrant.[75] Further, the authorities have allegedly installed "black boxes" on ISP networks,[76] which allow them to access and record communication transmitted via ICTs, though a warrant is required.[77] Nevertheless, there is no data on the extent to which they monitor ICTs or how regularly they do it.

In accordance with the EU Directive 2006/24/EC on data retention, ISPs and mobile phone companies in Hungary need to retain user data for up to one year, including personal data, location, caller phone numbers, the duration of phone conversations, IP addresses, and user IDs for investigative authorities and security services.[78] There is no data on these activities even though there is a legal obligation to provide the European Commission with statistics of the queries for data made by the investigating authorities.[79] Cybercafes, on the other hand, are not required to collect user information, and anyone can access internet at a cybercafe without registration.

Bloggers, ICT users, websites or their property are not subject to extralegal intimidation or physical violence by state authorities or any other actors. However, in September 2011, photographers of the news portals, Index.hu and Origo.hu, were banned from parliament because they had allegedly taken pictures of the prime minister's notes.[80] In a separate incident in December 2011, journalists from Index.hu were banned from parliament for being disrespectful after they posted a video of two reporters singing and dancing in the building.[81] The journalists were permitted to enter parliament again roughly a month later. In January 2012, a photographer from Vagy.hu was not admitted to the public ball of Debrecen city because the organizers claimed that the local news site was not registered with the NMHH.[82] These types of incidents impede the ability of journalists to cover the news, compromising the Hungarian news and information landscape.

In response to Hungary's 2010 media laws, the international hacker group Anonymous posted a video on YouTube threatening the Hungarian government with a cyberattack in August 2011.[83] Since then, two sites were attacked by Anonymous via distributed denial-of-service (DDoS) attacks: the website of the National Board Against Counterfeiting in

[75] Act CXXV of 1995, On the National Security Services, Art. 54.
[76] "Hungary – Privacy Profile," Privacy International, January 22, 2011, https://www.privacyinternational.org/reports/hungary.
[77] Act CXXV of 1995, On the National Security Services, Art. 56.
[78] Act C of 2003, Art. 159/A; "Hungary – Privacy Profile," Privacy International, January 22, 2011.
[79] Act C of 2003, Art. 159/A, par. 7.
[80] "Photographers banned from Hungarian Parliament,"Thecontrarianhungarian.worldpress.com (blog), September 20, 2011, http://thecontrarianhungarian.wordpress.com/2011/09/20/photographers-banned-from-hungarian-parliament/.
[81] "Hungary's leading online news portal banned from parliament," Politics.hu, December 22, 2011, http://www.politics.hu/20111222/hungarys-leading-online-news-portal-banned-from-parliament/.
[82] Zsolt Kácsor, "Debrecen nem kért a TV2 és az RTL kameráiból" [Debrecen did not want the cameras of TV2 and RTL Klub], Nol.hu, January 16, 2012, http://nol.hu/lap/mo/20120116-csak_a_helyi_teve_tudosithatott_a_rekordkiserletrol.
[83] "The Anonymous message to Hungarian government,"YouTube, accessed January 30, 2012, http://www.youtube.com/watch?v=SStDZ5De1Og.

response to the debate surrounding the Anti-Counterfeiting Trade Agreement (ACTA) in early 2012, and the personal website of the Minister of State for Education in protest against a new education bill.[84]

[84] Máté Nyusztay, "'A rendszert támadjuk' – Magyarország is az Anonymous célkeresztjében" ['We attack the system' – Hungary is among the targets of Anonymous], Nol.hu, February 15, 2012, http://nol.hu/belfold/a_rendszert_tamadjuk__-_magyarorszag_is_az_anonymus_celkeresztjeben.

INDIA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	12	13
Limits on Content (0-35)	8	9
Violations of User Rights (0-40)	16	17
Total (0-100)	**36**	**39**

* 0=most free, 100=least free

POPULATION: 1.3 billion
INTERNET PENETRATION 2011: 10 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/I USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Although India's internet penetration rate of less than 10 percent is low by global standards, the country is nonetheless home to over 100 million users, placing it third behind only China and the United States as of early 2012.[1] In the past, instances of the central government and state officials seeking to control communication technologies and censor undesirable content were relatively rare and sporadic. However, since the November 2008 terrorist attacks in Mumbai, which killed 171 people, the need, desire, and ability of the Indian government to monitor, censor, and control the communication sector have grown.[2] Given the range of security threats facing the country, many Indians feel that the government should be allowed to monitor personal communications such as telephone calls, email messages, and financial transactions.[3] It is in this context that Parliament passed amendments to the Information Technology Act (ITA) in 2008, expanding censorship and monitoring capabilities. This trend continued in 2011 with the adoption of regulations increasing surveillance in cybercafes. Meanwhile, the government and non-state actors have intensified pressure on intermediaries, including social media applications, to remove upon request a wide range of content vaguely defined as "offensive" and potentially pre-screen

[1] Eric Ernest, "India To Be World's Third Largest Internet Market," PC World, November 8, 2011, http://www.pcworld.in/news/india-be-worlds-third-largest-internet-market-57792011.
[2] Joshua Keating, "The List: Look Who's Censoring the Internet Now," Foreign Policy, March 24, 2009, http://www.foreignpolicy.com/articles/2009/03/23/the_list_look_whos_censoring_the_internet_now.
[3] "Security Forces, Media, 2 Pillars of Freedom: Poll," Times of India, August 15, 2010, http://timesofindia.indiatimes.com/home/sunday-toi/special-report/Security-forces-media-2-pillars-of-freedom-Poll/articleshow/6312697.cms.

user-generated content. Despite new comprehensive data protection regulations adopted in 2011, the legal framework and oversight surrounding surveillance and interception remains weak, and several instances of abuse have emerged in recent years.

The spread of information and communication technologies (ICTs) began accelerating in India with the liberalization of the telecommunications sector as part of the New Economic Policy in July 1991.[4] Throughout the early 1990s, various aspects of the telecommunications industry were opened to the private sector, including radio paging and mobile phones.[5] The government's New Telecom Policy of 1999 and New Internet Policy of 1998 have further spurred the growth of the ICT sector,[6] resulting in a large number of manufacturing units and internet service providers (ISP) setting up bases in the country.

OBSTACLES TO ACCESS

Internet usage in India continues to increase, with tens of millions of new users getting online each year, though the penetration rate remains low by global standards. Infrastructural limitations and cost considerations restrict access to the internet, especially to high-speed broadband connections. According to the International Telecommunications Union (ITU), internet penetration was 10 percent—or about 120 million people—at the end of 2011.[7] Among internet users, 90 million were "active," accessing it at least once a month (70 million urban and 20 million rural).[8]

Many of India's users access the internet via cybercafes, as only 3 percent of households had an internet connection, according to recent census data.[9] The share of urbanite users with home connections has been constantly increasing and about 20 percent of urban households

[4] Invest India Telecom, "Indian Telecom Sector," Ministry of Communications and Information Technology–Department of Telecommunications, accessed January 3, 2011, http://www.dot.gov.in/osp/Brochure/Brochure.htm.
[5] Ibid.
[6] Telecom Regulatory Authority of India, "New Telecom Policy 1999," accessed January 3, 2011, http://www.trai.gov.in/TelecomPolicy_ntp99.asp; Peter Wolcott, "The Provision of Internet Services in India," in *Information Systems in Developing Countries: Theory and Practice*, ed. R. M. Davison and others (Hong Kong: University of Hong Kong Press, 2005), http://mosaic.unomaha.edu/India_2005.pdf.
[7] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[8] The Internet and Mobile Association of India (IAMAI) similarly reported that by September 2011 about 112 million Indians (9 percent of the population) had used the internet at least once in their lifetimes, and estimated this number would climb to 120 million by year's end. This was an increase from 77 million in 2010. See, IAMAI, "Report on Internet in India (I-Cube) 2011," 2011, http://www.iamai.in/Upload/Research/11720111091101/icube_3nov11_56.pdf.
[9] Hari Kumar, "In Indian Homes, Phones and Electricity on Rise but Sanitation and Internet Lagging," India Ink (blog), New York Times, March 14, 2012, http://india.blogs.nytimes.com/2012/03/14/in-indian-homes-phones-electricity-on-rise-but-sanitation-internet-lagging/.

possessed a computer in early 2012,[10] but there remains a pronounced urban-rural divide. Approximately 24 million rural residents used the internet in 2011, a rise from past years, but still only a tiny fraction of the total rural population of 800 million.[11] While cost is an obstacle, surveys indicate that lack of electricity, low computer literacy, and limited awareness of the internet are more significant.[12] Low literacy rates, particularly in English, are also a major impediment. The availability of internet content in India's eight most widely spoken languages is growing, but remains poor. After the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) approved the use of domain names in Hindi, Bengali, Punjabi, Urdu, Tamil, Telugu, and Gujarati,[13] the Indian government was preparing to roll out Hindi domain names in mid-2012, with other local language to follow.[14] U.S.-based software and internet giants Microsoft, Google, and Yahoo have launched initiatives to incorporate Indian languages into their programs and services.[15]

Broadband penetration is limited and slow. According to the Telecom Regulatory Authority of India (TRAI), as of December 2011 there were only 13.3 million broadband subscriptions in the country, most of them via ADSL rather than fiber-optic cable, contributing to lower speeds.[16] Testing by the technology firm Akamai in November 2011 indicated that the average connection speed in India was only 844 Kbps, an improvement from early 2011 but still low by international standards.[17]

The government and private companies are working to expand India's broadband infrastructure. According to a new telecom policy released in October 2011, the government plans to increase the number of broadband users to 175 million by 2017. One way they plan to achieve this is by pressuring cable television operators to shift from analog to digital services, so they can offer broadband internet via the same connections as cable TV

[10] Ibid.
[11] IAMAI, "Report on Internet in India (I-Cube) 2011."
[12] IAMAI, "84% of Rural India Not Aware of Internet," news release, September 13, 2010, http://www.iamai.in/PRelease_Detail.aspx?nid=2159&NMonth=9&NYear=2010.
[13] Surabhi Agarwal and Shauvik Ghosh, "Domain Names in Regional Languages Soon," Livemint.com, August 17, 2010, http://www.livemint.com/2010/08/17220818/Domain-names-in-regional-langu.html#.
[14] Surabhi Agarwal, "Hindi domain name to bridge digital divide," Livemint.com, November 4, 2011, http://www.livemint.com/2011/11/04005330/Hindi-domain-name-to-bridge-di.html.
[15] Ishani Duttagupta and Ravi Teja Sharma, "Google, Microsoft Focus on Regional Languages," Economic Times, August 2, 2010, http://economictimes.indiatimes.com/infotech/internet/Google-Microsoft-focus-on-regional-languages/articleshow/6242139.cms; Suw Charman-Anderson, "Yahoo India expands into five more Indian languages," Firstpost Technology, February 3, 2012, http://www.firstpost.com/tech/yahoo-india-expands-into-five-more-indian-languages-203034.html.
[16] Leslie D'Monte and Deepti Chaudhary, "Broadband user base still has a long way to go," Livemint.com, November 14, 2011, http://www.livemint.com/2011/11/14204650/Broadband-user-base-still-has.html?h=B; "Broadband Users at 13.3M; 3.4M Mobile Users Switch Cellular Operator in Dec," TechCircle.in, January 31, 2012, http://techcircle.vccircle.com/500/broadband-users-at-13-3m-3-4m-mobile-users-switch-cellular-operator-in-dec/.
[17] "Average connection speed in India stands at 844 kbps," Ciol.com, November 17, 2011, http://www.ciol.com/Technology/Networking/News-Reports/Average-connection-speed-in-India-stands-at-844-kbps/156663/0/.

subscriptions.[18] Plans to expand the country's international bandwidth may also yield increased speeds and lower prices.[19]

India's overall mobile phone penetration figures continue to grow at fast speeds, and an increasing number of Indians are also getting online via mobile devices. According to the TRAI and ITU, the total mobile phone subscriber base was 890 million by the end of 2011, including about 300 million in rural areas, an increase of 160 million subscribers compared to 2010.[20] Access to the internet through mobile phones has risen as well, apparently due to a series of inexpensive rate plans introduced in early 2010 and the long-awaited rollout of 3G services in early 2011 after years of bureaucratic delays.[21] According to the Internet and Mobile Association of India (IAMAI), of the 70 million active urban internet users, 26.3 million had access via their mobile devices in late 2011.[22] In March 2012, the government announced plans to allocate frequencies for a 4G network, which will further facilitate mobile web use.[23]

There were no reports of government-imposed internet connectivity disruptions in 2011 and 2012. However, in January 2012, mobile phone providers in Jammu and Kashmir shut off their services for one day as part of security precautions in place for Republic Day, reportedly due to fears that mobile phones could be used by terrorists to remotely detonate bombs.[24]

Three major operators sell international internet bandwidth at the wholesale level: Tata Group's VSNL, Bharti Airtel, and Reliance Globalcom. Since the deregulation of the telecommunications sector in the late 1990s, users in India have been able to choose among hundreds of different public and private service providers. BSNL and MTNL, both state owned, are the two largest ISPs, with a combined 70 percent of subscribers.[25] They retain a dominance established before the appearance of private competitors that each control under

[18] Bruce Einhorn, "India Seeks Access to the Broadband Highway," Bloomberg Businessweek, November 21, 2011, http://www.businessweek.com/magazine/india-seeks-access-to-the-broadband-highway-11172011.html.
[19] Rohin Dharmakumar, "The Long Arm of Broadband," Forbes India, February 5, 2010, http://business.in.com/article/breakpoint/the-long-arm-of-broadband/9592/1.
[20] "Broadband Users at 13.3M; 3.4M Mobile Users Switch Cellular Operator in Dec," TechCircle.in
[21] Bruce Einhorn, "After Years of Delays, India Finally Gets 3G," Bloomberg Businessweek, February 17, 2011, http://www.businessweek.com/magazine/content/11_09/b4217042858674.htm.
[22] IAMAI, "Report on Internet in India (I-Cube) 2011."
[23] "4G services: Govt to allocate airwaves in 700 MHz band," The Times of India, March 6, 2012, http://timesofindia.indiatimes.com/tech/news/telecom/4G-services-Govt-to-allocate-airwaves-in-700-MHz-band/articleshow/12159694.cms.
[24] "Republic Day: Mobile phone blackout in Kashmir," The Economic Times, January 26, 2012, http://economictimes.indiatimes.com/news/politics/nation/republic-day-mobile-phone-blackout-in-kashmir/articleshow/11637307.cms.
[25] TRAI, *The Indian Telecom Services Performance Indicators: January–March 2010* (New Delhi: TRAI, July 2010), http://www.trai.gov.in/WriteReadData/trai/upload/Reports/51/finalperformanceindicatorReport9agust.pdf.

10 percent of the market.[26] Few of the 104 service providers authorized to offer broadband have been able to penetrate the market given the strong position occupied by BSNL and MTNL.[27] However, both companies have been forced to offer lower rates to stave off the private ISPs.

Private companies have met with more success in the mobile phone service market. The top 10 providers are Bharti Airtel, BSNL, Vodafone Essar, Reliance Communications, Idea Cellular, Tata Communications, Tata Teleservices, Aircel, MTNL, and Tata Teleservices (Maharashtra) Limited (TTML).[28] Licenses are issued following a bidding process, but launching a mobile phone service business in practice requires considerable financial clout and access to important government officials. In a decision highlighting such tendencies and other corrupt practices in the telecommunications sector, the Supreme Court in February 2012 canceled 122 licenses for 2G mobile phone services. The licenses had been sold at artificially low prices in 2008 to a small number of favored firms.[29]

The TRAI is the main regulatory body for telecommunications matters, with authority over ISPs and mobile phone service providers. It functions as an independent agency, offering public consultations and other participatory decision-making processes. The TRAI is generally perceived as fair, though its reputation was tarnished by the above Supreme Court decision. The Ministry of Communications and Information Technology (MCIT) and the MHA also exercise control over several aspects of internet regulation, and interventions by the MHA in particular carry considerable weight. There have been no publicized disputes between the ministries and the TRAI to date.[30]

Although opening a cybercafe was relatively simple in the past, the authorities have complicated the process in recent years. Obtaining a license now requires approval from as many as six different agencies. New regulations passed in April 2011 require cybercafes to engage in more censorship, monitoring, and data storage (see details below), placing an additional burden on owners. These difficulties, combined with increases in home and mobile internet connections, have dimmed prospects for new entrants to the cybercafe market.

[26] Ibid.
[27] Nivedita Mookerji, "Stage Set for New Broadband Policy," Daily News & Analysis (DNA), June 11, 2010, http://www.dnaindia.com/money/report_stage-set-for-new-broadband-policy_1394639.
[28] "10 Top Telecom Service Providers in India," Rediff.com, August 9, 2010, http://business.rediff.com/slide-show/2010/aug/09/slide-show-1-10-top-telcos-in-india.htm#contentTop.
[29] Vikas Bajaj, "Indian Court Cancels Contentious Wireless Licenses," New York Times, February 2, 2012, http://www.nytimes.com/2012/02/03/business/global/india-supreme-court-cancels-2g-licenses.html?_r=1&ref=asia.
[30] B. Raman, "The Internal Security Czar," Outlook, December 24, 2009, http://www.outlookindia.com/article.aspx?263528.

LIMITS ON CONTENT

As of early 2012, the Indian authorities blocked a small number of websites, including some with content in the public interest. More prevalent has been administrative censorship and requests for removal of content by both government and private actors. Such removals increased after passage of new regulations governing intermediary responsibilities in April 2011. Meanwhile, public debate intensified over the balance between free speech and protection of communities' religious sensibilities amidst a series of civil lawsuits—and at least one criminal case—against social media websites seeking to hold them responsible for content posted by users that some Indians found offensive.

Since 2003, the institutional structure of internet censorship and filtering has centered on the Indian Computer Emergency Response Team (CERT-IN), a body created in 2003 within the MCIT's Department of Information Technology (DIT). CERT-IN serves as a nodal agency for accepting and reviewing requests from a designated pool of government officials to block access to specific websites. When it decides to block a site, it directs the Department of Telecommunications—also part of the MCIT—to order all licensed Indian ISPs to comply with the decision.

In tests conducted in 2010 on four ISPs, the OpenNet Initiative (ONI) found selective, but consistent filtering of various extremist sites, as well as "websites with information on human rights in India, Internet tools such as proxies, and content related to free expression." The ISPs used DNS tampering[31] as their method of filtering, enabling targeted blocking of individual blogs, for instance, rather than an entire hosting service.[32] In April 2011, the Center for Internet and Society obtained a list of 11 banned websites from the DIT in response to a freedom of information request. All of the blocks were apparently implemented after a judicial order from a low-level court. For most of the websites, users encountered a technical error alert rather than a message explaining that inaccessibility was due to a court decision or government request.[33] Among the websites on the list were two related to the grassroots news organization Indymedia, a Facebook group called "I Hate Ambedkar" (a reference to B.R Ambedkar, one of the drafters of independent India's constitution), and Zone-H, an Italian security company serving as a repository for hacked

[31] According to ONI, "DNS tampering is the practice of preventing nameservers from returning the actual website requested by the user, and instead either showing an error page or explaining that it is blocked." See, Kendra Albert, "DNS Tampering and the ICANN gTLD Rules," OpenNet Initiative, June 23, 2011, http://opennet.net/blog/2011/06/dns-tampering-and-new-icann-gtld-rules.

[32] "India," OpenNet Initiative, December 2011, http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-india.pdf.

[33] Pranesh Prakash, "DIT's Response to RTI on Website Blocking," Center for Internet & Society, April 7, 2011, http://cis-india.org/internet-governance/blog/rti-response-dit-blocking.

websites.[34] Also blocked was an article on Bloggernews.net reporting about the Zone-H case.[35] Freedom House tests conducted in April 2012 indicated that the pages were still inaccessible from at least one major ISP. Regulations passed in April 2011 require cybercafes to equip computers with filtering software that blocks access to pornography or other "obscene information," though enforcement has reportedly been lax.[36]

Advanced web applications like the video-sharing site YouTube, the social-networking site Facebook, or the Twitter microblogging platform are freely available and becoming increasingly important in India. As of February 2012, Facebook was the third most popular site in the country, followed by YouTube at fourth, and Twitter at eleventh. In a dramatic drop, the social-networking site Orkut slipped from eighth to 37th.[37] With about 45 million Facebook users as of May 2012, India had the third largest subscriber base in the world, surpassed only by the United States and Brazil.[38]

In a bizarre incident in early 2011, some ISPs appeared to be blocking the websites of several smaller applications—including Typepad.com (a blog-publishing platform), Mobango.com (a mobile applications website), and ClickATell.com (a service for sending out bulk text-messages). Beginning on February 27, internet users reported being unable to access these websites, in some instances receiving a message stating, "This site has been blocked per request from the Department of Telecom."[39] Following a public outcry, Typepad was available again by the first week of March, though the other two sites remained inaccessible as of May 2012. The cause for the block remained unclear, as the Department of Telecom denied ordering it but did not provide any further explanation for the disruption.[40]

[34] The blocking of the latter emerged after a New Delhi court ordered CERT-IN to restrict access to Zone-H as part of a dispute with Indian security firm E2 Labs. Zone-H accused E2 Labs of inappropriately using its logo and E2 Labs responded by suing Zone-H for defamation. Zone-H claimed that it had not received sufficient notification to defend itself in court. See, Ketan Tanna, "Virtual Democracy?" Infochange Agenda, July 2011, http://infochangeindia.org/agenda/the-limits-of-freedom/virtual-democracy.html; Rahul Bhatia, "India Should Watch Its Internet Watchmen," Wall Street Journal, March 28, 2011, http://online.wsj.com/article/SB10001424052748704396904576226460167553174.html.

[35] Simon Barrett, "Blogger News Censored in India," Blogger News Network, July 12, 2012, http://www.bloggernews.net/124890; "Is E2 labs right in getting zone-h.org blocked?" Blogger News Network, March 12, 2012, http://www.bloggernews.net/124029.

[36] Aparna Viswanathan, "Big Brother is looking over your shoulders," The Hindu, October 13, 2011, http://www.thehindu.com/opinion/lead/article2532036.ece?homepage=true.

[37] "Top Sites in India," Alexa.com, accessed February 1, 2012, http://www.alexa.com/topsites/countries;0/IN.

[38] "India Facebook Statistics," Socialbakers.com, accessed May 1, 2012, http://www.socialbakers.com/facebook-statistics/india.

[39] Nikhill Pahwa, "Updatde: Indian Government Blocks Typepad, Mobango, Clickatell; Screenshots," Medianama.com, March 4, 2011, http://www.medianama.com/2011/03/223-indian-government-blocks-typepad-mobango-clickatell/.

[40] The claim was made in a response to a freedom of information request from civil society groups. Nikhill Pahwa, "#IndiaBlocks: India's IT Dept's Response To RTI Requests On Internet Blocking," Medianama.com, April 7, 2011, www.medianama.com/2011/04/223-indiablocks-indias-it-depts-response-to-our-rti-request-our-stand/; Pranesh Prakesh, "RTI Applications on Blocking of Websites," Center for Internet & Society, March 9, 2011, http://www.cis-india.org/internet-governance/blog/rtis-on-website-blocking; Priscilla Jebaraj, "Telecom Department orders ban on blog hosting site?" the Hindu, March 5, 2011, http://www.hindu.com/2011/03/05/stories/2011030564792200.htm; Rahul Bhatia, "India Should Watch Its Internet Watchmen."

More common than website blocking is the removal of content based on judicial orders, government directives, and citizen complaints. This phenomenon that has increased in recent years and in some cases, targeted content on political, social, and religious topics. Google's "Transparency Report" showed that the Indian authorities had submitted 68 removal requests covering 358 items between January and June 2011. According to Google, 255 items related to what it categorized as "Government Criticism," while 39 involved defamation and 8 pertained to hate speech. Google reportedly declined many of the requests, including one from "a local law enforcement agency to remove 236 communities and profiles from Orkut that were critical of a local politician," but in some cases it did restrict local access to "videos that appeared to violate local laws prohibiting speech that could incite enmity between communities."[41]

Bloggers are rarely forced by the government to take down their writings. However, in December 2011, the website "Cartoons against Corruption"[42] run by artist Asseem Trivedi was suspended by its hosting company after a lawyer filed a complaint to the Mumbai police that the site contained cartoons that "ridicule the Indian Parliament, the national emblem and the national flag."[43] Trivedi subsequently opened a blog on Google's Blogger platform where he reposted the cartoons.[44]

In April 2011, the government instituted Information Technology (Intermediary Guidelines) Rules, which require intermediaries—including search engines and social-networking sites—to remove content within 36 hours if an individual complains that it is offensive. The list of potentially offensive content is both wide-ranging and vague. It includes information that is "disparaging," "harmful," "blasphemous," "pornographic," "encourages gambling," "infringes proprietary rights," or "threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign states or public order."[45] Under the 2008 ITA, intermediaries in India are protected from prosecution for content posted by third parties, but according to the 2011 rules, they risk losing such immunity if they do not remove the offensive content within 36 hours of notification. Meanwhile, the rules do not provide an avenue for content producers to be informed of the removal or to contest the

[41] Google, "India," Google Transparency Report, accessed September 19, 2012, http://www.google.com/transparencyreport/governmentrequests/IN/.
[42] Original link: www.cartoonsagainstcorruption.com [site discontinued].
[43] Preetika Rana, "Cartoonist Faces Ban on Right to Poke Fun," India Real Time (blog), Wall Street Journal, January 4, 2012, http://blogs.wsj.com/indiarealtime/2012/01/04/cartoonist-faces-ban-on-right-to-poke-fun/?KEYWORDS=aseem+trivedi.
[44] "Ban on Website" [in Hindi], Cartoons Against Corruption (blog), accessed September 19, 2012, http://www.cartoonsagainstcorruption.blogspot.com/p/ban-on-website.html.
[45] "Information Technology Act, 2000," Ministry of Communications and Information Technology, April 11, 2011, p.12, http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf.

decision.[46] In March 2012, a cyberlaw expert in Kerala submitted a court petition challenging the constitutionality of the new regulations, specifically emphasizing the lack of transparency in the censorship process, even relative to more politically repressive countries like Saudi Arabia.[47]

In December 2011, Kapil Sibal, the Minister of Communications and Information Technology, introduced to the upper house of parliament controversial amendments to the Copyright Act, which critics complain would require internet companies to remove content flagged by other users as an infringement with little additional investigation.[48] The bill was pending at year's end and appeared unlikely to pass.

While most observers acknowledge that incendiary online content could pose a real risk of violence, particularly given India's history of periodic communal strife, press freedom and civil liberties advocates have raised concerns over the far-reaching scope of the ITA and the 2011 rules, their potential chilling effect, and the possibility that the authorities could abuse it to suppress political speech.[49] In December 2011, the Center for Internet and Society revealed the results of testing it conducted of intermediaries' responses to user requests to remove supposed "offensive" material.[50] The study found that rather than closely examining take down notice requests, intermediaries were erring on the side of caution and often over-complying.[51] This over-compliance was either due to their lacking the human resources to closely assess each complaint or fears of the legal and financial consequences of not removing remove material that might later be found to have been "offensive."

In late 2011, pressure was growing from some officials to take intermediary censorship to another level, such as requiring social networking sites to pre-screen user-generated content

[46] Vikas Bajaj, "India Puts Tight Leash on Internet Free Speech," New York Times, April 27, 2011, http://www.nytimes.com/2011/04/28/technology/28internet.html?_r=2&scp=1&sq=vikas%20bajaj%20Internet%20india&st=cse.

[47] Prachi Shrivastava, "Read parts of first writ challenging censorious IT Act Intermediaries Rules in Kerala," Legally India, March 6, 2012, http://www.legallyindia.com/201203062622/Bar-Bench-Litigation/read-first-writ-challenging-censorious-it-act-intermediaries-rules-in-kerala.

[48] "Kapil Sibal introduces Copyright Bill, Education Bills likely to suffer," The Economic Times, December 21, 2011, http://articles.economictimes.indiatimes.com/2011-12-21/news/30542786_1_education-bills-controversial-bills-copyright-bill; Pranesh Prakesh, "Invisible Censorship: How the Government Censors Without Being Seen," Center for Internet & Society, December 15, 2011, http://cis-india.org/internet-governance/invisible-censorship.

[49] Amol Sharma and Jessica E. Vascellaro, "Google and India Test the Limits of Liberty," Wall Street Journal, January 4, 2010, http://online.wsj.com/article/SB126239086161213013.html.

[50] For example, in six of the seven test cases, the intermediary removed the requested content and in several instances, more than what was asked for. See, Heather Timmons, "'Chilling' Impact of India's April Internet Rules," India Ink (blog), New York Times, http://india.blogs.nytimes.com/2011/12/07/chilling-impact-of-indias-april-internet-rules/; Pallavi Polanki, "How 'private-censorship' is making online content disappear, quietly," First Post India, December 15, 2011, http://www.firstpost.com/india/how-private-c ensorship-is-making-online-content-disappear-quietly-156545.html.

[51] Rishabh Dara, "Intermediary Liability in India: Chilling Effects on Free Expression on the Internet 2011," Center for Internet & Society, April 2012. http://cis-india.org/internet-governance/chilling-effects-on-free-expression-on-internet/intermediary-liability-in-india.pdf.

for potentially offensive information. Beginning in September 2011, Sibal, the Minister of Communications and Information Technology, held a series of meetings with leading internet companies, urging them to develop a voluntary code of conduct for removing content deemed offensive. Among the content of particular concern to the minister were reportedly webpages considered insulting to Prime Minister Monmohan Singh, ruling Congress party leader Sonia Gandhi, and religious leaders. The firms resisted, explaining that content which is legal and does not violate their policies will not be removed, even if it is considered controversial by some, and that a massive pre-screening process would be virtually impossible to implement. In December, Sibal suggested publicly that the government require internet companies to pre-screen and delete such content. The announcement sparked a flood of criticism from Indian media outlets, bloggers, internet experts, and civil society, many of whom questioned whether such a system would be constitutional.[52] In the face of the public outcry, no formal rules were introduced.

Nevertheless, the following month, the government sanctioned pursuit of a criminal case against 21 foreign internet firms including Facebook, Microsoft, Google, and Yahoo, accusing them of negligence for not removing offensive content. The case was initiated in December 2011 by a private citizen, journalist Vinay Rai, after he found content on their websites—including disrespectful images of the Prophet Mohammed or Hindu gods—and felt they offended Indians' religious sensibilities. If found liable, the defendants could face jail time or high fines. The government has drawn criticism for approving the prosecution although Rai had not first notified the companies, the process outlined under the 2008 ITA.[53] Google subsequently reported back to the court that it had removed the content in question from its search results, YouTube and Orkut social-networking site.[54] The case was still proceeding as of May 1, 2012.[55]

[52] John Ribeiro, "India May Overstep Its Own Laws in Demanding Content Filtering," PCWorld, December 5, 2011, http://www.pcworld.com/businesscenter/article/245548/india_may_overstep_its_own_laws_in_demanding_content_filtering.html.

[53] In January 2012, the internet firms lodged their own petition before the Delhi High Court asking it to quash the case. Meanwhile, the presiding judge told the companies to "develop a mechanism to check and remove offensive and objectionable material from their web pages," while warning that "Otherwise, like China, we may pass orders banning all such websites." In March 2012, the judge quashed the complaint against Yahoo and Microsoft, as they do not host user-generated content in the same manner. See, Amol Sharma, "Facebook, Google to Stand Trial in India," Wall Street Journal, March 13, 2012, http://online.wsj.com/article/SB10001424052702304537904577277263704300998.html; Andrew MacAskill and Pratap Patnaik, "Google, Facebook Seek Halt to Prosecution as India Objects to Some Content," Bloomberg, January 16, 2012, http://www.bloomberg.com/news/2012-01-16/google-facebook-seek-halt-to-case-as-india-objects-to-content.html; "Indian Court Threatens to Block Google and Facebook," Huffington Post, January 13, 2012, http://www.huffingtonpost.co.uk/2012/01/13/indian-court-threatens-to-block-google-and-facebook_n_1204005.html.

[54] Pratap Patnaik and Bibhudatta Pradhan, "Indian Court Quashes Charges Against Microsoft on Content," Bloomberg, March 19, 2012, http://www.bloomberg.com/news/2012-03-19/indian-court-quashes-charges-against-microsoft-in-content-case.html.

[55] Amol Sharma, "India Court Postpones Google, Facebook Censorship Hearing," Wall Street Journal, January 19, 2012, http://online.wsj.com/article/SB10001424052970204301404577170372338107512.html?mod=googlenews_wsj.

Internet companies have also faced several civil lawsuits over content deemed religiously offensive or defamatory. One high-profile case initiated by a Muslim cleric in December 2011 also targeted over 20 internet firms, including foreign social-networking sites.[56] Other cases lodged around the country focused on individual companies.[57] Taken together, the large number of suits, their continuation even after the offending content had been removed, and the apparent disregard for procedures outlined in the 2008 law have sent a chill through the IT sector. The cases have increased fears among IT firms large and small that they are vulnerable to frivolous legal action and could be held liable for not removing content posted by users even without receiving notification.[58]

Online discourse in India is vibrant, but online journalists and bloggers approach certain topics with caution. These include religion, communalism, the corporate-government nexus, links between government and organized crime, Kashmiri separatism, and hostile rhetoric from Pakistan. Such topics are addressed by online writers, but handled carefully to avoid inciting violence, particularly by non-state actors.

The Indian blogosphere is quite active and eloquent, complementing the rise in internet use by different interest groups and civil society actors, though the actual number of bloggers remains relatively small. A growing number of crowd-sourcing initiatives are being used to improve governance or counter societal harassment. Programs, often organized by non-governmental organizations, that enable reporting via text-message or online are tracking villagers' complaints, trash pick-up, bribery allegations, and incidents of sexual harassment.[59]

---

[56] Anuradha Shetty, "Google India, 7 others dropped from objectionable content lawsuit," Tech2, April 13, 2012, http://tech2.in.com/news/social-networking/google-india-7-others-dropped-from-objectionable-content-lawsuit/298102; "Court accepts Yahoo plea, fines complainant," Sify Finance, March 5, 2012, http://www.sify.com/finance/court-accepts-yahoo-plea-fines-complainant-news-national-mdfuEqaabbh.html?ref=false; "Google removes offensive content, Facebook says it doesn't control, operate servers," The Times of India, February 7, 2012, http://timesofindia.indiatimes.com/tech/news/internet/Google-removes-offensive-content-Facebook-says-it-doesnt-control-operate-servers/articleshow/11785178.cms; "Facebook India to court: Not responsible for user-generated content," The Times of India, February 29, 2012, http://timesofindia.indiatimes.com/tech/news/internet/Facebook-India-to-court-Not-responsible-for-user-generated-content/articleshow/12080208.cms.

[57] For example, in December 2011, an activist from Lucknow in Uttar Pradesh lodged a complaint against Facebook for posting comments that spread hatred against the sacred Hindu scripture Bhagavad Gita. Meanwhile, Google was facing a defamation case reportedly filed by an asbestos-manufacturing firm in Andhra Pradesh. See, "FIR against Facebook, user for anti-Gita comments," Daily Bhaskar, December 25, 2011, http://daily.bhaskar.com/article/UP-case-against-facebook-user-for-anti-gita-comments-2675251.html; Amol Sharma, "Google-Facebook Hearing Is Delayed in India," Wall Street Journal, May 3, 2012, http://online.wsj.com/article/SB10001424052702304743704577381790489739930.html. In January 2012, Facebook was forced to delete some allegedly defamatory content posted against Star News on a forum called "Fight against corruption in media."

[58] Amol Sharma, "Is India Ignoring its own Internet Protections?" India Real Time (blog) Wall Street Journal, January 16, 2012, http://blogs.wsj.com/indiarealtime/2012/01/16/is-india-ignoring-its-own-internet-protections/.

[59] Rama Lakshimi, "Indians use cellphones to plug holes in governance," Washington post, October 28, 2011, http://www.washingtonpost.com/world/asia-pacific/indians-use-cellphones-to-plug-holes-in-governance/2011/10/24/gIQAooAmOM_story.html.

The year 2011 also saw the emergence of a mass anti-corruption movement revolving around 76-year-old activist Anna Hazare, and propelled in large part by online media. As Hazare began a "fast to the death" in April 2011 to pressure the government to enact legislation that would create an effective, autonomous anti-corruption agency, news and support of his demands traveled quickly. Within days, his name became the most searched term on India's Google search engine, was trending on Twitter, and his Facebook page garnered 70,000 fans.[60] The movement grew to include dozens of protests and rallies across India. After ending his fast in August, Hazare turned to online media to directly communicate with his fans, launching a personal blog the following month with the help of aides, who say some posts have received over one million hits.[61] Although no new legislation had been passed as of May 2012, the government had promised to explore options.

VIOLATIONS OF USER RIGHTS

The Indian constitution, particularly Article 19, protects freedom of speech and expression.[62] Along with the right to life and liberty under Article 21, Article 19(1) (a) has also been held to apply to the privacy of telephone conversations. Established guidelines regulate the ability of state officials to intercept communications,[63] but India lacks an appropriate legal framework and procedures to ensure proper oversight of intelligence agencies' growing surveillance and interception capabilities, opening the possibility of misuse and unconstitutional invasion of citizens' privacy.

ICT usage is governed primarily by the Telegraph Act, the penal code, the code of criminal procedure, and the ITA. The 2008 amendments to the ITA, which took effect in October 2009,[64] raised fears about an expansion of state surveillance capacity, including interception of email and mobile phone text messages. Several provisions of the revised law entail possible restrictions on users' rights, including classifying a broader scope of activities as criminal offenses.

Internet users in India have sporadically faced prosecution for online postings. In 2009, the Supreme Court ruled that both bloggers and moderators can face libel suits and even

[60] Samyuktha Krishnappa, "Social media support pours in for anti-corruption crusader Hazare in India," April 8, 2011, http://www.ibtimes.com/articles/132110/20110408/anna-hazare-fast-corruption-photos-video-social-media-internet-facebook-twitter-youtube.htm.
[61] Atikh Rashid, "Anna is new kid on the blog, and he is loving it," Express India, October 24, 2011, http://www.expressindia.com/story_print.php?storyId=864395.
[62] Government of India, "The Constitution of India," As modified up to the 1st December, 2007, http://lawmin.nic.in/coi/coiason29july08.pdf.
[63] *PUCL v. Union of India* (1997) 1 SCC 301. See also Vikram Raghavan, *Communications Law in India* (London: LexisNexis Butterworths, 2007), 760–761.
[64] The amended act is available at http://www.naavi.org/ita_2008/ch1_2008.htm, accessed September 19, 2012.

criminal prosecution for comments posted by other users on their websites. In April 2012, a professor at a university in West Bengal and several others were arrested for circulating a caricature via email and Facebook that mocked a number of government officials, including the railway minister.[65] They were charged under the ITA and criminal defamation provisions of the penal code, but released on bail.[66] In a troubling sign, at least two other ministers told media they supported the police action. No other high-profile arrests for online offenses were reported in 2011 or early 2012.

The overall level of ICT surveillance in India remains unclear, though it is believed to have grown in scale and sophistication since the Mumbai terrorist attacks in 2008. A series of scandals and new measures in recent years have exacerbated concerns over the lack of a legal framework or parliamentary oversight to regulate such activities. Private companies hosting content—including ISPs, cybercafes, and mobile phone operators—are obliged by law to hand over user information to the authorities. Prior judicial approval for communications interception is not required under either the Telegraph Act or the ITA, and the revised ITA grants both central and state governments the power to issue directives on interception, monitoring, and decryption.[67] Regulations passed in April 2011 increased monitoring requirements in cybercafes, requiring owners to obtain a copy of each user's photo ID and retain that record, as well as logs of all websites visited by the user, for one year.[68] The rules also contain specifications for the venue's layout, including placing limits on the height of cubicle partitions and requiring that certain monitors face the central area of the cybercafe.[69] Mobile phone operators are permitted to activate SIM cards only after users register their personal details with the carrier.

In January 2012, responding to a freedom of information request, the Home Ministry reported that the Central government orders 7,500 to 9,000 phone interceptions per

[65] "Professor arrested for poking fun at Mamata," Hindustan Times, April 13, 2012, http://www.hindustantimes.com/India-news/WestBengal/Professor-arrested-for-poking-fun-at-Mamata/Article1-839847.aspx.

[66] They were charged under Article 66 of the ITA, which appears to punish hacking offenses not online expression. See, Soudhriti Bhabani, "Professor held for uploading caricature of Mamata on social site," Daily Mail, April 13, 2012, http://www.dailymail.co.uk/indiahome/indianews/article-2129588/Professor-held-uploading-caricature-Mamata-social-site.html#ixzz246uKzJSf.

[67] The ITA's Section 69 expands the circumstances under which communications may be monitored, intercepted, and decrypted. Section 69B, for instance, allows the central government to collect traffic data from any computer source without a warrant, whether the data are in transit or in storage. See, "Yes, Snooping's Allowed," Indian Express, February 6, 2009, http://www.indi.anexpress.com/news/yes-snoopings-allowed/419978/0.

[68] Regulation reads: "When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorized for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance."

[69] "Information Technology Act, 2000," Ministry of Communications and Information Technology, April 11, 2011, http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf.

month.[70] Such activities have not been without controversy. Throughout 2011, media reports relayed accusations of intelligence and law enforcement agencies liberally engaging in phone and data interceptions, and in one case, two senior Mumbai police officers were found to have abused their ability to obtain user data in order to make a profit.[71]

Several court cases also highlighted both the government's and service providers' occasional sloppiness in handling requests for user information. Yahoo filed a case after the Controller of Certifying Authorities (CCA) had imposed a fine of 1.1 million Rupees (about US$22,000) when the company refused to hand over information related to about a dozen Yahoo IDs and IP addresses that the government said it suspected were being used by Islamic terrorists or Maoists. Yahoo refused the request, claiming it was not made through the channels required by law and argued in court that the CCA was not authorized to impose such a fine. In September 2011, the judge overturned the fine, but asked Yahoo to provide the information within one week.[72] In another long-running case, it emerged that Reliance Communications had tapped phone conversations of parliament member Amar Singh in 2005 based on a fraudulent letter allegedly from Delhi Police, despite the message being replete with grammar and spelling mistakes. In February 2011, the Supreme Court censured the government for not taking action against Reliance for its negligence.[73] These cases followed several scandals in 2009 and 2010 that revealed phone-tapping of lawmakers, politicians, and journalists.[74]

In recent years, the Indian authorities have reportedly enhanced their technical surveillance capabilities, but oversight has not always kept pace.[75] In December 2011, *The Hindu* newspaper reported on the proliferation and, in some cases misuse, of surveillance equipment purchased following the 2009 Mumbai terror attacks. The report alleged that the National Technical Research Organization had deployed monitoring equipment at key internet hubs, enabling large-scale surveillance of a particular area. Variants of such technologies then spread to police at the state level in places like Uttar Pradesh and

[70] Shyamlal Yadav, "9,000 orders for phone interception a month: Govt," Indian Express, January 23, 2012, http://www.indianexpress.com/news/9-000-orders-for-phone-interception-a-month-govt/902831/.
[71] "Two Delhi cops may land in the dock for selling cell call records," The Times of India, March 11, 2012, http://m.timesofindia.com/PDATOI/articleshow/12214794.cms.
[72] "Yahoo moves Delhi HC against govt," The Times of India, November 25, 2011, http://articles.timesofindia.indiatimes.com/2011-11-25/internet/30440468_1_internet-portal-web-portal-delhi-hc.
[73] "Supreme Court slams Centre over Amar Singh phone-tapping case," NDTV, February 12, 2011, http://www.ndtv.com/article/india/supreme-court-slams-centre-over-amar-singh-phone-tapping-case-84983.
[74] Saikat Datta, "We, the Eavesdropped," Outlook, May 3, 2010, http://www.outlookindia.com/article.aspx?265191; "800 New Radia Tapes," Outlook, December 10, 2010, http://www.outlookindia.com/article.aspx?268618; "Government Mulling Law to Regulate Phone Tapping," Daily News & Analysis, December 16, 2010, http://www.dnaindia.com/india/report_government-mulling-law-to-regulate-phone-tapping_1481790.
[75] For example, three Indian firms were named in documents published by the anti-secrecy group Wikileaks as producing and selling sophisticated forms of surveillance equipment—including ones enabling speech analysis, location-tracking, and text-message monitoring. http://spyfiles.org/

Maharashtra. In an effort to reign in such activity, the federal Intelligence Bureau has reportedly tried to shut down 33 passive interception units, though with limited success. Meanwhile, officials in some states, like Andhra Pradesh, shut down such capabilities themselves after sensitive conversations among top officials were among the communications intercepted.[76] In November 2011, the authority to intercept phone calls, emails, and data communications domestically was extended to India's external intelligence agency, the Research and Analysis Wing, to facilitate the tracking of terrorist communications with individuals in foreign countries like Pakistan.[77] In March 2011, lawmaker Manish Tewari introduced a bill that would increase parliamentary oversight of intelligence agencies, but multiple stages of review remained before it might become law.[78] The executive branch has given little indication of intending to improve the legal framework surrounding surveillance activities.

Rather, India has emerged as a leader among countries urging telecommunications companies to reveal their codes or provide other ways for the authorities to intercept their traffic. The government threatened to shut down BlackBerry services in 2010, demanding that the device's manufacturer, Research in Motion (RIM), provide it with the capacity to read encrypted e-mail and instant messages sent via BlackBerry.[79] The dispute was partly resolved in 2011, as RIM established a facility in India to respond to government interception requests. Under the arrangement, the government can submit the name of a suspect it wants to wiretap and RIM will return decoded messages for that individual, provided it determines that the request was indeed lawful. Government officials have also reportedly expressed the desire to monitor communications transmitted over applications like Skype, Facebook, and Twitter more closely.[80]

India lacks a comprehensive privacy law and critics of the 2008 ITA amendments have raised concerns that the law did not adequately protect personal information held by corporations. However, the government has taken steps in recent years to improve the situation. In April 2011, the Indian parliament passed new, comprehensive data protection rules, which observers cited as comparable in some respects to European Union regulations. Though an

[76] Praveen Swami, "The government's listening to us," The Hindu, December 1, 2011, http://www.thehindu.com/news/national/article2678501.ece.
[77] "RAW gets power to tap phones, track emails," The Times of India, December 19, 2011, http://timesofindia.indiatimes.com/india/RAW-gets-power-to-tap-phones-track-emails/articleshow/11161977.cms.
[78] The Intelligence Services (Powers and Regulation) Bill, 2011, Bill No. 23 of 2011, 164.100.24.219/BillsTexts/LSBillTexts/asintroduced/7185LS.pdf.
[79] Bappa Majumdar, "BlackBerry Assures India on Access to Services," Reuters, August 13, 2010, http://www.reuters.com/article/idUSTRE67151F20100813; Mark Lee, "RIM Says BlackBerry Should Be Treated Equally as India Threatens Shut Down," Bloomberg, August 13, 2010, http://www.bloomberg.com/news/2010-08-13/rim-says-blackberry-should-be-treated-equally-as-india-threatens-shut-down.html.
[80] Amol Sharma, "RIM Facility Helps India in Surveillance Efforts," Wall Street Journal, October 28, 2011, http://online.wsj.com/article/SB10001424052970204505304577001592335138870.html#ixzz1itNw7Qq3.

improvement for privacy protection, the rules also drew criticism from the business community because they require immediate implementation (rather than having a transition period), do not allow online consent by users to suffice (written permission by fax, letter, or email is required), and were passed suddenly, quietly, and with little public consultation.[81] In early 2012, the Planning Commission went a step further, establishing a committee of experts to examine privacy laws in other countries and provide a detailed report on suggestions for a draft Privacy Bill for India.[82]

There have been no reports of government agents physically attacking bloggers or online activists. However, many online writers are cautious about what they post due to India's complex ethnic and religious make-up, occasional verbal intimidation, and concerns that online postings might spark communal violence, attacks from Maoists, or reprisals from religious extremists.

Several incidents occurred in 2011 highlighting the threat that hacking and cyber attacks could pose both for domestic and foreign affairs. In June 2011, intelligence agencies reported that a malicious virus was the suspected cause of technical problems at the Indira Gandhi International Airport that prompted the delay of dozens of flights.[83] Press reports in November 2011 indicated that the servers of India's National Informatics Centre had been compromised and used to launch attacks on other countries, including China, giving the impression that the attacker was the Indian government.[84] Meanwhile, loopholes in cyber security were exposed, as a reported 112 government websites were hacked between December 2011 and February 2012, including that of a state-owned telecom.[85]

[81] In August, the government clarified that firms in India's large outsourcing industry were exempt from the new rules. See, "Information Technology Act, 2000," Ministry of Communications and Information Technology; Miriam H. Wugmeister and Cynthia J. Rich, "India's New Privacy Regulations," Morrison & Foerster Client Alert. May 4, 2011, http://www.mofo.com/files/Uploads/Images/110504-Indias-New-Privacy-Regulations.pdf; Kochhar & Co, "2011 Indian Privacy Law," Outsourcing-Law.com, July 13, 2011, http://www.outsourcing-law.com/2011/07/2011-indian-privacy-law/; John Ribeiro, "India Exempts Its Outsourcers from New Privacy Rules," Network World, November 2, 2011, http://www.networkworld.com/news/2011/110211-india-exempts-its-outsourcers-from-252692.html.

[82] Vishwajoy Mukherjee, "New Bill to decide on individual's right to privacy," Tehelka, February 6, 2012, http://www.tehelka.com/story_main51.asp?filename=Ws060212Privacy.asp.

[83] Sidhartha Roy, "12-hour check-in failure at Terminal 3 caused by malicious virus attack?" Hindustan Times, July 5, 2011, http://www.hindustantimes.com/India-news/NewDelhi/12-hour-check-in-failure-at-Terminal-3-caused-by-malicious-virus-attack/Article1-717331.aspx.

[84] Josy Joseph, "Govt servers used for cyber attacks on China, other countries' networks," The Times of India, November 17, 2011, http://timesofindia.indiatimes.com/tech/news/internet/Govt-servers-used-for-cyber-attacks-on-China-other-countries-networks/articleshow/10760699.cms.

[85] John Ribeiro, "In India, 112 government websites hacked in three months," Network World, March 15, 2011, http://www.networkworld.com/news/2012/031512-in-india-112-government-websites-257311.html?hpg1=bn.

After details emerged on individuals from China infiltrating the Indian military and National Security Council,[86] indications surfaced that India was preparing an offensive cyber-warfare capability. According to press reports in August 2010, the government was considering a plan to enlist civilian professionals in efforts to hack the computer systems of hostile powers.[87] The reports of cyber-espionage from China also prompted fears that Chinese companies' growing stake in the telecommunications infrastructure market could facilitate future infiltration or sabotage.[88] In July 2010, the government issued regulations requiring equipment suppliers to allow the local operator, the government, or designated third-party agencies to "inspect the hardware, software, design, development, manufacturing facility and supply chain, and to subject all software to a security threat check."[89] The new rules have been met with significant objections from international companies, who warn that they exceed previous international practice.[90]

[86] "Shadows in the Cloud: Investigating Cyber Espionage 2.0," Information Warfare Monitor and Shadowserver Foundation, April 6, 2010, http://www.nartv.org/mirror/shadows-in-the-cloud.pdf.
[87] Harsimran Singh and Joji Thomas Philip, "Spy Game: India Readies Cyber Army to Hack Into Hostile Nations' Computer Systems," Economic Times, August 6, 2010, http://economictimes.indiatimes.com/news/news-by-industry/et-cetera/Spy-Game-India-readies-cyber-army-to-hack-into-hostile-nations-computer-systems/articleshow/6258977.cms.
[88] See, John Markoff and David Barboza, "Researchers Trace Data Theft to Intruders in China," New York Times, April 5, 2010, http://www.nytimes.com/2010/04/06/science/06cyber.html?_r=1; "Shadows in the Cloud: Investigating Cyber Espionage 2.0," Information Warfare Monitor and Shadowserver Foundation.
[89] Devidutta Tripathy, "Govt Tightens Telecom Rules on Security Concerns," Reuters, July 28, 2010, http://in.reuters.com/article/idINIndia-50466220100728.
[90] Erika Kinetz, "Tough Indian Telecom Rules Spark Foreign Backlash," R&D Magazine, August 3, 2010, http://www.rdmag.com/News/FeedsAP/2010/08/information-tech-tough-indian-telecom-rules-spark-foreign-backlash/.

INDONESIA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	14	11
Limits on Content (0-35)	13	11
Violations of User Rights (0-40)	19	20
Total (0-100)	**46**	**42**

* 0=most free, 100=least free

POPULATION: 241 million
INTERNET PENETRATION 2011: 18 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/I USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Internet communication in Indonesia began developing in 1994 when the first commercial internet service provider (ISP) introduced it to the public. Internet access and its ability to expand avenues for freedom of expression gained further momentum after 1998, when the authoritarian ruler Suharto resigned in the face of public protests. Since then, Indonesia has moved along the path of democratization, a process that has brought about new social, economic and political dynamics for society.

Since 2010, internet and mobile phone usage has continued to grow at a fast pace. Meanwhile, the popularity of social-networking applications has increased exponentially, with Indonesia becoming home to some of the largest contingents of Twitter and Facebook users in the world. The authorities have subsequently sought to regulate online content, citing fears of the internet's use for the spread of pornographic, blasphemous, and terrorism-related content. In the process, a number of actions taken, including passage of the Law on Information and Electronic Transactions (ITE Law) of 2008, have fallen short of international democratic standards. This trend continued in 2011 with the passage of the State Surveillance Law and increased filtering of content loosely defined as sexually explicit. Meanwhile, a surprising criminal conviction under the ITE Law of a housewife who disseminated critical information about a hospital and a series of other questionable criminal cases filed under the ITE exacerbated the atmosphere of legal uncertainty surrounding freedom of expression online and raised concerns of greater restrictions on internet freedom in the future.

OBSTACLES TO ACCESS

Access to the internet has increased consistently in recent years, rising from 5 percent of the population in 2006 to 18 percent—or about 45 million people—by the end of 2011, according to the International Telecommunications Union (ITU).[1] The consulting firm Business Monitor International (BMI) estimated an even higher population of internet users, citing 26 percent (65 million people).[2] Access has not been evenly distributed across the country, however, due to poverty and poor infrastructure in rural areas.

Given Indonesia's archipelagic geography, cable infrastructure is costly to provide and mostly confined to urban areas, particularly on the islands of Java and Bali. Consequently, although the largest broadband provider reported a 40 percent jump in fixed-line subscribers from 2010 to 2011,[3] broadband service remains prohibitively expensive or otherwise unavailable to many Indonesians. A personal broadband connection averages 150,000 Indonesian rupiah per month (US$15); by comparison, the average monthly per capita income among the poorest segments of the population is 200,000 rupiah (US$22),[4] and in Jakarta the minimum wage for workers is about 1.1 million rupiah (around US$122) per month.[5] Most of those with home broadband connections are therefore middle- or upper-class urban residents. Cybercafes have played a key role in enabling internet access to penetrate every corner of Indonesia at a relatively low price.

Internet access via mobile phones had grown exponentially in recent years, emerging as a key avenue for accessing the internet. A 2011 market survey found that 43 percent of Indonesian users cited mobile phones as their main device for internet access.[6] This increase is a combined result of already ubiquitous mobile phone usage and a price war among telecommunications operators. According to the ITU, in 2011 there were 236 million mobile phone users in the country, a penetration rate of nearly 98 percent and a dramatic

[1] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[2] "The Connected Archipelago: The Role of the Internet in Indonesia's Economic Development," Deloitte, December, 2011, http://www.deloitte.com/assets/Dcom-Australia/Local%20Assets/Documents/Services/Corporate%20Finance/Access%20Economics/Deloitte_The_Connected_Archiplelago_Eng_Dec_2011.pdf.

[3] "Info Memo Q3 2011," Telkom Indonesia Investor Report, accessed September 19, 2012, http://www.telkom.co.id/download/File/UHI/Tahun2011/InfoMemo9M11.pdf.

[4] "Badan Pusat Statistik, Jumlah dan Presentase Penduduk Miskin, Garis Kemiskinan, Indeks Kedalaman Kemiskinan, dan Indeks Keparahan Kemiskinan, Menurut Propinsi, pada Maret 2009" [Central Bureau of Statistics, Number and Percentage of Poor Population, Poverty Line, Poverty depth index, and index of severity of Poverty, by Province, March 2009], http://www.bps.go.id/tab_sub/view.php?tabel=1&daftar=1&id_subyek=23&notab=3.

[5] "UMP Jakarta 2010 Naik 4,5 Persen" [Jakarta Per Capita Minimum Wage increases 4.5 percent in 2010], Kompas.com, November 13, 2009, http://megapolitan.kompas.com/read/2009/11/13/18491935/UMP.Jakarta.2010.Naik.4.5.Persen.

[6] Nielsen, "Southeast Asia Digital Consumer Report 2011," p9, http://www.slideshare.net/actionstartup/the-digital-media-and-habits-attitudes-of-south-east-asian-consumers.

increase from the 30 percent rate in 2006.[7] BlackBerry devices by the Canadian firm Research in Motion (RIM) have especially grown in popularity by offering affordable plans. By May 2012, an estimated five million people were using these devices.[8]

The Indonesian government, and especially the Ministry of Communications and Information Technology (MCI), has made the expansion of internet usage a priority. To connect rural areas, the MCI launched a program to establish so-called Smart Villages (Desa Pintar), which would have high quality internet access and mobile phone reception. By 2011, Municipal Internet Service Centers had reportedly been built in 5,330 villages out of a total of 5,748,[9] though not all were fully functional yet.[10]

Indonesia has a range of digital media service providers, though some privately-owned ones are known to have close ties to government ministers. As of 2011, there were 252 ISPs operating throughout Indonesia, the two largest being PT Telecom (a majority state-owned firm) and Indosat, followed by a number of medium-sized ISPs.[11] Their dominance, together with regulatory obstacles imposed by the government, have created a significant barrier for small ISPs to enter the market legally. As of early 2010, there were nine mobile phone service providers, of which the most prominent were PT Telkomsel, PT Indosat, and PT XL Axiata, with Telkomsel itself covering 50 percent of the market.[12] The country's main network-access providers (NAPs), which link retail level ISPs to the internet backbone, are concentrated on Java, and particularly in Jakarta.

The MCI, with its Directorate General of Post and Telecommunication (DGPT), is the primary body overseeing telephone and internet services; it is responsible for issuing licenses

[7] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[8] Rizagana, "Blackberry Mania Shows No Signs of Slowing in Indonesia," Jakarta Globe, May 23, 2012, http://www.thejakartaglobe.com/business/blackberry-mania-shows-no-signs-of-slowing-in-indonesia/519269

[9] Ministry of Communication and Information, "Siaran Pers No. 1/PIH/Kominfo/1/2012 tentang Catatan Strategis dan Prestasi Kementerian Kominfo" [Press Release No. 1/PIH/Kominfo/1/2012 on Strategic Notes and Achievements of Ministry of Communication and Information], January 2, 2012, http://kominfo.go.id/siaran_pers/detail/2365/Siaran+Pers+No.+1-PIH-Kominfo-1-2012+tentang+Catatan+Strategis+dan+Prestasi+Kementerian+Kominfo.

[10] The Failure of PLIK (Program Layanan Internet Kecamatan/Subdistrict Internet Service Program), Summary from various sources on Open Wiki, 2012, Kegagalan PLIK, http://opensource.telkomspeedy.com/wiki/index.php/Kegagalan_PLIK.

[11] Ronald J Deibert et al., "Indonesia" in *Access Contested: Security, Identity, and Resistance in Asian Cyberspace,* ed. (Massachusets Institute of Technology, 2012), http://www.apjii.or.id/index.php?option=com_content&view=article&id=53&Itemid=11.

[12] Hendarsyah Tarmizi, "Mergers and acquisitions inevitable in mobile phone industry," Jakarta Post, March 1, 2010, http://www.thejakartapost.com/news/2010/03/01/mergers-and-acquisitions-inevitable-mobile-phone-industry.html; "Direktorat Jenderal Pos dan Telekomunikasi, Kementerian Komunikasi dan Informasi, Buku Statistik Bidang Pos dan Telekomunikasi 2009" [The Directorate General of Post and Telecommunication, The Ministry of Communication and Information, Statistics Book on Post and Telecommunication 2009], http://www.postel.go.id/webupdate/Download/Data_Statistik_Smt-1_09.pdf; Chanuka Wattegama, Juni Soehardjo, and Nilusha Kapugama, "Telecom Regulatory and Policy Environment in Indonesia: Results and Analysis of the 2008 TRE Survey," March 18, 2008, p. 8 [henceforth "TRE Survey"], http://www.lirneasia.net/wpcontent/uploads/2009/07/TRE_Indonesia_2009Mar18.pdf.

for ISPs, cybercafes, and mobile phone service providers. In addition, the Indonesia Telecommunication Regulation Body (BRTI) conducts regulation, supervision, and control functions related to telecommunications services and networking. In practice, there is an unclear overlap between the mandates and work of the two agencies. Based on the ministerial decree that established it, BRTI is supposed to be generally independent and includes nongovernment representatives. However, observers have questioned its effectiveness and independence, as it is headed by the DGPT director, and draws its budget from DGPT allocations.[13] In April 2011, the MCI Minister added two more members to BRTI for a total of nine members, with six of them representing the public. In September 2011, the MCI began the process for electing new public representatives to BRTI for the 2012-2015 term.[14]

LIMITS ON CONTENT

The internet has expanded Indonesians' access to information, as they are no longer dependent on traditional media (television, radio, and newspapers) for news. Many Indonesians, especially those from the urban middle and upper classes, have adopted the internet as their main information source. In response, the government's approach to the internet has shifted as well. In March 2008, the government passed the ITE Law, which broadened the authority of the MCI to include supervision of the flow of information and possible censorship of online content.[15] Also passed in 2008 was an Anti-Pornography law, which was upheld by the courts in 2010.[16] Since then, filtering of pornographic and violent content has increased. Strong opposition from civil society and, to an extent, from ISPs has successfully derailed some plans for more stringent censorship.

To date, the authorities are not known to have placed any restrictions on content addressing domestic political issues or criticizing the authorities. A draft Regulation on Multimedia

[13] TRE Survey, 16.

[14] "Press Release No. 64/PIH/KOMINFO/9/2011, "Opening Position for 6 Candidates Member of Telecomunication Regulation Committee (BRTI) from Public Element, Kominfo, Sep 7, 2011" [Siaran Pers No. 64/PIH/KOMINFO/9/2011, "Pembukaan Lowongan Bagi 6 Calon Anggota Komite Regulassi Telekomunikasi BRTI (Badan Regulasi Telekomunikasi Indonesia) Dari Unsur Masyarakat], Indonesian Telecommunications Regulatory Authority, September 8, 2011, http://brti.or.id/component/content/article/75-press-release/236-seleksi-brti-2012.

[15] Article 40(2) of ITE Law states that "the government, in compliance with the prevailing laws and regulations, aims at protecting public interest from all forms of disturbances that result from the abuse of electronic information and electronic transaction. Law No. 11 of 2008 on Electronic Transaction and Information, available at http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=1969&filename=UU%2011%20Tahun%202008.pdf.

[16] Karishma Vaswani, "Indonesia Upholds Anti-pornography Bill," BBC News, http://news.bbc.co.uk/2/hi/8586749.stm; "Indonesia To Ask Internet Providers To Block Porn," Reuters, July 14, 2010, http://www.reuters.com/article/2010/07/14/us-indonesia-porn-idUSTRE66D2MQ20100714; "Government Orders ISPs To Start Anti-porn Filtering," Reporters Without Borders, August 11, 2010, http://en.rsf.org/indonesia-government-orders-isps-to-start-11-08-2010,38118.html.

Content introduced in early 2010 prompted a public outcry and fears of increased internet censorship, but it remained on hold since. In July 2011, MCI Minister Tifatul Sembiring commented to the media that the authorities should do more to control social media, which he said had been used to destabilize governments in Tunisia and Libya.[17] His statement was widely criticized in the blogosphere, and no subsequent action was taken to restrict dissemination of information via social media tools.

Websites related to pornography, violent extremism, or censorship circumvention are blocked. Efforts to restrict access to pornography gained momentum after sexual videos of several celebrities were posted online and began circulating widely in mid-2010. Testing by the OpenNet Initiative conducted on several ISPs in late 2010 found that internet filtering was inconsistent across providers, but that most blocked various websites related to pornography.[18] Several ISPs also blocked a wider range of content, including information related to sex education, LGBT material, or websites like Freespeechcoalition.com run by representatives of the adult entertainment industry in the United States. Also blocked by some ISPs was the website Freespeech.org belonging to a U.S. online news network, as well as sites providing anonymizing and circumvention tools.[19] As of May 2012, the situation remained the same, with the inconsistency across ISPs particularly notable. In January 2011, RIM agreed to begin filtering pornographic websites on their BlackBerry devices in Indonesia after the government regulator warned that the firm's market access could be restricted if it failed to comply.[20] When attempting to access a blocked site, BlackBerry users reportedly encounter a technical error rather than a message informing them that access to the site has been deliberately restricted.

In September 2011, the MCI announced that it would begin blocking Islamist websites with content promoting violence, radicalism and terrorism. The announcement came one week after a suicide bomber attacked a church in Central Java.[21] According to the ministry, initially 300 websites would be blocked based on provisions in the ITE law.[22] This was out of

[17] "Tifatul Calls for Social Media Control," Jakarta Globe, July 14, 2011, http://www.thejakartaglobe.com/home/tifatul-calls-for-social-media-controls-to-avoid-arab-spring-style-uprisings/452907.
[18] "Country Profile—Indonesia," OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/indonesia.
[19] Ronald J Deibert et al., "Indonesia" in *Access Contested: Security, Identity, and Resistance in Asian Cyberspace,* ed. (Massachusets Institute of Technology, 2012), http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-indonesia.pdf
[20] Femi Adi, "RIM Says Committed To Indonesia, Will Block Porn on BlackBerrys," Bloomberg, January 17, 2011, http://www.bloomberg.com/news/2011-01-17/rim-says-committed-to-indonesia-will-block-porn-on-blackberrys.html; Ardhi Suryadhi, "Sensor di Blackberry terus diawasi" [Censorship on Blackberry Continuously Observed], Detik Inet, January 21, 2011, http://www.detikinet.com/read/2011/01/21/142056/1551687/328/sensor-di-blackberry-terus-diawasi.
[21] Patrick Barta, "Suicide Attack Strikes Church in Indonesia," Wall Street Journal, September 26, 2011, http://online.wsj.com/article/SB10001424052970204831304576592103793435480.html.
[22] Ardhi Suryadhi, "Kominfo:300 Situs Radikal Sudah Diblokir" [MCI: 300 radical websites has been blocked], Detik Inet, September 28 2011, http://www.detikinet.com/read/2011/09/28/122150/1732179/398/kominfo-300-situs-radikal-sudah-diblokir; Ratri Adityarani, "To Fight Terrorism Indonesia Blocks 300 Websites," TechinAsia, September 29, 2011, http://www.penn-olson.com/2011/09/29/terrorism-indonesia-blocks-300-websites/.

a list of 900 website compiled from public submissions. The specific criteria used to select the blocked sites remain unclear. The list of sites has not been published, rendering it impossible to independently confirm if they were indeed blocked.[23]

The government also signaled that it would begin blocking or shutting down file-sharing websites. In July 2011, representatives of the Indonesian music industry urged the MCI to shutter 20 websites that enabled users to download songs without permission from the artists.[24] As of May 2012, four of the 20 sites were no longer operational, while the others remained accessible.[25]

There were no reports of the Indonesian authorities engaging in significant administrative deletions. According to Google's Transparency Report, the Indonesian government had made fewer than 10 requests for content removal from the company's various services between January and June 2011.[26]

Transparency surrounding the online censorship has improved somewhat, but much remains unclear as evident from the above discussion of terrorism-related blocks. The government maintains a website called Trust Positif that provides a database of blacklisted domains and URLs deemed illegal (such as those involving pornography, hate speech, etc). The purpose of the database is to serve as a reference for ISPs and other providers on what content to filter on their networks.[27] As of mid-2012, there were 745,235 domain names and 54,795 URLs related to pornographic content listed on the site. The site also provides an email address and form for individuals to report illegal content. The MCI decides which sites to blacklist and no judicial order is required.

Indonesians are avid social media users. With growing access to the internet via mobile phones, engagement on social media surpassed email as the number one online activity in 2011, according to a recent market survey.[28] The video-sharing site YouTube, the social-

[23] Camelia Pasandaran, "Tifatul Says Websites Promoting Terrorism Would Be Blocked," Jakarta Globe, April 29, 2011, http://www.thejakartaglobe.com/home/tifatul-says-web-sites-promoting-terrorism-would-be-blocked/438194.
[24] Achmud Rouzni Noor II, "Menkominfo Didesak Tutup 20 Situs Musik Ilegal" [MCI Pushed to Close Down 20 Illegal Music Website], Detik Inet, July 21 2011, http://www.detikinet.com/read/2011/07/21/161521/1686205/398/menkominfo-didesak-tutup-20-situs-musik-ilegal.
[25] The sites Mp3lagu.com, Pandumusica.info, Musik-flazher.com, Freedownloadmp3.org are no longer accessible, but there was no confirmation that they were shut down by the authorities rather than being discontinued for some other reason. See, "Situs 4shared Akan Diblokir Menkominfo" [The website 4shared.com will be blocked by MCI], August 8 2011, Okezone.com, http://music.okezone.com/read/2011/08/08/386/489495/situs-4shared-akan-diblokir-menkominfo.
[26] "Google Transparency Report," Google, January-June, 2011, accessed August 21, 2012, http://www.google.com/transparencyreport/governmentrequests/ID/?p=2011-06&t=CONTENT_REMOVAL_REQUEST
[27] MCI TRUSTPOSITIF Database, last modified February 28 2012, http://trustpositif.kominfo.go.id/files/downloads/index.php?dir=database%2F.
[28] Nielsen, "Southeast Asia Digital Consumer Report 2011," p12, Slideshare, October 2011, http://www.slideshare.net/actionstartup/the-digital-media-and-habits-attitudes-of-south-east-asian-consumers

networking site Facebook, and the microblogging platform Twitter are generally available without interference. By May 2012, Indonesia had 42 million Facebook users (the fourth highest globally),[29] and at least 19 million Twitter accounts registered (the fifth highest globally), of which five million were active.[30] One study found that Indonesians send 1.3 million tweets per day, over 80 percent of them from mobile devices.[31]

The development of Indonesia's blogosphere began around 1999, with most early blogs written by Indonesians living abroad who worked in the information technology industry. In 2001, the younger generation came to dominate Indonesian blogs, largely writing about their daily lives. By 2005 and 2006, blogs had begun to specialize in various topics, including politics, economics, media, food, and entertainment. However, as Facebook and Twitter use has grown, the popularity of blogging as declined. Nevertheless, according to Salingsilang.com, a directory of Indonesian bloggers, there were over 5.2 million Indonesian blogs as of the end of 2011.[32] An analysis of the topics covered by these blogs reveals that most of them are more concerned with popular culture, like Korean artists, or international current events, like the Tsunami in Japan, rather than domestic politics.

Traditional media outlets and professional journalists—rather than bloggers or citizen journalists—typically cover important political developments and corruption investigations. Nevertheless, in 2011, several Twitter accounts gained prominence as they posted messages with up-to-date information on corruption cases or behind-the-scenes details about political affairs. For example, the Twitter account "@benny_israel," allegedly belonging to a user with a background in intelligence, was created in November 2010. By early 2011, it had gathered thousands of followers for its tweets whose topics range from past human right violation cases to corruption cases to predictions on political developments, though some netizens doubted their credibility.[33] In April 2011, another user created the Twitter account "@TrioMacan2000," which quickly became famous for its Twitter lectures, a stream of sometimes 200 tweets at a time relaying background information about widely reported corruption cases.[34]

[29] "Facebook Statistics By Country," Social Bakers, accessed August 21, 2012, http://www.socialbakers.com/facebook-statistics/?interval=last-6-months.
[30] "Geolocation Analysis of Twitter Accounts by Semiocast," Semiocast, January 31, 2012, http://semiocast.com/publications/2012_01_31_Brazil_becomes_2nd_country_on_Twitter_superseds_Japan.
[31] Salingsilang, "Indonesia Social Media Landscape Report: A Snapshot of Indonesian User Behavior," SlideShare, August 5, 2011, http://www.slideshare.net/salingsilang/indonesia-social-media-landscape-h1-2011-3rd-salingsilangcom-report.
[32] Direktori Blog: Salingsilang.com, http://blogdir.salingsilang.com/.
[33] Stefanus Yugo Hindarto, "'Kicauan' Benny Israel Timbulkan Pro-Kontra" [Procons surrounding Tweets from Benny Israel], Okezone.com, January 23 2011, http://news.okezone.com/read/2011/01/23/339/417003/kicauan-benny-israel-timbulkan-pro-kontra.
[34] "Wajar Muncul Akun Psidonim di Twitter" [It's common to see pseudonym account on Twitter], Tempo.com, February 11, 2012, http://www.tempo.co/read/news/2012/02/11/072383226/Wajar-Muncul-Akun-Psidonim-di-Twitter.

In November 2011, Indonesia and its newly established local chapter of the Association of Southeast Asian Nations (ASEAN) Blogging Community hosted the first regional ASEAN Blogger conference.[35] About 200 bloggers from across Southeast Asia gathered in Bali in parallel to the main ASEAN summit. At the conclusion of the one-day meeting, they issued a collective declaration[36] committing to cooperate at using social media to realize ASEAN's political, economic, and cultural potential and to promote international understanding, while also aspiring to uphold freedom of expression based on the Universal Declaration of Human Rights. [37]

VIOLATIONS OF USER RIGHTS

Indonesia's constitution guarantees freedom of opinion in its third amendment, adopted in 2000.[38] The constitution also includes the right to privacy and the right to gain information and communicate freely.[39] These rights are further protected by various laws and regulations.[40] However, a range of other laws limit free expression, despite legal experts' claims that they conflict with the constitution.[41] Approximately seven different laws address internet freedom in one respect or another, the most prominent being the 2008 ITE Law. This legal framework is fairly harsh, although the authorities do not always use the full range of powers granted by the laws.[42] In October 2011, the Indonesian parliament passed a new State Intelligence Law, which adds severe penalties (including up to ten years imprisonment

[35] Haz Pohan, "Indonesia Established First Chapter of ASEAN Blogger Community," ASEAN Blogger, May 12, 2011, http://aseanblogger.com/?p=636

[36] Aris Heru Utomo,"The role of bloggers in the ASEAN Community," Jakarta Post, November 17, 2011, http://www.thejakartapost.com/news/2011/11/17/the-role-bloggers-asean-community.html.

[37] Iman, "ASEAN Blogger Declaration," Iman Brotoseno (blog), November 16, 2011, http://blog.imanbrotoseno.com/?p=1521.

[38] Constitution of 1945, Article 28E(3).

[39] Ibid., Articles 28F and 28G(1).

[40] Among others, Law No. 39 of 1999 on Human Rights, available at http://www.legalitas.org/incl-php/buka.php?d=1900+99&f=uu39-1999eng.htm; Law No. 14 of 2008 on Freedom on Information, available at http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=1971&filename=UU%2014%20Tahun%202008.pdf; and Law No. 40 of 1999 on the Press, available at http://www.legalitas.org/incl-php/buka.php?d=1900+99&f=uu40-1999.htm.

[41] Wahyudi et al., "Elsam, Asesmen Terhadap Kebijakan Hak Asasi Manusia dalam Produk Legislasi dan Pelaksanaan Fungsi Pengawasan DPR RI" [Assesment to the Human Rights Policy in Legislation Product and the Implementation of the Parliament Monitoring Function], 2008. Hard copy on file with the author.

[42] Pieces of legislation that limit free expression in Indonesia, include: Criminal Code, Law No 1 Year 1946 on Regulation of the Criminal Law, Law No 1/PNPS/1965 on Blasphemy, Law No 27 Year 1999 on Crimes against State Security, Law No 32 Year 2002 on Broadcasting, Law No 32 Year 2004 on Regional Government, Law No 10 Year 2008 on General Election, Law No 11 Year 2008 on Information and Electronic Transaction (ITE), Law No 42 Year 2008 on Presidential Election, Law No 44 Year 2008 on Pornography, Law No 24 Year 2009 on Flag, Official Language, State Emblem and National Anthem, and Intelligence Law.

and fines of over US$10,000) for revealing or disseminating "state secrets," a term defined very vaguely in the legislation.[43]

Provisions of the 2008 ITE Law have been repeatedly used to prosecute Indonesians for online expression. The law calls for heavier penalties for criminal defamation, hate speech, and inciting violence than those set out in the penal code. For example, anyone convicted of committing defamation online may face up to six years in prison, and a fine of up to 1 billion rupiah (US$111,000).[44] The landmark online defamation case of Prita Mulyasari is perhaps the most important among eight indictments issued since 2008 under the ITE Law. Prita, a young housewife, was arrested in May 2009, held for three weeks, and charged with defamation for an email message she circulated to friends and relatives in which she criticized her treatment at a private hospital in Tangerang.[45] The hospital also filed a parallel civil suit. She soon gained popular support, including from bloggers and local civil society groups.[46] In December 2009, the Banten High Court ruled against Prita in the case, ordering her to pay 204 million rupiah (US$19,600) in damages to the hospital.[47] The blogging community responded with a huge campaign called Koin Keadilan, or Justice Penny, and succeeded in collecting over 600 million rupiah on her behalf.[48] By the end of 2010, the Supreme Court had decided in Prita's favor regarding the civil suit,[49] and she won her criminal case in Tangerang District Court, which acquitted her on all charges.[50] However, an appeal by prosecutors to the Supreme Court in 2011 resulted in an unexpected guilty verdict in July under the ITE Law.[51] Though she did not serve any jail time, Prita was given a six-month suspended sentence and placed on probation for one year, during which she must be careful not to commit a similar offense. The decision was widely criticized by legal

[43] "Indonesian Parliament passes controversial intelligence bill," Engage Media, October 25, 2011, http://www.engagemedia.org/Members/emnews/news/indoneisan-parliament-passes-controversial-intelligence-bill.
[44] ITE Law, Article 45.
[45] Nadya Kharima, "UU ITE Makan Korban Lagi" [ITE Bill creates a victim again], Primaironline, May 28, 2009, http://primaironline.com/berita/detail.php?catid=Sipil&artid=uu-ite-makan-korban-lagi.
[46] Hertanto Soebijoto, "Kasus Prita: Lima LSM Ajukan 'Amicus Curiae'" [Prita case: 5 NGOs submit Amicus Curiae], Kompas, October 14, 2009, http://megapolitan.kompas.com/read/2009/10/14/16474375/Kasus.Prita:.Lima.LSM.Ajukan..quot.Amicus.Curiae.quot.
[47] Cyprianus Anto Saptowalyono, "Humas PT Banten: Putusan buat Prita belum berkekuatan hukum tetap" [Banten Corporate Public Relations: Verdict for Prita does not have legal power], Kompas, December 7, 2009, http://m.kompas.com/news/read/data/2009.12.07.13135791.
[48] Mega Putra Ratya, "Penghitungan selesai total koin Prita Rp. 650.364.058" [Counting of Coins for Prita has collected a total of Rp. 650,364,058], Detikcom, December 19, 2009, http://m.detik.com/read/2009/12/19/113615/1262652/10/penghitungan-selesai-total-koin-prita-rp-650364058.
[49] Ina Parlina, "Supreme Court Overturns Acquittal of Housewife Prita," The Jakarta Post, July 9, 2011, http://www.thejakartapost.com/news/2011/07/09/supreme-court-overturns-acquittal-housewife-prita.html.
[50] Ismira Lutfia, Heru Andriyanto, Putri Prameshwari, and Ronna Nirmala, "Prita Acquitted, But Indonesia's AGO Plans Appeal," Jakarta Globe, December 29, 2009, http://www.thejakartaglobe.com/home/prita-mulyasari-cleared-of-all-charges/349844; Yudi Rahmat, "PBHI Apresiasi putusan hakim PN Tangerang di Kasus Prita" [PBHI appreciates verdict of Tangerang State Court judge in Prita Case], Primaironline, December 29, 2009, http://primaironline.com/berita/detail.php?catid=Sipil&artid=pbhi-apresiasi-putusan-hakim-pn-tangerang-di-kasus-prita.
[51] Faisal Maliki Baskoro and Rangga Prokosso, "Shock Guilty Verdict in Prita Mulyasari Saga," Jakarta Globe, July 9, 2011, http://www.thejakartaglobe.com/jakarta/shock-guilty-verdict-in-prita-mulyasari-saga/451797.

analysts and bloggers, who argued that it was inconsistent with the court's decision on the civil suit and set a dangerous precedent that any consumer who complained online about service by a private entity could face criminal punishment.[52] Prita and her lawyers filed a request for review of the case by the Indonesian Judicial Committee, but no further developments had been reported by May 2012.[53]

In another case reminiscent of Prita's, criminal defamation charges were filed in January against Ira Simatupang, a doctor from a hospital in Tangerang, over a series of private emails to colleagues and friends. According to some news reports, the messages contained accusations of sexual harassment against a colleague, while others asserted the content was legitimately offensive and defamatory.[54] The trial was ongoing as of May 2012.[55] Meanwhile, throughout 2011 and early 2012, several other criminal cases were filed under the ITE Law, in some instances for acts that under international free expression standards would typically draw civil rather than criminal penalties.[56] The cases ranged from a news website editor filing a police complaint over a copyright violation by an aggregator site,[57] to defamation charges filed by a member of parliament against someone who circulated over Twitter alleged photos of her drunk and dancing at a cafe,[58] to a politician claiming another politician had defamed him via mobile phone text messages.[59] Most of the cases were ongoing as of

[52] "Membaca Putusan Kasasi MA Dalam Kasus Prita" [Reading into Supreme Court Decision in Prita Case], Dunia Angara, July 22, 2011, http://anggara.org/2011/07/22/membaca-putusan-kasasi-ma-dalam-kasus-prita/.

[53] Prita Mulyasari, "Prita Laporkan Tiga Hakim Agung ke KY" [Prita report on 3 Supreme Court Judges to Indonesian Judicial Commission], Republika, August 15, 2011, http://www.republika.co.id/berita/nasional/hukum/11/08/15/lpyiij-prita-laporkan-tiga-hakim-agung-ke-ky.

[54] "Indonesian Doctor Facing Defamation for Telling Friends of Sexual Harassment," Jakarta Globe, January 26, 2012, http://www.thejakartaglobe.com/home/indonesian-doctor-facing-defamation-for-telling-friends-of-sexual-harassment/493949; "Prosecutor Demands Six Months in Prison for Doctor Who Sent Offensive Emails," Jakarta Globe, June 13, 2012, http://www.thejakartaglobe.com/lawandorder/prosecutor-demands-six-months-in-prison-for-doctor-who-sent-offensive-emails/524137; "Language Expert: Ira Email Meaningful Defamation" [in Bahasa], Satelit News, May 1, 2012, http://satelitnews.co.id/pakar-bahasa-email-ira-bermakna-fitnah.

[55] In July ,Simatupang was found guilty and received a five-month suspended sentence. See, "Ira Simatupang Sentenced To Five Months, The Prosecutor Appeals," Satelit News, July 18, 2012, http://satelitnews.co.id/ira-simatupang-divonis-5-bulan-jaksa-banding.

[56] A series of other cases involved crimes such as fraud or child pornography that would draw criminal penalties in most democratic societies. See, Mega Putra Ratya, "Cabuli Anak-anak, Warga Inggris Ditangkap di Batam" [British child sex offender caught in Batam], Detik News, June 11, 2011, http://news.detik.com/read/2011/11/06/143126/1761334/10/cabuli-anak-anak-warga-inggris-ditangkap-di-batam; E Mei Amelia R,"Catut Nama Erwin Aksa di Facebook Seorang PNS Diciduk Polda Metro" [Pretending to be Erwin Aksa on Facebook a civil servant detained by Jakarta Police], Detik News, April 26, 2011, http://news.detik.com/read/2011/04/26/132049/1625793/10/catut-nama-erwin-aksa-di-facebook-seorang-pns-diciduk-polda-metro.

[57] Wahyu Romadani, "Laporkan CEO Perusahaan Grup Djarum ke Polisi" [CEO of Djarum Grup to Police], Gres News, August 15, 2011, http://www.gresnews.com/berita/hukum/1326158-gresnews-com-laporkan-ceo-perusahaan-grup-djarum-ke-polisi.

[58] Lia Harahap, "Kartika Siap Hadapi Laporan Anggota F-Gerindra Noura Gara-gara Twitter" [Kartika ready to report Gerindra Faction Member Noura because of Twitter], Detik News, May 13, 2011, http://news.detik.com/read/2011/05/13/095041/1638812/10/kartika-siap-hadapi-laporan-anggota-f-gerindra-noura-gara-gara-twitter

[59] Aprisal Rahmatullah, "Yusuf Supendi Coba Jerat Presiden PKS Dengan Pasel ITE" [Yusuf Supendi use ITE law to report PKS (Social Justice Party) President], Detik News, March 29, 2011, http://news.detik.com/read/2011/03/29/180409/1604007/10/yusuf-supendi-coba-jerat-presiden-pks-dengan-pasal-ite.

May 2012, but there were nor reported indictments. Such prosecutions under the ITE Law have contributed to an increased atmosphere of caution and self-censorship among online writers and average users. They have also spurred public demand for amendment of the ITE Law. However, as of mid-2012, there had been no proposed changes made, although several ministries were reportedly reviewing it.[60]

Online users may also face criminal charges based on the penal code and a 1965 law that criminalizes blasphemy and the dissemination of atheism.[61] In January 2012, police arrested Alexander Aan, a 30-year-old civil servant in West Sumatra, on blasphemy charges after radical Islamists beat him and reported to the authorities that he had created a Facebook page titled "Ateis Minang" (Minang Atheist) that received about 1,200 "likes."[62] Among the items Aan had posted to the page was a cartoon involving the Prophet Muhammad. He was charged under blasphemy provisions of the penal code and the ITE Law for allegedly disseminating via the internet information that "incites religious hatred and animosity."[63]

Several other laws relating to online communications have been passed or considered in recent years. Law No. 44 of 2008 on Pornography regulates the publication of pornographic materials. Critics say the law defines the crime of disseminating "pornography" very broadly, while requiring cybercafe owners to monitor their customers. In 2010, the government introduced another draft law to parliament called the Computer Crimes Law (Tindak Pidana Teknologi Informasi (TPT)).[64] Although the draft bill mostly deals with penalties related to electronic business transactions, it also stipulates numerous restrictions on computer and internet usage, often prescribing harsher penalties for offenses already covered in the criminal code and other legislation.[65] Passage of the new measure would increase the number of laws regulating criminal defamation to eight, with each calling for a different

[60] "Siaran Pers No. 1/PIH/Kominfo/1/2012 Tentang Catatan Strategis dan Prestasi Kementerian Kominfo", Kementerian Komunikasi dan Informatika Republik Indonesia, January 2, 2012 [Press Release No. 1/PIH/Kominfo/1/2012 on Strategic Notes and Achievements of Ministry of Communication and Information" Indonesian Department of Communications and Information, January 2, 2012], http://kominfo.go.id/siaran_pers/detail/2365/Siaran+Pers+No.+1-PIH-Kominfo-1-2012+tentang+Catatan+Strategis+dan+Prestasi+Kementerian+Kominfo.

[61] Law No 1/PNPS/1965 on Blasphemy.

[62] Stofiardi Bachyul, "Atheist civil servant arrested for blasphemy," The Jakarta Post, January 20, 2012, http://www.thejakartapost.com/news/2012/01/20/atheist-civil-servant-arrested-blasphemy.html/.

[63] In June 2012, Aan was found guilty and sentenced to two and a half years imprisonment and a fine of 100 million Rupees (US$10,500). See, "Indonesia: Atheist in Padang sentenced to two and a half years imprisonment," Asia Pacific Solidarity Network, June 15, 2012, http://asia-pacific-solidarity.net/southeastasia/indonesia/statements/2012/ahrc_indonesiaatheistinpadangs_150612.htm; Kimberly Winston, "Atheists rally for persecuted unbeliever in Indonesia," Washington Post, July 19, 2011, http://www.washingtonpost.com/national/on-faith/atheists-rally-for-persecuted-unbeliever-in-indonesia/2012/07/19/gJQAfg2JwW_story.html.

[64] Wendy Zeldin, "Indonesia: Cyber Crime Bill," Library of Congress, January 13, 2012, date accessed August 21, 2012, http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205401769_text.

[65] Muhammad Aminudin,"Cyber Crime Menggurita, DPR Kebut UU Tindak Pidana TI" [Cybercrimes Imminent, Parliament Speedup Cybercrime Law], Detik Inet, March 3, 2012, http://inet.detik.com/read/2012/03/25/091604/1875607/399/cyber-crime-menggurita-dpr-kebut-uu-tindak-pidana-ti.

sentence. MCI Minister Tifatul Sembiring told media that he expected the law to pass during 2012.[66] Also under discussion has been a draft law on ICT convergence, one that would collectively replace the Telecommunications Law, Broadcasting Law, and possibly the ITE Law. Critics have raised concerns that under the law, ICT applications (including websites) would be required to obtain a license from the MCI for a fee, a process that could place restrictions on freedom of expression, as well as for the open source community,[67] and expansion of WiFi hotspots. [68]

Fears of abusive surveillance practices increased in 2011 with the passage in October of a new State Intelligence Law, though several problematic provisions were removed prior to passage.[69] Previously, surveillance was not a serious concern. The new law, however, was widely criticized by international and domestic human rights groups for granting broader authority to the State Intelligence Body (Badan Intelijen Negara, or BIN) to intercept communications. Although a court order is required in most cases, concerns remain that due to limits on judicial independence, permission will be granted too easily.[70] The State Intelligence Law is one of at least nine laws that allow the authorities to conduct surveillance or wiretapping.[71] The only other one that explicitly states the need for judicial oversight is Law No. 35 of 2009 on Narcotics, and even in that instance the requisite procedures are unclear. There is little oversight or checks in place to prevent abuse by agencies conducting monitoring for the purposes of combating terrorism and identifying terrorist networks, the most known use of surveillance techniques. At present, the police,[72] the Indonesian Corruption Commission (KPK),[73] and the National Narcotics Board (Badan Narkotika

[66] "Pemerintah Berharap UU Tindak Pidana TI Rampung Tahun Ini" [Government Hope Cybercrime Law Finalized This Year Kompas Tekno], July 17, 2012, http://tekno.kompas.com/read/2012/07/17/16365063/Pemerintah.Berharap.UU.Tindak.Pidana.TI.Rampung.Tahun.Ini.

[67] Taken from his tweet "@sufehmi" on 8 October 2010, 23:30, Harry Sufehmi is 2nd Deputy Chairperson of AOSI and IT Practitioner.

[68] Interview with Harry Sufehmi, 2nd Deputy Chairperson of AOSI and IT Practitioner.

[69] Ezra Sihite and Anita Rachman, "Indonesia's Intelligence Bill Passage Prompts 'Big Brother' Fears," Jakarta Globe, October 12, 2011, http://www.thejakartaglobe.com/home/indonesias-intelligence-bill-passage-prompts-big-brother-fears/471058; International Crisis Group, "Indonesia: Debate over a New Intelligence Bill," Asia Briefing No 124, July 12, 2011, http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia/B124-indonesia-debate-over-a-new-intelligence-bill.aspx.

[70] "Indonesia: Repeal new Intelligence Law. Overbroad Provisions Facilitate Repression," Human Rights Watch, October 26, 2011, http://www.hrw.org/print/news/2011/10/26/indonesia-repeal-new-intelligence-law.

[71] The laws are, among others, (1) Chapter XXVII Indonesian Criminal Code, Article 430—434; (2) Law No. 5 of 1997 on Psychotropic Drugs; (3) Law No. 31 of 1999 on Eradication of Corruption; (4) Law No. 36 of 1999 on Telecommunication; (5) Government Regulation in Lieu of Law No. 1 of 2002 on Combating Terrorism; (6) Law No. 18 of 2003 on Advocates; (7) Law No. 21 of 2007 on Combating Human Trafficking; (8) Law No. 11 of 2008 on Electronic Transaction and Information; and (9) Law No. 35 of 2009 on Narcotics.

[72] Law No. 16 of 2003 on the Stipulation of Government Regulation in Lieu of Law No. 1 of 2002 on the Eradication of Crimes of Terrorism (State Gazette No. 46 of 2003, Supplement to the State Gazette No. 4285), available at:http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=1548&filename=PP_Pengganti_UU_No_1_th_2002.pdf.

[73] Law No. 30 of 2002 on the Anti-Corruption Commission, available at: http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=300&filename=UU_no_30_th_2002.pdf.

Nasional) also have the legal authority to conduct surveillance.[74] In January 2012, the Alliance for Independent Journalists (AJI), four other civil society groups, and 13 individuals filed a request for judicial review of the State Intelligence Law with the Constitutional Court.[75]

Mobile phone users are obliged to register their numbers upon purchasing a phone by submitting their identity information directly to the government via text message. In practice, however, this obligation is often ignored. The government continued in 2011 to pressure RIM to set up local servers for its BlackBerry devices in Indonesia—whose users number over five million—amidst concerns that the encrypted communication network would hinder anti-terrorism and anti-corruption efforts.[76] In December 2011, the BRTI threatened to terminate RIM's BlackBerry services in the country if they refused to comply, though no deadline was set. Throughout 2011, RIM reportedly accommodated isolated requests for user data from law enforcement agencies.[77]

Apart from the above-mentioned beating of Alexander Aan, there have been no reports of extralegal attacks, intimidation, or torture of bloggers or other internet users. However, it is common for police—and sometimes Islamic fundamentalist groups—to conduct searches of cybercafes without prior notice, since the venues are perceived as places conducive to accessing pornography.[78] Most of the searches are conducted without warrants and are rarely followed by court proceedings, leading observers to believe the raids are carried out by police for the purpose of extracting bribes from cybercafe owners.

[74] Law No. 35 of 2009 on Narcotics, available at: http://www.setneg.go.id/components/com_perundangan/docviewer.php?id=2351&filename=UU%2035%20Tahun%202009.pdf.

[75] "Indonesia: State Intelligence law challenged in court," Southeast Asian Press Alliance, January 25, 2012, http://www.seapabkk.org/alerts/36-updates/100558-indonesia-state-intelligence-law-challenged-in-court.html. Ezra Sihite; Keyko Ranti Ramadhani, "Indonesian Rights Activists Challenge to Intelligence Law," Jakarta Globe, January 6, 2012, http://www.thejakartaglobe.com/home/indonesian-rights-activists-challenge-to-intelligence-law/489358.

[76] Associated Press, "Indonesia Says Blackberry Will Filter Out Porn," Ipolitics, January 11, 2011, http://ipolitics.ca/2011/01/11/indonesia-says-blackberry-to-filter-out-porn/; John Ribeiro, "Indonesia Presses RIM Over its Blackberry Service," Network World, August 5, 2010, http://www.networkworld.com/news/2010/080510-indonesia-presses-rim-over-its.html.

[77] Arientha Primanita and Faisal Maliki Baskoro, "Pressure on BlackBerry Maker to Build Servers in Indonesia," Jakarta Globe, December 14, 2011, http://www.thejakartaglobe.com/business/pressure-on-blackberry-maker-to-build-servers-in-indonesia/484588; John Terauds, "RIM must install local data centre, demands Indonesia," The Star, December 12, 2011, http://www.thestar.com/business/article/1100543--rim-must-install-local-data-centre-demands-indonesia; Ardhi Suryadhi, "Nasib Blackberry Ditentukan Hari ini" [Fate of Blackberry Decide Today], Detik Inet, January 17, 2011, http://www.detikinet.com/read/2011/01/17/101648/1548007/328/nasib-blackberry-ditentukan-hari-ini.

[78] "Police Bust High School Students for Cutting Class in Favor of Facebook," Jakarta Globe, March 3, 2010, http://www.thejakartaglobe.com/home/police-bust-high-school-students-for-cutting-class-in-favor-of-facebook/361673; "Indonesia rounds up students in cybercafés," Agence France-Presse, February 23, 2010, http://newsinfo.inquirer.net/breakingnews/infotech/view/20100223-254794/Indonesia-rounds-up-students-in-cybercafs.

Politically motivated cyberattacks against civil society groups have not been reported in Indonesia. However, several government websites including those of the Indonesian Police Force (POLRI), the MCI, and the Indonesian state-owned oil company Pertamina were victims of cyberattacks in May 2011 that defaced their home pages.[79] Blaming the incompetence of the websites' administrators, a hacker by the name of Yogyacarderlink left a message warning them to be more careful in the future.[80] The attacked websites were quickly restored without incurring permanent damage.[81]

[79] Rachmatunisa, "Situs Kominfo Dibobol Lagi" [MCI website hacked again], Detik Inet, May 31, 2011, http://www.detikinet.com/read/2011/05/31/151008/1651012/398/situs-kominfo-dibobol--lagi-.
[80] Fajar Widiantoro, "Giliran Situs Pertamina Disambangi Hacker" [It's Pertamina Website turn now Hacked], Detik Inet, May 19, 2011, http://www.detikinet.com/read/2011/05/19/104928/1642239/398/giliran-situs-pertamina-disambangi-hacker.
[81] Ardhi Suryadhi, "Tidak Diurus Situs Polri Gampang Dibobol" [With no maintenance Indonesian Police website easily hacked], Detik Inet, May 19, 2011, http://www.detikinet.com/read/2011/05/19/142347/1642552/323/tidak-diurus-situs-polri-gampang-dibobol.

IRAN

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	21	21
Limits on Content (0-35)	29	32
Violations of User Rights (0-40)	39	37
Total (0-100)	**89**	**90**

* 0=most free, 100=least free

POPULATION: 79 million
INTERNET PENETRATION 2011: 21 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

The Iranian regime has long had an ambivalent relationship with the internet, viewing it alternately as a catalyst for economic development or as an invading force that threatens the Islamic state's strict social, religious, and political values. Over the past three years, the balance has markedly shifted towards the latter, as the leadership has decisively chosen political control over the benefits of a more open society. After the internet played an important role in the opposition movement that followed the disputed presidential election of June 12, 2009, the Iranian authorities waged an active campaign against internet freedom, employing extensive and sophisticated methods of control that went well beyond simple content filtering. The government also reportedly allocated US$500 million in its 2010–11 annual budget for the purpose of combating of what it termed a "Soft War" being waged against the regime by its perceived enemies via media and online activities. The regime's increasing tendency to view the internet as a threat and the importance of countering the "Soft War" were reflected in various official statements in 2011.[1]

These circumstances contributed to an overall deterioration in the internet freedom environment in 2011 and early 2012, although the mass arrests and denial-of-service attacks that characterized the previous two years were less prominent. Instead, the regime turned to more nuanced and sophisticated tactics for subverting free expression online. These included: upgrading the filtering technology and using it to block particular types of traffic,

[1] For instance, Reza Taghipour, the ICT Minister, said that "the Internet has been formed based on liberal and humanistic values, which is dangerous and needs to be changed," http://www.mehrnews.com/fa/NewsDetail.aspx?NewsID=1431708.

hacking two international firms' digital certificates to undermine user privacy, and implementing the first stages towards establishing a National Internet. Together, these measures indicate the regime's intention to increasingly cut off Iranian internet users from websites and others online resources based outside the country. Alongside this enhanced technical sophistication, however, the regime also continued to use low-tech repression to punish and intimidate bloggers, journalists, and ordinary users. Over the past two years, Iranian judicial authorities meted out some of the harshest sentences in the world for online activities, including imposing the death penalty on three bloggers and information technology (IT) professionals.

The government first introduced the internet into Iran in the 1990s to support technological and scientific progress in an economy that had been badly damaged by eight years of war with Iraq. Until 2000, the private sector was the main driver of internet development. This changed under the government of the reformist President Mohammad Khatami (1997–2005), when the authorities invested heavily in expanding the internet infrastructure, but also began to clamp down on free expression online. Meanwhile, Supreme Leader Ali Khamenei first asserted control over the internet through a May 2001 decree that centralized service providers' connection to the international internet.[2]

OBSTACLES TO ACCESS

The Khatami administration worked to connect different cities with fiber-optic cables and otherwise improve infrastructure, resulting in a rapid expansion in internet use in the country. According to the International Telecommunication Union (ITU), there were 625,000 internet users in Iran at the beginning of 2000. By the end of Khatami's presidency in 2005, the number had increased to several million, spurred forward by the country's increasingly youthful demographics.

Present day statistics on the number of internet users in Iran are inconsistent and highly disputed, though most observers agree that usage continues to grow. According to the ITU, which receives statistics from the government on different information and communications technology (ICT) indicators, Iran's internet penetration rate was 21 percent by the end of 2011.[3] Other sources place penetration as low as 15 percent[4] or as high as 39 percent.[5] The

[2] "Country Profile—Iran," OpenNet Initiative, June 16, 2009, http://opennet.net/research/profiles/iran.
[3] International Telecommunication Union Database, "Internet 2010," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2010&RP_intLanguageID=1&RP_bitLiveData=False.
[4] A January 2011 survey conducted by the Iran Statistics Centre found the penetration rate to be almost 15 percent, or 11 million users, an increase of about 4 percent compared to the center's findings in 2010. "21.4 % of families have Internet access," Wimax News, March 11, 2011, http://wimaxnews.ir/NSite/FullStory/News/?Id=3190.

vast majority of these users (an estimated 94 percent) reside in urban centers, particularly Tehran, Shiraz, Mashhad, Esfahan, and Tabriz. Mobile phone use is significantly more widespread. The ITU estimates that there were 56 million users in 2011, for a penetration rate of 75 percent. However, this does not appear to take into consideration subscriptions from all providers, which would amount to approximately 85 million users, a penetration rate of over 100 percent.[6]

The cost of internet access in Iran remains very high and most users connect to the internet from home, meaning they are predominantly urban middle and upper class. Moreover, the speeds of internet connections in Iran are extremely slow. A recent study by the Iran Statistics Centre found that 84 percent of the country's users still use dial-up connections. Even for those subscribed to ADSL services, speeds remain slow. A government survey revealed that some ADSL subscribers (whose connections should be attaining 128 Kbps download speeds, the maximum speed permitted by the government for personal use) were only able to download at a dismal 6.1 Kbps.[7] According to the Director of Iran's Telecommunications Company (TCI), the government of President Mahmoud Ahmadinejad has halted planning for further expansion of the IT infrastructure, exacerbating this problem.[8]

The telecommunications system in Iran is tightly controlled by the government or related entities. In recent years, the role of the Islamic Revolutionary Guards Corps (IRGC)—a politically important branch of the security forces that also controls large sections of the economy—in the ICT sector has notably increased.[9] In September 2009, for example, the IRGC purchased a controlling stake in the TCI, the country's main provider of internet and mobile phone services. The Data and Communication Company (DCC), which operates under the TCI, retains a monopoly on internet traffic flowing in and out of Iran. Other providers must purchase bandwidth from the DCC. In March 2012, the DCC increased the price for private providers of broadband,[10] causing some observers to speculate that it intends to capture their market share and further increase its dominance of the information landscape. Direct access to the internet via satellite is only permitted to certain institutes, and is prohibited for personal use. The mobile phone market is similarly under state

[5] A survey conducted jointly by the U.S.-government funded Broadcasting Board of Governors and Gallup in March 2012, found that among the 2,000 respondents in 31 provinces, 39 percent had accessed the internet during the previous week. BBG Research Series Briefing, *Iran Media Use 2012*, June 12, 2012, http://www.bbg.gov/wp-content/media/2012/06/BBG-Iran-ppt.pdf.
[6] There are two main mobile service providers in Iran. No accumulative number of subscribers have been published, but there are reports of 54 million subscribers of MCI and 31 million for IranCell/MTN. A third mobile operator (Rightel) was also launched recently but had only 10,000 subscribers at the time of writing.
[7] "Average speed of Internet in Iran," ITNA, September 20, 2011, http://itna.ir/vdcj8mev.uqeh8zsffu.html#.
[8] "The 10th Government has ignored ICT," ITNA, May 14, 2011, http://itna.ir/vdcgnz9q.ak97w4prra.html.
[9] "The Revolutionary Guards is entering the IT market," Digarban, December 12, 2011, http://www.digarban.com/node/3715.
[10] "Internet price to increase in 2011," Entekhab, March 26, 2011, http://www.entekhab.ir/fa/news/22391.

influence. The second mobile operator, IranCell, is owned in part by a web of proxy companies controlled by the IRGC (there are a number of high profile IRGC ex-commanders among its management). The third operator, Rightel, was launched in early 2011. It too is a government-owned entity, but as of May 2012 had gained only a few thousand subscribers.

During the 2009 protests, the authorities used their control over the internet infrastructure to curb access by causing a massive drop in the speed of connectivity, making it difficult to conduct basic online activities. Ports used by instant-messaging and chat platforms were also tampered with and mobile phone text messaging was shut down nationwide for 40 days. Similar periodic disruptions continued in 2011 and early 2012 but appeared to be linked to adjustments applied to the content filtering system rather than an effort to thwart protests on sensitive dates.

There is no independent regulatory body for ICTs in Iran. The Communications Regulatory Authority (CRA) is responsible for telecommunications licensing. It is part of the ICT Ministry and its head is appointed by the minister.[11] In March 2012, the broader decision making process related to ICTs underwent a change, when Iran's Supreme Leader Khamenei issued a decree establishing "The Supreme Council on Cyberspace" (SCC). The SCC is intended to provide a centralized focal point for policy making and regulation of Iran's virtual space, effectively removing such authority from the executive, legislative and judiciary branches of the government and bringing it under Khamenei's direct control. Observers believed this reflected Khamenei's dwindling trust of President Ahmadinejad and hesitation to leave such an important area of policy under his authority.

LIMITS ON CONTENT

Internet filtering, which began toward the end of the Khatami presidency in 2005, has become more severe since June 2009. The authorities employ a centralized filtering system that can effectively block a website within a few hours across the entire network in Iran. Private internet service providers (ISPs) are forced to either use the bandwidth provided by the government or route their send traffic (which contains site-visit requests) through government-issued filtering boxes developed by software companies inside Iran. The boxes search for banned text strings—either keywords or domain names—in the URL requests submitted by users, and block access accordingly.

[11] Communications Regulatory Commission of Iran, accessed July 31, 2012, http://www.cra.ir/Portal/Home/.

Throughout 2011 and early 2012, the Iranian authorities continued to restrict access to tens of thousands of websites, particularly those of international news sources, the opposition Green Movement, ethnic and religious minorities, and human rights groups. Some previously accessible websites and blogs also began being blocked, including news sources like Yahoo News and Reuters.[12] Ahead of parliamentary elections in March 2012, the Office of the General Prosecutor threatened to block any website that published calls to boycott, protest, or question the credibility of the polls, a threat that was reportedly acted upon.[13] Websites addressing economic issues were also subject to censorship. In January 2012, shortly after the value of Iran's currency hit a record low against the dollar, the website Mesghal.ir, which provides real time reports on the value of the Rial against other currencies, was blocked.[14] Its manager was arrested and accused of reporting misinformation and causing the fluctuating exchange rates.[15]

The government's filtering also tracked tensions in foreign policy. In December 2011, the authorities blocked access to the website of the British Embassy in Tehran following a diplomatic crisis that led to the closure of the mission.[16] That same month, the United States' Virtual Embassy was blocked the day after being launched.[17]

Even websites operating within the official discourse have not escaped filtering. A number of websites and blogs belonging to Ahmadinejad supporters who publicly criticized some of his government's policies were blocked, reflecting the growing polarization within the regime. In May 2011, the website of Haft-e-Sobh (Seven in the Morning), a group close to Ahmadinejad, was blocked.[18]

As of May 2012, all major international social media tools like the social-networking site Facebook, the video-sharing portal YouTube, the microblogging service Twitter, and the photo-sharing application Flickr were blocked. The periodic disruption of access to services

[12] "Reuters and Yahoo News have been filtered," FardaNews, January 31, 2011, http://www.fardanews.com/fa/news/135558/%D8%B1%D9%88%DB%8C%D8%AA%D8%B1%D8%B2-%D9%88-%DB%8C%D8%A7%D9%87%D9%88-%D9%86%DB%8C%D9%88%D8%B2-%D9%81%DB%8C%D9%84%D8%AA%D8%B1-%D8%B4%D8%AF%D9%86%D8%AF.

[13] "The Iranian State warns the sites: don't joke with the election," BBC Persian, December 31, 2011, http://www.bbc.co.uk/persian/iran/2011/12/111231_l10_election_boycott_warning_majlis9th.shtml.

[14] "The Rial Drops, And Iran Blocks The News," Radio Liberty, January 9, 2012, http://www.rferl.org/content/rial_drops_iran_censors/24446672.html.

[15] "The webmaster of Mesghal has been arrested/The government tries to make excuses for the economic crisis," Saham News, February 5, 2012, http://sahamnews.net/1390/11/165722/.

[16] Saeed Kamali Dehghan, "Iran blocks access to British embassy website," The Guardian, December 22, 2011, http://www.guardian.co.uk/world/2011/dec/22/iran-blocks-access-british-embassy-website.

[17] "US Condemns Iran's Blockage of 'Virtual Embassy Tehran'," Payvand Iran News, August 12, 2011, http://www.payvand.com/news/11/dec/1077.html?utm_source=Payvand.com+List&utm_campaign=b6064ec252-RSS_EMAIL_CAMPAIGN&utm_medium=email.

[18] "Haft-e-Sobh, a website close to Ahmadinejad's team has been filtered," Digarban, June 2, 2011, http://digarban.com/node/1230.

based overseas—such as Google's fairly well-encrypted email and blogging platforms, Gmail and Blogger, or its new social network Google+—appear designed to frustrate users and eventually force them to seek more easily monitored alternatives based in Iran. Although many Iranians have been able to access the blocked platforms using various circumvention techniques, the authorities have actively worked to disrupt such efforts, forcing users to constantly search for new solutions.

The regime has also employed administrative measures to remove unwanted content from the web. The Computer Crime Law (CCL) makes service providers, such as blogging platforms, responsible for any content that appears on their sites. This has led to the suspension of blogs or shuttering of news websites hosted on platforms inside Iran, under orders from government officials. Blogfa, one of the main blogging platforms inside Iran, reportedly receives orders to shut down an average of 50 blogs each week, though on some occasions this has reached 10,000 blogs per week.[19] In other cases, website owners have been forced to register their sites with the Ministry of Culture and have then received requests to remove particular posts deemed unacceptable by the government. According to Alireza Shirazi, the founder and manager of Blogfa, such massive censorship has damaged the Iranian blogosphere by discouraging users from blogging.[20]

Many people have instead shifted to posting on social-networking platforms like Facebook, accessing the blocked site with the use of circumvention tools. Facebook is perceived to offer a safer environment for expressing views among a limited audience of contacts. Some individuals associated with the regime have sought to discourage this practice. In July 2011, the deputy director of the ministry in charge of IT development declared that linking to filtered websites in an online post could be considered "against the spirit of the law" and therefore punishable by a fine or imprisonment.[21] The Iranian Cyber Police seconded this warning in November 2011, stating that exchanging information on foreign social-networking sites could constitute a criminal act and lead to prosecution.[22] Speaking from a different perspective, in January 2012, an Iranian cleric declared Facebook to be un-Islamic and that membership constituted a sin.[23]

[19] Fanavaran, Alireza Shirazi, interviewed by Shabnam Kohanchi, "Filtering killed the indicators of blogosphere," December 17, 2011, http://www.itmen.ir/index.aspx?pid=10324&articleid=3954.
[20] Ibid.
[21] "The internet manager of Ministry of Culture: Iranian users should use Iranian social networks," Gerdab, July 27, 2011, http://www.gerdab.ir/fa/news/6652/%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86%DB%8C-%D8%A7%D8%B2-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%DB%8C-%D8%AF%D8%A7%D8%AE%D9%84%DB%8C-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%DA%A9%D9%86%D9%86%D8%AF.
[22] "Is being a member of social networks a crime?" Jahan News, November 17, 2011, http://www.jahannews.com/vdcdkk0fxyt0no6.2a2y.html.
[23] Amrutha Gayathri, "Muslim Cleric Says Facebook is Un-Islamic, Membership Sin," International Business Times, January 11, 2012, http://www.ibtimes.com/articles/280026/20120111/muslim-cleric-facebook-un-islamic-membership-sin.htm.

As with blocking, the targets of such censorship have included websites and blogs associated with high-ranking officials. In May 2011, the website of Kashan's Friday Prayer leader was taken offline after he revealed details about the conflict between Khamenei and Ahmadinejad.[24] The following month, the news website *MojmelNews* had its Iran-based servers shut down after it reported that Ahmadinejad was not cooperating with the reinstated Minister of Intelligence.[25] In December 2011, the website of influential cleric and ex-President Akbar Hashemi Rafsanjani was blocked and temporarily shut down;[26] Rafsanjani heads an advisory body to Supreme Leader Khamenei but has been openly critical of Ahmadinejad.

There have also been periodic reports that mobile phone text messages with banned keywords were being filtered, typically around politically sensitive events. Prior to parliamentary elections in March 2012, Iranian Member of Parliament Aliakbar Olya reported that mobile phone operators were blocking text messages containing the keywords "parliament," "provincial governors," "date," or "meeting."[27] In January 2012, around the time of the currency plunge, users reported that text messages containing the word "dollar" or "foreign currency" were also blocked.[28]

In an effort to show that content filtering is based on a legal framework and not arbitrary, institutions to oversee internet filtering have been created. The CCL enacted in 2009 upgraded the mandate of the Committee in Charge of Determining Unauthorized Websites, initially created in 2002. The committee is empowered to identify sites that carry forbidden content and report that information to the TCI and other major ISPs for blocking. The committee is headed by the prosecutor general and other members are representatives from 12 governmental bodies. The law also identifies the violations that might result in a website being marked for filtering. These are defined very broadly and range from insulting religious figures and government officials to distributing pornographic content and illegal circumvention tools.[29]

In practice, little information is available about the inner workings of the committee, and censorship decisions are often arbitrary and nontransparent. According to the law, the committee should meet biweekly to decide on any website bans, but a TCI vice president

[24] "Kashan's Friday prayer leader's website has disappeared," Aftabnews, June 1, 2011, http://aftabnews.ir/vdccx4qs42bqie8.ala2.html.
[25] "Majmal News website has become out of rich," Digarban, June 29, 2011, http://www.digarban.com/node/1499.
[26] "Iran ex-President Rafsanjani's website blocked," BBC News, December 30, 2011, http://www.bbc.co.uk/news/world-middle-east-16368472.
[27] "SMS services are going to be filtered?!," ITNA, October 30, 2011, http://itna.ir/vdcdnf0x.yt0zx6a22y.html.
[28] "UPDATE 1-Iran rial slides, 'dollar' text messages appear blocked," Reuters, January 10, 2012, http://www.reuters.com/article/2012/01/10/iran-currency-idUSL6E8CA2MQ20120110.
[29] "12 memebers of Committee in Charge of Determining Unauthorized Sites," Weblognews, December 16, 2009, http://weblognews.ir/1388/09/mediablog/5740/.

said in 2010 that the rate of filtering was 200 to 300 websites per day, meaning the bulk of filtering decisions are likely made upon discovery of objectionable content, or by a small technical team. This would leave the committee to decide on only the most controversial blocking decisions. In addition, owners of websites registered with the Ministry of Culture have complained that they received no explanation when their websites were filtered.[30] Among them was Zahra-hb, a well-known conservative blogger, whose blog was blocked in March 2012 without notification.[31] The authorities claim there is a procedure for disputing filtering decisions. However, the process is highly inefficient, and even conservative bloggers have failed to have their webpages unblocked by lodging complaints.[32] Moreover, the dispute process requires the website owner to disclose his or her personal information and accept responsibility for any misconduct in the future, a commitment that few are willing to make given the risk of severe punishment.

Alongside the expansion of existing controls, in July 2011, the Iranian authorities began referring to the creation of a National Internet. Iran's fifth development plan from June 2010, which the government is obliged to implement, provides for the establishment of a "National Information Network," although the plan does not specify the objectives of creating it. According to the Minister of ICT, the objectives include protecting the exchange of data within the country from security breaches, monitoring emails, and creating a "safe internet."[33] The particular technical specifications of the plan remain unclear and officials have used various names to describe the initiative, including a "Halal" or "Clean" internet, while others have issued conflicting statements about the project's end result. Media coverage and public discussions have often described the National Internet as a national intranet that, upon its launch, would cut off users inside Iran from the global internet. However, according to some experts, the cut off may not be absolute. Dr. Siavash Shahshahani, known as the founder of the internet in Iran, was quoted as comparing the initiative's outcome to China's censorship model, saying: "What is … referred to as the National Internet means that we will have good and expansive local connections but all our foreign connections are to pass through a controllable channel."[34]

[30] "The News stie's reporter will be insured," Hamshahri Online, November 1, 2011, http://www.hamshahrionline.ir/news-150108.aspx.
[31] Zahra HB, "When the filtering purposes are being violated," 30Mail (blog), April 7, 2012, http://30mail.net/weblog/2012/apr/07/sat/16886.
[32] "On filtering of Ahestan," Ahestan (blog), January 15, 2010, http://ahestan.wordpress.com/2010/01/15/ahestan.
[33] "Iran to launch national data network," Press TV, August 10, 2011, http://www.presstv.ir/detail/193306.html; "The ICT Minister: email management is one of the aims of launching national internet," Radio Farda, July 27, 2011, http://www.radiofarda.com/content/f10_iran_information_minister_managing_emails_collecting_information_national_internet/24278324.html.
[34] "The controversial comment of the founder of Internet in Iran about national internet," Jam News, March 5, 2012, http://www.jamnews.ir/NSite/FullStory/News/?Id=65655.

Although the final goal of the National Internet project remains unclear, available evidence indicates that the ICT Ministry has been tasked with implementing it in several phases, the initial of which appear to have already been put in place.[35] The first phase involves an upgrade in filtering capacity to enable more nuanced management, blockage, monitoring, and redirecting of traffic. On numerous occasions throughout 2011, users across Iran reported the slowing of internet speeds and heightened blockage of circumvention tools. Although no official explanations were offered, a number of news websites suggested the disruptions were related to an upgrade of the internet infrastructure.[36] Some observers noted that a growing percentage of domestic internet traffic was being routed only through Iranian servers rather than external ones, as would normally be the case. Then, in the run-up to the 2012 parliamentary elections, the authorities blocked all encrypted international traffic for several days. This confirmed that the government had developed a new capability, using sophisticated deep-packet inspection technologies to recognize different types of traffic and throttle them as deemed necessary. For instance, during the pre-election disruptions, traffic to services using the Secure Sockets Layer (SSL) protocol and based outside Iran was effectively blocked, restricting users' ability to access applications like Gmail. At the same time, however, users encountered no problems accessing online banking services within Iran that also run on SSL (displaying addresses beginning with "https"). Users also complained of trouble using virtual private networks (VPNs) to circumvent censorship. This new technical capacity will allow the Iranian authorities to control access to particular international communication flows during periods of political unrest without the need to shut down all domestic services or the entire network.

The next stage of the National Internet project is the mandatory registration of internet protocol (IP) addresses assigned to users (see "Violations of User Rights"). The final stage for implementing the National Internet is to move the hosting of government-approved websites to servers based inside the country and to launch Iranian equivalents of major online services like email, social-networking sites, and search engines. According to Iran's Deputy Minister of ICT, the government has already moved more than 90 percent of its websites to providers based inside the country and is now pressuring privately owned websites to follow suit.[37] Compliance has been limited, however, primarily because hosting services offered by Iranian companies are significantly more expensive than those of their overseas competitors.

[35] "Internet for all, internet for some," ITNA, July 16, 2011, http://www.itna.ir/vdcbfwb8.rhbw5piuur.html.
[36] "Continued disruption in the Internet," Kaleme, December 8, 2011, http://www.kaleme.com/1390/09/17/klm-82762/.
[37] "The ministry promises 20 Mbps internet again," Mashregh News, July 23, 2011, http://www.mashreghnews.ir/fa/news/59736/%D9%88%D8%B9%D8%AF%D9%87-%D9%85%D8%AC%D8%AF%D8%AF-%D9%88%D8%B2%DB%8C%D8%B1-%D8%AF%D8%B1%D9%85%D9%88%D8%B1%D8%AF-%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-20%D9%85%DA%AF%D8%A7%D8%A8%DB%8C%D8%AA%DB%8C.

Launching viable national equivalents of major online services, as has happened in China, is considered to be the most critical stage of rolling out the National Internet. Iranian users will then be effectively cut off from the global internet and transnational conversations. However, successfully implementing this stage will be challenging for various reasons. First, several equivalents of major online services have been launched since 2010 but have subsequently gone out of business after failing to attract large numbers of users due to poor design. Second, international sanctions on Iran over its nuclear program have limited the government's ability to purchase the equipment required to run data centers on the scale needed to host a national email service, for example.[38] Existing data centers are incapable of servicing a large number of users. The Iranian authorities have been trying to entice the private sector to get involved, but due to a lack of experience and expertise in running large-scale web services, private firms have also not managed to get many popular platforms off the ground.

In addition to censorship, the state counters critical content and online organizing efforts by extending regime propaganda into the digital sphere. There are at least 400 news websites either directly or indirectly supported by the state. They seek to set the agenda by providing pro-government commentary or publishing rumors. In April 2011, an official from the Ministry of Culture and Islamic Guidance stated that 40 firms had received over US$56 million from the ministry to produce digital content.[39] There have also been a large number of government-backed initiatives to promote blogging among its supporters and members of the Basij paramilitary group. In July 2011, the head of the Basij said there were three million members active online and praised their activities.[40] Despite this large contingent, the content produced is limited in quality and quantity, constraining its practical influence over online discourse. In response, paramilitary commanders have called for the allocation of more resources, recruitment of another ten million Basiji bloggers, and the creation of a cyber army of loyalist content producers to fight the "Soft War."[41]

Self-censorship is extensive, particularly on political matters. The widespread arrests and harsh sentences meted out to reporters and activists after the 2009 elections, as well as

[38] "Persian email service, Chaapaar will be launched in December," IRNA, September 27, 2011, http://www.irna.ir/NewsShow.aspx?NID=30583255.
[39] "Reuters has Iran accreditation revoked for offensive headline; Cyber Council: 'use cyberspace to further the regime'; Cyber-defense curriculum to be introduced in some graduate level programs; OFAC lifts some IT sanctions-what does it mean for Iranians?" Iran Media Programme, April 2, 2012, http://www.iranmediaresearch.org/en/newsletter/12/04/02/901.
[40] "Basij have had large and effective measures in cyberspace," Fars News, October 11, 2011, http://www.farsnews.com/newstext.php?nn=13900719001180.
[41] "Basij should be equipped to deal with the soft war," Fars News, November 16, 2011, http://www.farsnews.com/newstext.php?nn=13900825001411.;
"10 million Basij should have 10 million blogs," Fars News, July 9, 2012, http://www.farsnews.com/newstext.php?nn=13900624000195; "The first Iranian cyber army to be launched," IT Analyze, February 21, 2012, http://itanalyze.com/news/2012/02/21/16506.php.

perceptions of pervasive surveillance, have increased fear among online journalists and bloggers. Many of them either abandoned their online activities or use pseudonyms. The result has been a palpable drop in the amount of original content being produced by users based inside the country.

Furthermore, the majority of independent content producers lack the financial resources to operate in such a hostile environment. The online advertising market in Iran is exclusively limited to apolitical and pro-government websites. Even businesses based outside Iran avoid political websites to maintain trading relationships with the country. Although the United States adjusted its sanctions against Iran to enable American internet companies to provide services to Iranian users, Google Advertising does not recognize Persian as one of the languages in its system, disadvantaging Persian content producers.[42]

Despite all of these limitations, the internet remains the only means available for Iranian citizens and dissenters to obtain news and organize themselves. Traditional media outlets are tightly controlled by the authorities, and satellite broadcasting from outside Iran is subjected to heavy jamming. Paralleling the rise in censorship, the use of VPNs, proxies, and other circumvention tools has also grown dramatically since 2009. Data from AnchorFree, a popular VPN distributor, shows that usage of its services in Iran increased ten-fold between July 2010 and July 2011, reaching over 360,000 users by that time.[43] This increase occurred despite repeated statements by the Minister of ICT that the use of circumvention tools and VPNs is a punishable crime.[44] Nevertheless, compared to the high level of online organization and mobilization in 2009 and 2010, one of the most notable changes since January 2011 has been the sharp drop in offline activities sparked by online communications.

VIOLATIONS OF USER RIGHTS

Iranian internet users suffer from routine surveillance, harassment, and the threat of imprisonment for their online activities, particularly those critical of the authorities. The constitution provides for limited freedom of opinion and expression, but numerous, haphazardly enforced laws restrict these rights in practice. The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or

[42] Jamal Abdi, "Obama Norooz promise a good step, more needed to ensure U.S. not part of 'Electronic Curtain,'" NIAC InSight, March 21, 2012, http://www.niacinsight.com/2012/03/21/obama-promises-to-ease-internet-restrictions-in-norooz-message/.

[43] Elizabeth Flock, "Iranians using proxy servers 10 times more than they were last year," Washington Post, April 15, 2012, http://www.washingtonpost.com/blogs/blogpost/post/iranians-using-proxy-servers-10-times-more-than-they-were-last-year/2012/02/15/gIQA4LFMGR_blog.html.

[44] "Are Millions Of Iranians Criminals?" Radio Liberty, October 25, 2011, http://www.rferl.org/content/iran_internet_antifiltering_tools_censorship/24370376.html.

detrimental to public rights, none of which are clearly defined. The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize critical opinions. The 2009 Computer Crime Law (CCL) identifies punishments for spying, hacking, piracy, phishing, libel, and publishing materials deemed to damage "public morality" or to be a "dissemination of lies."[45] Punishments mandated in the CCL are severe. They include the death penalty for offenses against public morality and chastity, as well as long prison sentences, draconian fines, and penalties for service providers who fail to enforce government content restrictions.

Since June 2009, the authorities have cracked down on online activism through various forms of judicial and extralegal intimidation. An increasing number of bloggers have been threatened, arrested, tortured, kept in solitary confinement, and denied medical care, while others have been formally tried and convicted. At least 50 bloggers and online activists were arrested in 2009 and 2010. Although the number of new arrests decreased in 2011, many individuals detained during the previous two years were sentenced, often harshly. Three bloggers and IT professionals—Saeed Malekpour, Vahid Asghari and Ahmad Reza Hasempour—were sentenced to death between October 2011 and January 2012 on various questionable charges. Malekpour, for example, was prosecuted because a software program he had designed was used to upload pornography, although it was done without his knowledge.[46] The Committee to Protect Journalists speculated that the three were targeted because of their technical knowledge and ability to assist in the building and hosting of independent websites.[47] Other bloggers have been sentenced to prison terms of up to 20 years. Blogger Hossein Ronaghi-Maleki continues to serve a 15-year sentence imposed in December 2009 for "spreading propaganda against the regime" and insulting the Supreme Leader.[48] In June 2011, Hossein Derakhsan, considered the father of the Iranian blogosphere, lost his appeal against a 19-year sentence imposed on charges of cooperating with hostile countries, spreading propaganda against the regime, and insulting Islamic thought and religious figures. [49]

[45] *Islamic Republic of Iran: Computer Crimes Law Article 19*, January 30, 2012, www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf.

[46] Saeed Malekpour, interviewed by Olivia Ward, "Saeed Malekpour: A Canadian on Iran's death row," The Star, February 18, 2012, http://www.thestar.com/news/world/article/1132483--a-canadian-on-iran-s-death-row; Amnesty International, "Iran must halt execution of web programmer," January 19, 2012, http://www.amnesty.org/en/news/iran-must-halt-execution-web-programmer-2012-01-19.

[47] Danny O'Brien, "Online publishers, developers sentenced to death in Iran," Committee to Protect Journalists, January 20, 2012, http://cpj.org/internet/2012/01/online-publishers-and-developers-sentenced-to-deat.php.

[48] "Iranian blogger on hunger strike close to death, warn fellow prisoners," The Guardian, June 6, 2012, http://www.guardian.co.uk/world/iran-blog/2012/jun/06/iran-blogger-hossein-ronaghi-maleki-hunger-strike.

[49] "Iranian blogger loses appeal against 19-year sentence," The Guardian, June 9, 2011, http://www.guardian.co.uk/world/2011/jun/09/jailed-iran-blogger-loses-appeal.

Despite the relative decrease in new arrests, several bloggers and online activists were detained in 2011 and subsequently sentenced to prison. In February 2011, the Ministry of Intelligence arrested eight bloggers who had been critically discussing Islamic doctrine over the internet. In January 2012, they were all sentenced to prison terms ranging from five to nine years.[50] In another round of arrests in early 2012, security forces detained at least six journalists and bloggers in what appeared to be a preemptive measure to thwart protests surrounding the March parliamentary elections.[51]

Members of ethnic and religious minorities have also faced harsh punishment for expressing their views online or using websites to disseminate information. In May 2011, at least 30 Baha'is were arrested in coordinated raids in Tehran, Karaj, Isfahan, and Shiraz. The detained individuals were involved in an online university initiative to provide higher education to Baha'i students.[52] In September 2011, the administrators of a website related to the Daraawiish Sufi Muslim group were arrested.[53] In December, a user in Kurdistan province was reportedly arrested by police on charges of insulting officials and promoting an opposition group on social-networking sites.[54] In June 2011, Sakhi Reigi, a blogger from the Baluch ethnic minority was sentenced to 20 years in prison for acting against national security, a charge commonly used to jail members of ethnic minorities advocating for more rights.[55]

In other instances, ordinary users were detained for engaging in apolitical online activities deemed socially inappropriate by the regime. In March 2012, the authorities arrested the administrators of a soccer betting website, as betting is prohibited under Islam.[56] In September 2011, a handful of people who tried to organize a water fight at a Tehran park

[50] "8 people imprisoned in Iran for holding discussion on Islam in internet," APA, January 21, 2012, http://en.apa.az/news.php?id=164113.; "Iran sentences 8 people to prison for expressing religious beliefs in internet social network," HARDIP, January 20, 2012, http://hrdip.com/iran-sentences-8-people-to-prison-for-expressing-religious-beliefs-in-internet-social-network/.

[51] Rick Gladstone and Artin Afkhami, "Pattern of Intimidation Is Seen in Arrests of Iranian Journalists and Bloggers," The New York Times, January 25, 2012, http://www.nytimes.com/2012/01/26/world/middleeast/iran-steps-up-arrests-of-journalists-and-bloggers.html?_r=1&scp=1&sq=afkhami&st=cse.

[52] "Government Attacks Baha'i Online University, Detains 30 Instructors," International Campaign for Human Rights in Iran, May 23, 2011, http://www.iranhumanrights.org/2011/05/bahai-university-attacked/.

[53] "The managers of Majzoobanoor website have been arrested," 30Mail (blog), September 5, 2011, http://www.30mail.net/news/2011/sep/05/mon/11602.

[54] "The publisher of offensive materials to national authorities has been arrested," ISNA, November 27, 2011, http://www.isna.ir/isna/NewsView.aspx?ID=News-1899523.

[55] "Sakhi Rigi, Baluch blogger, was sentenced to 20 years imprisonment," Green Waves News, June 8, 2012, http://www.greenwavenews.com/1390/03/18/%D9%85%D8%AD%DA%A9%D9%88%D9%85%D9%8A%D8%AA-%D8%B3%D8%AE%DB%8C-%D8%B1%D9%8A%DA%AF%DB%8C%D8%8C-%D9%88%D8%A8%D9%84%D8%A7%DA%AF%E2%80%8C%D9%86%D9%88%D9%8A%D8%B3-%D8%A8%D9%84%D9%88%DA%86-%D8%A8%D9%87/.

[56] "Feta police will react to disturbing the public opinion," IT Analyze, March 26, 2012, http://itanalyze.com/news/2012/03/26/16968.php.

over Facebook were detained.[57] In another Facebook-related case, Iranian authorities arrested two men and two women in January 2012 on charges of "promoting vulgarity and corruption." The four had maintained a page on the social-networking site that acted as an online beauty contest, to which thousands of young people posted glamorous photos of themselves. [58]

The scale and arbitrariness of such arrests, as well as the harsh punishments meted out, have created a climate of fear among Iranian internet users. As a result, a large number of bloggers, journalists, and activists have gone underground or fled the country to seek political asylum in neighboring countries, mainly Turkey.[59] Meanwhile, ordinary users tread carefully when communicating online, unclear of what kinds of activities might inadvertently put them at risk.

Since early 2011, the authorities have increased technical measures to curb anonymous communications. On several occasions, around politically sensitive dates, ISPs blocked the SSL protocol, denying millions of Iranians secure access to their email addresses. In a similar move that also affected internet users outside of Iran, two international companies responsible for issuing digital certificates for popular online services like Gmail, Yahoo, Hotmail and Skype were hacked during 2011.[60] The precise number of users whose privacy was compromised remains unclear, but the forged certificates could have been used to potentially spy on some 300,000 users in Iran.[61] In September 2011, Google issued a warning to its users from Iran urging them to change their passwords as a precaution.[62]

Such blocks have generated criticism from within the government. In March 2012, Rasool Jaafarian, an influential cleric and director of the parliamentary library criticized the obstacles imposed on accessing informational websites, arguing that this has caused frustration among researchers because there is no domestic replacement for such services.[63] Iranian Member of Parliament (MP) Ahmad Tavakoli seconded this assessment, warning that

[57] "Iran makes arrests over new water fight attempt," Iran Focus, September 5, 2011, http://www.iranfocus.com/en/index.php?option=com_content&view=article&id=23670:iran-makes-arrests-over-new-water-fight-attempt-&catid=4:iran-general&Itemid=26.
[58] J. David Goodman, "Iranian Authorities Arrest Four Over Facebook Beauty Contest," The New York Times, January 31, 2012, http://thelede.blogs.nytimes.com/2012/01/31/iranian-authorities-arrest-four-over-facebook-beauty-contest/.
[59] "Iran and Cuba have the most exiled journalists," BBC Persian, June 20, 2012, http://www.bbc.co.uk/persian/iran/2011/06/110620_l39_cpj_iran_cuba_journalists_exile.shtml.
[60] The first hacking incident was of Comodo which took place in March 2011 and the second incident was the hacking of DigiNator which was made public in August 2011.
[61] Byron Acohido, "Authenticity of Web pages comes under attack," USA Today, September 29, 2011, http://www.usatoday.com/tech/news/story/2011-09-27/webpage-hackers/50575024/1.
[62] "Google issues warning to Iranian Gmail users," The Hindu, September 13, 2011, http://www.thehindu.com/sci-tech/article2449951.ece.
[63] "Internet disconnection and playing with the passion and talent of youth," Khabar Online, February 20, 2012, http://www.khabaronline.ir/detail/199918/weblog/jafarian.

the blockage of online services using the SSL protocol was creating widespread discontent that could be very costly for the regime, as more users seek out how to circumvent censorship and render the blocking of other sites ineffective.[64]

The Iranian authorities have taken a range of measures to monitor online communications and use them as a basis for criminal punishment. A number of protesters put on trial after the 2009 election were indicted for their activities on Facebook and Balatarin, a Persian content-sharing site. Many arrested activists reported that interrogators had confronted them with copies of their emails, asked them to provide the passwords to their Facebook accounts, and questioned them extensively on their relationships with individuals on their "friends" list. The authorities actively exploited the fear created by these reports, claiming that they had access to all the email and text messages exchanged in Iran.

The CCL obliges ISPs to record all the data exchanged by their users for a period of six months, but it is not clear whether the security services have the technical ability to process all this data. When purchasing a mobile phone subscription or prepaid SIM card, users must present identification, facilitating the authorities' ability to track down the authors and recipients of specific messages. Despite international legal restrictions placed on the selling of surveillance equipment to the Iranian government, in 2011 there were numerous media reports that Chinese and some Western companies have been providing the Iranian authorities with technology to monitor citizens' digital activities. Specifically, investigative reports by Reuters and the *Wall Street Journal* found that Huawei Technologies[65] and ZTE Corporation,[66] both Chinese firms, were key providers of surveillance technology to Iran's government, allegations both companies have denied.

As noted above, the second stage of the National Internet plan involves the mandatory registration of IP addresses. Bill 106 issued by the Communications Regulatory Authority in March 2012 requires the registration of all of the IP addresses in use inside Iran, in order to organize and systematize them beyond the data already collected. Implementing such registration will allow the authorities to more to track users' online activities even more thoroughly.

[64] "Iranian MP denounces internet service disruptions," Payvand, April 13, 2012, http://www.payvand.com/news/12/feb/1135.html?utm_source=Payvand.com+List&utm_campaign=128035d177-RSS_EMAIL_CAMPAIGN&utm_medium=email.

[65] Steve Stecklow, Farnaz Fassihi, and Loretta Chao, "Chinese Tech Giant Aids Iran," The Wall Street Journal, October 27, 2011, http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html.

[66] "UANI Calls on Chinese Telecom Giant ZTE to Withdraw from Iran," Market Watch, press release, March 26, 2012, http://www.telecomyou.com/newscenter/news/uani-calls-on-chinese-telecom-giant-zte-to-withdraw-from-iran-marketwatch-press-release.

In January 2011, the government announced new regulations that require customers of cybercafes to provide personal information (such as their name, father's name, national ID number, and telephone number) before using a computer. Cafe owners are required to keep such information, as well as customers' browsing history, for six months. They are also required to install closed-circuit surveillance cameras and retain the video recordings for six months.[67] The regulations came into effect in March 2012.

Filtering and physical intimidation are supplemented by hacking and distributed denial-of-service (DDoS) attacks on the websites of government critics, including leading opposition figures. In the days after the disputed 2009 presidential election, many of the news websites set up by supporters of opposition candidates were taken offline through intense DDoS attacks. Technical evidence confirmed that government-owned IP addresses were used to launch the attacks.[68] Other websites were rendered either permanently or temporarily unavailable by means of hacking, primarily by a group calling itself the Iranian Cyber Army. This phenomenon continued in 2011 and early 2012 but on a smaller scale. In March 2012, for instance, the Iran Cyber Army hacked the website of the Association of Combatant Clerics, a reformist organization under the leadership of former president Mohammad Khatami, and the Baran Foundation, another organization linked to Khatami.[69]

A number of non-Iranian sites were targeted by more sophisticated attacks. The domain of the U.S. government-funded Persian service of Voice of America was hijacked by the Iranian Cyber Army in February 2011. Similarly, the British Broadcasting Corporation (BBC) reported a "sophisticated cyber-attack" in March 2012. It was believed to be linked to other Iranian efforts during that time to disrupt the BBC Persian Service.[70]

Initially, there was some speculation about the connection between the Iranian Cyber Army and the Iranian authorities. In May 2010, however, Iranian officials confirmed these suspicions by publicly announcing that the Iranian Cyber Army was under the command of the IRGC.[71] Since then, IRGC commanders have explicitly welcomed hackers willing to "work for the goals of the Islamic Republic."[72] In a sign of the further institutionalization of

[67] Golnaz Esfandiari, "Iran Announces New Restrictions For Internet Cafes," Payvand, January 5, 2012, http://www.payvand.com/news/12/jan/1048.html?utm_source=Payvand.com+List&utm_campaign=d6730c3065-RSS_EMAIL_CAMPAIGN&utm_medium=email.
[68] Norooz News, "Norooz is revealing the names of 4 governmental entities behind the attacks against reformist websites," October 17, 2010.
[69] "Bonyad Baran and Majma rohanioun's website have been hacked," Radio Farda, February 27, 2012, http://www.radiofarda.com/content/f12_two_khatami_related_sites_hacked/24497610.html.
[70] "Cyber-attack on BBC leads to suspicion of Iran's involvement," BBC News, March 14, 2012, http://www.bbc.co.uk/news/technology-17365416.
[71] "IRGC has formed the second cyber army in the world," Fars News, May 20, 2010, http://www.farsnews.com/newstext.php?nn=8902300353.
[72] "Iran Says It Welcomes Hackers Who Work For Islamic Republic," Radio Liberty, March 7, 2011, http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html.

such efforts, an IRGC commander reported in November 2011 that the organization had established two Cyber War Centers and organized 2,000 officers to take part in the regime's Cyber War activities, which may include both hacking and production of pro-regime online content.

ITALY

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	6	4
Limits on Content (0-35)	8	7
Violations of User Rights (0-40)	12	12
Total (0-100)	**26**	**23**

* 0=most free, 100=least free

POPULATION: 61 million
INTERNET PENETRATION 2011: 57 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Italy's internet penetration rate—which stood at approximately 57 percent at the end of 2011—lags behind many other European countries. Mobile telephone usage is ubiquitous, however, and internet access via mobile phones has grown significantly in recent years. Italian authorities do not generally engage in political censorship of online speech, and, as in previous years, no bloggers were imprisoned as of mid-2012. In 2011, several decrees that posed a challenge to internet freedom in Italy either expired or were put on hold. In addition, a number of judicial decisions asserted that intermediaries are not liable for the content posted by users. Despite these positive developments, some government efforts to restrict political content were documented, including the shuttering of a well-known blog. Moreover, overbroad interpretations of liability in defamation or intellectual property rights cases resulted in unusual judicial decisions and disproportionate burdens placed on online news providers.

The push to restrict internet freedom in recent years had stemmed in part from the media ownership structure in Italy. Former Prime Minister Silvio Berlusconi owns, directly and indirectly, a large private media conglomerate, and his previous political position also gave him significant influence over the appointment of state television officials and telecommunications regulators. Such financial and editorial dominance over the broadcast media created an incentive for the country's leadership to restrict the free flow of information online, whether for political reasons or to influence the competition for viewers arising from online video. Berlusconi's November 2011 resignation and replacement by

Mario Monti changed these dynamics and appeared to reduce the government's pressure to restrict online communications.

A group of nuclear physicists created Italy's first computer network in 1980, with the intent of connecting all nuclear research institutes in the country. At the beginning, the internet was just one of several packet-switching networks that coexisted in Italy. The dominant telecommunications firm at the time, Telecom Italia, tried to impose its privately owned system, while various center-left governments, aware of the importance of interconnectivity, supported integration among the networks. Ultimately, the adaptability and simplicity of the internet prevailed. Access to the internet was available to private users after 1995, and the number of internet service providers (ISPs) soared within a short period of time. Among the remaining obstacles to greater internet penetration include a lack of familiarity with computers and with the English language, as well as the dominance of commercial television and the diversion of consumers' telecommunications spending to mobile telephony.

OBSTACLES TO ACCESS

Since the 1990s, the Italian government has supported the internet as a catalyst for economic growth, increased tourism, reduced communication costs, and more efficient government operations. According to the International Telecommunication Union (ITU), Italy had an internet penetration rate of 56.8 percent at the end of 2011, an increase from 38 percent in 2006.[1] While Italy's internet penetration rate is higher than the global average, it is lower than the overall rate in Western Europe. The relatively low penetration rate is not due to infrastructural limitations as much as unfamiliarity with the internet among the older generations and a general affinity for mobile phone devices rather than desktop computers.

The main point of internet access is the home, with some 22 million people using home connections at least once a month, as of October 2011.[2] The workplace is the second most common access point, followed by schools and universities. Less than half of Italy's internet users are female, though women comprise 55 percent of new users.[3] Cost is not a significant

[1] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011 & 2006, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[2] Giancarlo Livraghi, ed., "Dati sull'internet in Italia" [Data on the Internet in Italy], accessed February 20, 2012, http://www.gandalf.it/dati/dati3.htm.

[3] Ibid.

barrier to access. The price for a broadband connection may range from €20 to €40 (US$26-52) per month, compared to average monthly per capita income of around US$2,600.[4]

Access to the internet for private users is offered by 13 different ISPs. Telecom Italia has the largest share of the market, followed by Vodafone, Fastweb, and Tiscali. Telecom Italia owns the physical network, but it is required by European Union (EU) legislation to provide fair access to competitors.[5] ADSL broadband connections are available on about 96 percent of Italy's territory.[6] This is the basic service and it covers the whole territory. However, the faster broadband subscription rate is still relatively low (22 percent), as not all internet subscribers opt for higher speeds.[7] Meanwhile, fiber-optic cables remain underdeveloped. In 2010, the three large telecommunications operators Fastweb, Wind, and Vodafone Italia, announced plans to invest €2.5 billion (US$3.3 billion) over a five-year period to connect 15 of Italy's largest cities using fiber-optic cable. Telecom Italia announced a similar plan of its own to invest €9 billion (US$11.8 billion) in infrastructure. These plans have subsequently been put on hold, however, as Italy faces the most serious financial crisis in its modern history. Nevertheless, in February 2012, the government of Prime Minister Mario Monti launched a "Digital Agenda" initiative, which aims to expand broadband access and e-government efforts.[8] As of May 2012, few additional details of the program were available.

Mobile phone use is much more widespread than internet access, with the penetration rate reaching 152 percent in 2011.[9] The majority of subscriptions are prepaid. Telecom Italia

[4] "Broadband—Italy," Socialtext, accessed March 4, 2011, https://www.socialtext.net/broadband/index.cgi?italy; "Italy," Population Reference Bureau, accessed August 21, 2012, http://www.prb.org/DataFinder/Geography/Data.aspx?loc=453.

[5] Lorenzo Pupillo, *Duct and Pole Sharing: An Operator's Perspective* (Rome: Telecom Italia, April 10, 2008), slide 14, http://www.oecd.org/dataoecd/35/61/40460866.pdf (site discontinued).

[6] "Domestic Market," Telecom Italia, November 7, 2011, http://www.telecomitalia.com/tit/en/about-us/profile/domestic-market.html.

[7] "OECD Key ICT indicators, Broadband subscribers per 100 inhabitants in OECD countries," OECD, last updated on June 23, 2011, http://www.oecd.org/internet/broadbandandtelecom/oecdkeyictindicators.htm; "OECD Key ICT indicators, Availability of Digital Subscriber Lines (DSL) in OECD countries," OECD, last updated on June 30, 2011; Including portable and hand-held devices; "OECD Key ICT indicators, Households with access to a home computer," OECD, last updated on November 9, 2011; International Telecommunication Union (ITU), *Measuring the Information Society 2011* (Geneva: ITU, 2011), p.152; "OECD Key ITC indicators, Availability of Digital Subscriber Lines (DSL) in OECD countries," OECD, last updated on June 30, 2011, http://www.oecd.org/document/23/0,3746,en_2649_34449_33987543_1_1_1_1,00.html; "Including portable and hand-held devices; OECD Key ITC indicators "Households with access to a home computer," OECD, last updated on November 9, 2011; ITU, *Measuring the Information Society 2011,* p.152.

[8] Riccardo Luna, "'Migliaia di aziene al via I giovani imparino a creare lavoro'" [Thousands of companies launch and young people learn to create jobs], La Repubblica, February 6, 2012, http://www.repubblica.it/politica/2012/02/06/news/profumo_piano_digitale-29408048/; "Profumo: 'Priorità Internet per tutti'" [Profumo: Priority internet for all], Corriere delle Comunicazioni, February 6, 2012, http://www.corrierecomunicazioni.it/pa-digitale/13686_profumo-priorita-internet-per-tutti.htm; Andrea Di Maio, "Italy and its Digital Agenda: New Government, Old Risks," Gartner Blog, February 9, 2012, http://blogs.gartner.com/andrea_dimaio/2012/02/09/italy-and-its-digital-agenda-new-government-old-risks/

[9] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

Mobile (TIM), Vodafone, Wind, and 3 Italia are the major carriers, and all of them operate third-generation (3G) networks. Access to the mobile internet has been increasing in recent years, and as of 2011, some 59.4 percent of internet users reported accessing the internet through their smart phones.[10] As elsewhere, sales of tablet computers have been on the rise among the younger generation since 2010 and are likely to keep growing in the coming years.

In a positive development, the year 2011 witnessed the final demise of the Pisano decree, a regulation requiring businesses to obtain a license from the police in order to offer WiFi access to customers. The decree also required users to produce identification documents to access WiFi in public places and for operators to preserve records of internet use. The measures were instituted for security reasons in the wake of terrorist bombings in London in 2005 and were renewed annually over the next several years. They were widely viewed as having stunted the spread of WiFi in Italy, as many businesses chose not to offer such services given the added nuisance and cost involved in complying with the decree. In November 2010, the government announced that it would abolish the decree and remove restrictions on public access to WiFi starting in January 2011. In practice, it was only in December 2011 under the new Monti government, that the Pisano decree was finally allowed to expire.[11]

The main regulatory body for telecommunications is the Authority for Communications Security (AGCOM), an independent agency that is accountable to the parliament. Its responsibilities include providing access to networks, protecting intellectual property rights, regulating advertisements, and overseeing public broadcasting. The parliament's majority party appoints AGCOM's president, and commissioners have been known to come under pressure from the government to take certain actions regarding television broadcasts, particularly when Berlusconi was prime minister.[12] Although Berlusconi resigned from his position in November 2011, concerns remained that his significant economic and political influence could still effect government decisions related to audio-visual broadcasts, including the allocation of digital television frequencies.

Another important player in the field of communications is the Italian Data Protection Authority (DPA). Set up in 1997, the DPA has a staff of more than 100 people, and four of its main members are elected by parliament for seven-year terms. The DPA is tasked with supervising compliance by both governmental and nongovernmental entities with data

[10] ITU, *Measuring the Information Society 2011,* p.154, http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf.
[11] "Decreto- Legge 29 dicembre 2011, n. 216," Gazzetta Ufficiale, December 29, 2011, www.gazzettaufficiale.biz/atti/2011/20110302/011G0260.htm.
[12] Michael Day, "Silvio Berlusconi caught out trying to stifle media," The Independent, March 18, 2010, http://www.independent.co.uk/news/world/europe/berlusconi-caught-out-trying-to-stifle-media-1923147.html .

protection laws, and "banning or blocking processing operations that are liable to cause serious harm to individuals."[13] It is generally viewed as professional and fair in carrying out its duties.

LIMITS ON CONTENT

The Italian authorities engage in some blocking of internet sites, though this does not involve restrictions on politically-oriented content for the most part. Italians have access to the websites of a wide range of domestic and international news sources and human rights groups. In a positive development, throughout 2011 and early-2012, several court decisions affirmed that intermediaries are not liable for the content posted by users, though in Italy's civil-law system, some judges occasionally still issued rulings imposing responsibilities on intermediaries to regulate user-generated content. At the same time, at least one blog dealing with a sensitive criminal trial was shut down and, as in previous years, the government considered several proposals that raised alarm bells for free expression advocates, though after local and international outcry, these were dropped. The social-networking site Facebook, the Twitter microblogging service, and international blog-hosting sites are all freely available.

Since 2006, online gambling has been permitted only via state-licensed websites, and ISPs are required to block access to international or unlicensed gambling sites identified on a blacklist compiled by the Autonomous Administration of State Monopolies (AAMS). The list of banned sites is available on the AAMS website and updated regularly.[14] A similar blacklist system is in place for websites containing child pornography. A law passed in February 2006 (Law No. 6) called for the establishment of a National Center for the Fight against Child Pornography on the Internet within the Postal and Communications Police Service. Based on its own research and on complaints from citizens, the center maintains a list of sites deemed inappropriate and forwards it to ISPs for blocking.[15] As with the AAMS list, the child pornography blacklist is publicly available, though some child advocates have raised concerns that this encourages visits to the sites by users with circumvention tools. ISPs also offer subscribers "family internet" packages that block access to adult pornography and sites with violent content, in exchange for a small premium.

[13] "The Italian Data Protection Authority: Who We Are," Data Protection Authority, November 17, 2009, http://www.garanteprivacy.it/garante/doc.jsp?ID=1669109.
[14] The blacklist is available (in Italian) at http://www.aams.gov.it/site.php?id=2484.
[15] "Centro nazionale per il contrasto alla pedopornografia sulla rete" [National Center for the Fight against Child Pornography on the Internet], State Police, March 10, 2010, http://www.poliziadistato.it/articolo/view/10232/.

In 2011, two controversies arose surrounding the regulation of copyrighted content. In July, AGCOM was considering a resolution that would give it the power to block websites and remove content upon review by an internal panel but without prior judicial approval.[16] Following domestic and international opposition to the plan, AGCOM voted to review the proposed resolution,[17] and a decision is expected by the summer of 2012. Also in July 2011, the Guardia di Finanza (GdF, the police entity responsible for cybercrime) ordered the blocking of access to the website Proxyitalia.com, a general proxy site that among other websites, enabled access to Btjunkie, a torrent search engine. The GdF justified the block by stating that the domain had been created after magistrates had ordered Btjunkie blocked in April 2011 and had censured two ISPs for failing to stop users from accessing it.[18] As of May 2012, the website was still blocked.[19]

In March 2012, AGCOM also ordered the block of an online fashion retailer website following complaints by customers who claimed that the website included content that could mislead consumers about the availability of certain products. Such an executive decision was quite controversial as, until then, provisional orders against third parties had always been given by the ordinary courts. The case remains open as of mid-2012.[20]

Italian authorities have also requested the removal of specific content. According to Google, the government issued 65 requests for content removal between January and December 2011, including 20 without a court order. Google complied with 74 percent of the requests. In one notable example, Google reported receiving a request from the Central Police in Italy to "remove a YouTube video that satirized Prime Minister Silvio Berlesconi's lifestyle," but the technology firm refused.[21] In an indication of the sensitivity to content broadly

[16] "Subject: Internet censorship in Italy—via administrative procedure," European Parliament, July 13, 2011, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2011-006948+0+DOC+XML+V0//EN; Francesca Biggio, "Freedom of the Web at Risk in Italy, Copyright to Hide Censorship," Toonari Post, July 2, 2011, http://www.toonaripost.com/2011/07/world-news/freedom-of-the-web-at-risk-in-italy-copyright-to-hide-censorship/.

[17] "Italian Agency to Review Internet Filtering Project," Reporters Without Borders, July 7, 2011, http://en.rsf.org/italy-italian-agency-poised-to-assume-05-07-2011,40595.html; "Internet Blocking Stopped in Italy (for Now), Digital Civil Rights in Europe, July 13, 2011, http://www.edri.org/edrigram/number9.14/internet-blocking-agcom-italy.

[18] "Diritto d'autore e caso Btjunkie: oscurato anche Proxyitalia. Gli Isp favoriscono la pirateria?" [Copyright and case Btjunkie: Proxyitalia also obscured. Do ISPs promote piracy?], Key4biz, July 15 2011, http://www.key4biz.it/News/2011/07/15/Policy/proxyitalia_AIIP_fastweb_ngi_Btjunkie_torrent_diritto_d_autore_internet_provider_Enzo_Mazza_204544.html.

[19] See, http://proxyitalia.appspot.com/btjunkie.org; The Guardia di Finanza at times displays excessive zeal in seizing web sites, because in addition to blocking the Btjunkie, it also blocked "two innocent websites, italianstylewebsite.net and freeplayclub.org. See, "Italian Police blocks sites that had banners to alleged illegal websites," Digital Civil Rights in Europe, November 30, 2011, http://www.edri.org/edrigram/number9.23/italian-police-blocks-legal-websites.

[20] "Italy: Problematic Internet blocking decision against fraudulent website," Digital Rights Europe, March 28, 2012, http://www.edri.org/edrigram/number10.6/italy-internet-blocking-case.

[21] Google, "Italy," Google Transparency Report, accessed August 21, 2012, http://www.google.com/transparencyreport/removals/government/IT/?p=2011-12.

interpreted as defamatory, nearly half of the requests (32 in total) involved such materials. One incident that drew widespread criticism occurred in May 2011 when, per a judicial order, Google shut down the high-profile blog of freelance journalist Frank Sfarzo, a move that press freedom advocates said was inappropriate and disproportionate.[22] Sfarzo's blog had closely tracked developments in the trial of Amanda Knox for the 2007 murder of British exchange student Meredith Kercher and was highly critical of the prosecution's handling of the case. The lead prosecutor filed a defamation case against Sfarzo, which led to the shuttering of his blog. Sfarzo responded by creating a mirror blog, which remained available as of May 2012.[23]

In 2009 and 2010, several judicial decisions appeared to hold intermediaries liable for content posted by users, worrying free expression advocates and technology firms.[24] However, since early 2011, other decisions have ultimately asserted that content hosts are not responsible for prescreening content but only for removing it upon receiving notice from a judicial authority. Several of the decisions were based on the European eCommerce Directive that takes such an approach.[25] In July 2011, a Rome court specializing in intellectual property overturned an earlier decision that held Yahoo liable for not removing all of the links from its search results that allowed users to access illegal copies of the Iranian film, "About Elly."[26] The judge found that, based on existing jurisprudence, service providers could not be required to censor search results.[27]

In another decision in December 2011, a Rome court ruled that web platforms were not in breach of the law if users streamed copyrighted materials, so long as they removed it upon being notified. The decision was in response to a complaint by RTI, a subsidiary of the

[22] Steve Shay, "Google shuts down site run by Italian blogger critical of Amanda Knox prosecutor Mignini," West Seattle Herald, May 11, 2011, http://www.westseattleherald.com/2011/05/11/news/google-shuts-down-site-run-italian-blogger-critic; "Italian prosecutor files defamation lawsuit, shutters blog," Committee to Protect Journalists, May 11, 2011, http://cpj.org/2011/05/italian-prosecutor-files-defamation-lawsuit-shutte.php.

[23] Perugia Shock (blog), accessed August 21, 2012, http://perugiashock.com/

[24] See for example, a February 2010 decision in a case widely referred to as the "Vivi Down" case. A judge sentenced Google executives to jail sentences in abstentia for having allowed circulation of a video posted by a user that showed a mentally disabled child being bullied by his classmates, although Google removed the video as soon as it was notified.

[25] Martine Wubben, "Court of Appeal Rome: no monitoring requirement for hosting provider Yahoo," Future of Copyright, July 16, 2011, http://www.futureofcopyright.com/home/blog-post/2011/07/16/court-of-appeal-rome-no-monitoring-requirement-for-hosting-provider-yahoo.html.

[26] Giulio Coraggio, "Yahoo! Liable for Searchable Contents!" *IPT Italy Blog*, April 3, 2011, http://blog.dlapiper.com/IPTitaly/entry/yahoo_liable_for_searchable_contents; "PFA vs Yahoo: la decisione del Tribunale di Roma riapre il dibattito sulla responsabilità degli ISP nei casi di violazione del diritto d'autore" [PFA vs Yahoo: the decision of the Court of Rome reopens the debate on ISP liability in cases of violation of copyright], Key4biz, July 14 2011, http://www.key4biz.it/News/2011/07/14/Policy/About_Elly_yahoo_pfa_film_internet_service_provider_isp_diritto_d_autore_204511.html.

[27] "'About Elly'—Yahoo! Appea granted," Law & the Internet (blog), July 27, 2011, http://www.blogstudiolegalefinocchiaro.com/wordpress/?tag=about-elly; Martine Wubben, "Court of Appeal Rome: no monitoring requirement for hosting provider Yahoo."

Berlusconi-owned Mediaset, against Google after users on the Blogger platform streamed Italian football matches from Mediaset's TV channels. RTI sought to impose the responsibility on Google to prevent users from doing so in the future. The court rejected RTI's argument, stating that to oblige providers to prescreen user content would be inconsistent with European Union rules and that, even if it were technologically feasible, it would be a violation of freedom of expression.[28] That same month, the Supreme Court said that editors of online magazines were not responsible for defamatory comments posted by readers, taking note of the difference between the printed and electronic press, and overturned a lower courts' guilty verdict.[29] Similarly, previously introduced bills that would require websites to engage in pre-publication censorship remained on hold as of early 2012, after facing public criticism.

Nevertheless, in 2011 and early 2012, cases of defamation have been brought against online content providers and intermediaries that have led to the blocking and/or filtering of ICT content. For example, in April 2011, an Italian businessman successfully sued Google for defamation in a Milan court because the autocomplete feature of the search engine had suggested terms like "fraud" and "conman" to the plaintiff's name when a search of his name was launched.[30] While Google argued that as a hosting provider, it was not liable for the content produced on its search engine, the Italian court maintained that Google was still responsible for producing the autocomplete suggestions, reasoning that not all users are quite capable or skilled enough to distinguish between what is a suggestion and what is an attribute to the search item.[31] In addition to a fine of €3,800 (US$5,500), the court ordered Google to filter the offending search results.

Similarly, in early February 2012, a court in Belluno found Tizziano Dal Farra, the webmaster of the disaster information site Vajont.info, guilty of defamation, leading to the website's seizure and blocking. The website's allegedly defamatory content concerned the 1963 Vajont dam disaster and the political cover-ups and court cases that had ensued, which parliamentarian Maurizio Paniz (the plaintiff) found to be libelous. In its guilty verdict

[28] Guido Scorza, "Mediaset e Google: tra copyright e libertà" [Mediaset and Google: between copyright and freedom], Punto Informatico, December 16, 2011, http://punto-informatico.it/3368416/PI/Commenti/mediaset-google-copyright-liberta.aspx; http://www.telecompaper.com/news/google-not-responsible-for-streaming-football-from-mediaset; "Court of Rome: not to precautionary controls of online content by intermediaries," Law & the Internet (blog), January 17, 2012, http://www.blogstudiolegalefinocchiaro.com/wordpress/?tag=rti.

[29] "Italian Supreme Court: web magazines are not to be held responsible for readers' comments," Law & the Internet (blog), December 14, 2011, http://www.blogstudiolegalefinocchiaro.com/wordpress/?p=279.

[30] "Google Loses Defamation Case in Italy," Legalzoom (blog), accessed August 21, 2012, http://blog.legalzoom.com/first-amendment/google-loses-defamation-case-in-italy/.

[31] "Il tribunale di Milano impone un filtro a Google Suggest," Itespresso.it, April 6, 2011, http://www.itespresso.it/il-tribunale-di-milano-impone-un-filtro-a-google-suggest-51323.html.

against the webmaster, the court ordered Italy's 226 ISPs to block the site altogether.[32] Nevertheless, the website continued to be available via mirror sites and ultimately, a different judge ruled in March 2012 that the DNS/IP blocking was illegal while another judge ordered the website to be "un-seized."[33]

Some unusual restrictions on internet content remain in place in Italy that are uncommon in other Western European countries. Drawing on a 1948 law against the "clandestine press," a regulation issued in 2001 holds that anyone who wants to provide a news service, including on the internet, must be a "chartered" journalist in the Communication Workers' Registry (ROC), with membership in the national journalists' association.[34] With the exception of one case from 2008, these rules have generally not been applied to bloggers, and in practice, millions of blogs are published in Italy without repercussions.[35] Nonetheless, as of early 2012, many people who create websites on a range of issues (including scholarly research) continued to collaborate with registered journalists to protect themselves from potential legal action.

In April 2012, the Supreme Court imposed an obligation on publishers to update their online archives to ensure that outdated facts do not inadvertently damage someone's reputation. The case involved a story about the 1993 arrest of a politician on corruption charges in northern Italy. Although the man was ultimately acquitted, news of his arrest continued to appear in search results. Following the European Union principle to "the right to oblivion," the Supreme Court found that there was no ground for libel against the online news outlet that posted the story because the events in the article were true and just incomplete given subsequent developments. The court ordered the outlet to update the account.[36]

Even in the absence of legal requirements, ISPs tend to exercise some informal self-censorship, declining to host content that may prove controversial or that could create friction with powerful entities or individuals. Online writers also exercise caution to avoid

[32] "Digital censorship – Italian judges close down disaster information site," Three Monkeys Online (blog), February 19, 2012, http://www.threemonkeysonline.com/digital-censorship-italian-judges-close-down-disaster-information-site/.
[33] Fore more details see the web page http://www.vajont.info/.
[34] Law No. 62, March 7, 2001, "Nuove norme sull'editoria e sui prodotti editoriali" [New Rules on Publishing and Publishing Products], InterLex, accessed August 21, 2012, http://www.interlex.it/testi/l01_62.htm.
[35] A known case is that of author Carlo Ruta whom, in September 2008, a judge in Sicily found guilty of publishing a "clandestine newspaper" in the form of a blog (Ruta was fined €250 and forced to take down his blog). See, John Ozimek, "How an Italian Judge Made the Internet Illegal," *The Register*, September 26, 2008, http://www.theregister.co.uk/2008/09/26/italian_law_kills_blog/.
[36] "Italian Supreme Court: the right to oblivion to be protected with newspaper archive updates," Law & the Internet (blog), April 23, 2012, http://www.blogstudiolegalefinocchiaro.com/wordpress/?p=360. See also, Morena Ragone, "Il diritto alla memoria, tra privacy e oblio" [The right to memory, including privacy and oblivion], LeggiOggi.it, April 10, 2012, http://www.leggioggi.it/2012/04/10/il-diritto-alla-memoria-tra-privacy-e-oblio/.

libel suits by public officials, whose litigation—even when unsuccessful—often takes a significant financial toll on defendants in the traditional media. The Italian government does not proactively manipulate news websites. However, coverage in traditional media does affect what is published on news websites, giving the outlets controlled by former Prime Minister Berlusconi an indirect influence over online reporting.

Blogging has become popular in Italy, though television remains by far the leading medium for obtaining news. Most policymakers, popular journalists, and figures in the entertainment industry have their own blogs, as do many ordinary citizens. Social-networking sites, especially Facebook[37] and Twitter, have emerged as crucial tools for organizing protests and other mass gatherings, such as concerts, parties, or political rallies, although at times, some content on social-networking platforms has been aggressive enough to potentially incite violence.[38] As of May 2012, the country was home to over 21 million Facebook users (about 37 percent of the population), the 11th highest number in the world.[39]

Italian internet users and free expression advocates have recently mobilized against two legal initiatives perceived to threaten internet freedom. In October 2011, Wikipedia's Italian edition took all entries offline to protest the reintroduction of draft wiretap bill to parliament, threatening to take down its Italian site entirely if the law was passed. Meanwhile, Italian protestors wearing gags gathered outside the legislature's building in Rome.[40] After the change of government in November 2011, the bill was effectively put on hold. In February 2012, internet rights activists scored another victory when parliamentarians across the political spectrum rejected legal amendments that had been called by the media the "Italian SOPA," a reference to a controversial anti-piracy bill that was under consideration in the United States. If passed, the Italian amendments would have enabled any "interested party" (rather than only the "competent authorities") to ask hosting providers to remove any content by claiming it to be an illegal infringement of copyright, rendering the provider legally liable without any judicial or other authorized entity needing to evaluate the claim. The free expression group Agora Digitale and other civil society representatives organized a press conference in late January to alert the public and parliamentarians to the ramifications of the proposed amendment. After the change was rejected, Luca Nicotra, president of the Agora Digitale, commented that the vote was "a

[37] As of November 2011, there were 21 million Italians on Facebook (out of 27 millions Internet users); see M. Vecchio, "Italia, la Repubblica di Facebook" [Italy, the Republic of Facebook], Punto Informatico, November 28, 2011, http://punto-informatico.it/3349331/PI/News/italia-repubblica-facebook.aspx.

[38] For example, in 2009, fan pages for imprisoned Mafia bosses emerged, as did a Facebook group called "Let's Kill Berlusconi." See Eric Sylvers, "Facebook to Monitor Berlusconi Content," The New York Times, December 15, 2009, http://www.nytimes.com/2009/12/16/technology/internet/16iht-face.html.

[39] "Italy Facebook Statistics," Socialbakers, accessed August 21, 2012, http://www.socialbakers.com/facebook-statistics/italy.

[40] "Italy wiretap law: Wikipedia hides pages in protest," BBC, October 5, 2011, http://www.bbc.co.uk/news/world-europe-15192757.

sign that there is a small all-party group of MPs determined to defend the values of an open and free Internet."[41]

VIOLATIONS OF USER RIGHTS

As a signatory to the European Convention on Human Rights and other relevant international treaties, freedoms of speech and the press, as well as the confidentiality of correspondence, are constitutionally guaranteed in Italy.[42] Yet, given the country's civil law system, inconsistent judicial interpretations are not unusual. This has created some uncertainty when judges issue conflicting decisions on similar cases related to internet freedom, such as intermediary liability (see "Limits on Content"). For this reason, online free expression advocates have focused their efforts on proposing legal amendments to improve protections and prevent censorship rather than engaging in public interest litigation.[43]

Defamation is a criminal offense in Italy, punishable by prison terms ranging from six months to three years and a minimum fine of €516 (US$670). In cases of libel through the press, television, or other public means, there is no prescribed maximum fine.[44] Though these provisions are rarely applied, civil libel suits against journalists, including by public officials and politicians, are a common occurrence, and the financial burden of lengthy legal proceedings may have chilling effects on journalists and their editors. As of May 2012, however, libel suits against bloggers and other online writers remain rare,[45] with only one defamation case against the blogger Frank Sfarzo occurring in 2011 (see "Limits on Content"). Nevertheless, as also noted above, there have been a few defamation cases brought against online content providers in recent years, such as the defamation case against Google in April 2011 that resulted in a fine and court order to filter out the offending content.

Monitoring of personal communications is permissible only if a judicial warrant has been issued, and widespread technical surveillance is not a concern in Italy. Nevertheless, the

[41] "Internet—Italian free speech groups claim victory," Giannifava.org, February 7, 2012, http://www.giannifava.org/it/doc-s-27-589-1-internet___italian_free_speech_groups_claim_victory.aspx.
[42] An English copy of the constitution is available at, http://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf. See especially Articles 15 and 21.
[43] Andrea Monti (lawyer specialized on Internet freedom and activist), interview with author, February 20, 2012.
[44] Organization for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, *Libel and Insult Laws: A Matrix on Where We Stand and What We Would Like to Achieve* (Vienna: OSCE, 2005), 79, http://www.osce.org/fom/41958.
[45] See for example the case of Roberto Mancini in, Reporters Without Borders, "A Blogger Unfairly Convicted of Defamation," news release, June 20, 2006, http://en.rsf.org/italy-a-blogger-unfairly-convicted-of-20-06-2006,18068.html.

country's authorities are known for engaging in a large number of wiretaps.[46] According to the most recent figures from the German think-tank, the Max Planck Institute, in 2006, Italy led the world in terms of wiretaps, with 76 intercepts per 100,000 people.[47] Wiretapping is generally restricted to cases involving ongoing legal proceedings, except for terrorism investigations. In such instances, since 2001, "pre-emptive wiretapping" may occur even if no formal prosecutorial investigation has been initiated. More lenient procedures are also in place for Mafia-related investigations.[48]

In early 2010, a draft wiretap bill was introduced in parliament. The bill's proponents said it aimed to address concerns over the right to privacy and the problem of news media regularly publicizing wiretap information that is leaked to them. However, several provisions appeared to threaten media freedom and the right of the public to access independent information. These included high fines and jail sentences for filming an individual without permission, and obligations for websites and blogs to issue corrections within 48 hours of receiving notice of an alleged error. Both the Organization for Economic Cooperation and Development's (OECD) representative on freedom of the media and the UN special rapporteur on freedom of expression criticized the bill in its proposed form. The bill was subsequently put on hold in late 2010 but revived in October 2011 after incriminating and embarrassing wiretaps of Berlusconi's conversations related to a sex scandal were published in newspaper and online.[49] However, after Berlusconi's resignation, the bill remained pending in parliament. Although not a priority for the Monti government, the executive branch, especially the minister for justice, decided not to drop entirely the matter as of spring 2012.

[46] Although it is difficult to determine the real number of people affected by wiretaps (estimates range from 25,000 to over 130,000), many individuals who are caught up in wiretaps have no incriminating connection to the main target of the eavesdropping. The current law stipulates that such peripheral communications cannot be transcribed and any recordings should be destroyed right away, though this is not always carried out in practice. Thus it may happen that some exchanges are recorded and leaked to the media. This is the problem that the proposed bill on electronic surveillance was meant to address. See for example Cristina Bassi, "Intercettazioni, quante sono e quanto costano" [Interceptions, How Many and How Much They Cost], *Sky TG24*, June 13, 2010, http://tg24.sky.it/tg24/cronaca/2010/06/12/intercettazioni_quante_sono_e_quanto_costano.html.

[47] Duncan Kennedy, "Italian bill to limit wiretaps draws fire," BBC, June 11, 2010, http://www.bbc.co.uk/news/10279312. It might be as high as 150,000 phones, which does not say anything about "people" (arguably one person has 2/3 fixed and mobile phones). See for example, "Intercettazioni: dati ufficiali" [Interceptions: official data], Il Chiodo (blog), June 19, 2010, http://ilchiodo.blogspot.it/2010/06/intercettazioni-dati-ufficiali.html.

[48] Privacy International, "Italy: Privacy Profile," in *European Privacy and Human Rights 2010* (London: Privacy International, 2010), https://www.privacyinternational.org/article/italy-privacy-profile.

[49] Tom Kington, "Berlusconi wiretaps reveal suspected pimp had visa to join him in China," The Guardian, September 18, 2011, http://www.guardian.co.uk/world/2011/sep/18/berlusconi-pimp-china-visa-wiretaps; Jeffery Kofman, "Silvio Berlusconi Wiretaps: 'Only Prime Minister in His Spare Time,'" ABC News, September 18, 2011, http://abcnews.go.com/International/silvio-berlusconi-wiretaps-prime-minister-spare-time/story?id=14546921; John Hooper, "Silvio Berlusconi faces fresh claims over parties, prostitutes and pay-outs," The Guardian, September 15, 2011, http://www.guardian.co.uk/world/2011/sep/15/silvio-berlusconi-claims-prostitutes-wiretap.

In March 2008, Parliament approved a law (No. 48 of 2008) that ratified the Council of Europe's Convention on Cybercrime, which established how long internet-related communication data should be retained.[50] This matter was further refined with the inclusion in the Italian legislative system of the 2006 EU Data Retention Directive.[51] Under the current legal framework, ISPs must keep users' traffic records—though not the content of communications—for 12 months. This includes broadband internet data, internet telephony, internet use via mobile phone, and email activity.[52] The records can only be disclosed in response to a request from a public prosecutor (a judge) or a defendant's lawyer, and, like their counterparts elsewhere in Europe, Italy's law enforcement agencies may ask ISPs to make such information readily available so that they can respond to the needs of criminal investigations. Given the technical burden of this directive, most ISPs now use a third-party service that offers the necessary security guarantees for encryption and data storage.

As Italy moves towards greater e-governance, some concerns have been raised over the protection of user data in the hands of public agencies. In June 2011, the national postal service Poste Italiane's certified electronic mail (PEC) service was named as the public agency most damaging to individual privacy at the annual Big Brother awards for its gross mishandling of private information kept by the government's "Registro delle Opposizioni," a register of people who wish to keep their contact information hidden from advertisement companies.[53] Nevertheless, in November 2011, it became mandatory for all business to use the PEC service in their communications with the public administration, to cut costs and reduce paperwork.[54]

Reports of extrajudicial intimidation or physical violence in response to online activity are rare in Italy, though individuals directly exposing the activities of organized crime in some parts of the country may be at risk of reprisals. Nevertheless, in April 2011, the Committee to Protect Journalists (CPJ) wrote to the Italian government to voice concerns over the harassment of blogger and freelance journalist Frank Sfarzo as he sought to cover the trial of Amanda Knox. According to the CPJ, Italian police regularly prevented Sfarzo from entering the courtroom, seized his mobile phone, and verbally insulted him. Moreover,

[50] For a useful timetable of the required retention periods, see Gloria Marcoccio, "Convention on cybercrime: novità per la conservazione dei dati" [Convention on Cybercrime: News on Data Retention], InterLex, April 10, 2008, http://www.interlex.it/675/marcoccio7.htm. See also Andrea Monti, "Data Retention in Italy. The State of the Art," Digital Thought (blog), May 30, 2008, http://blog.andreamonti.eu/?p=74.
[51] Legislative Decree No. 109, May 30, 2008.
[52] Privacy International, "Italy: Privacy Profile."
[53] Cristina Sciannamblo "Big Brother Awards Italia: tutti i vincitori," Punto Informatico, June 6, 2011, http://punto-informatico.it/3182022/PI/News/big-brother-awards-italia-tutti-vincitori.aspx.
[54] "Ulteriore Deroga fino a fine giugno 2012 per la casella PEC aziendale," IlSoftware.it, accessed July 24, 2012, http://www.i-node.it/2012/05/ulteriore-deroga-fino-fine-giugno-2012-la-casella-pec-aziendale/.

Sfarzo reported that in September 2010 police forcibly entered his apartment, assaulted him, tried to get a psychiatrist to issue a statement questioning his mental capacity, and then took him before a judge, attempting to charge him with "injuring an officer."[55]

Defacement or launching denial-of-service (DoS) attacks against websites—mostly government-linked ones—as a form of political protest are becoming increasingly common in Italy. More serious cyberattacks—particularly against banks, government institutions, and business websites—are a problem in Italy, as in other European Union member states. Despite some problems, Italy does not seem to rank high on the list of countries identified as points of origin for cybercrimes.[56]

The law enforcement agency with primary responsibility for cybercrimes is the Postal and Communications Police Service. Police officers are primarily concerned with cybercrime in the form of child pornography, cyber-bullying, and various forms of fraud.[57] A special branch within the service, the National Center for Infrastructure Protection (CNAIPIC), is tasked with the protection of the country's critical infrastructure.[58] However, in one incident that received widespread attention in July 2011, the hacker groups Anonymous and LulzSec claimed responsibility for hacking into CNAIPIC's own website and posting

[55] "In Italy, journalists threatened for reporting on murders," Committee to Protect Journalists, April 19, 2011, http://www.cpj.org/2011/04/journalists-threatened-for-reporting-on-murder-cas.php.

[56] "Italy leader in mobile attacks," Global Cyber Security Center (blog), accessed August 21, 2012, http://www.gcsec.org/blog/italy-leader-mobile-attacks. It should be noted, nonetheless, that the Global Cyber Security Center has been established by Poste Italiane. As active stakeholder in the area of cyber security, the agency may have a vested interest in presenting a picture of Italy's cyber security that is not reassuring by stressing weaknesses rather strengths of the Italian information infrastructure system. See, C. Giustozzi, "Italia patria del malware?" Punto Informatico, May 12, 2012 http://punto-informatico.it/3513450/PI/Commenti/italia-patria-del-malware.aspx. The "Symatec Threat report 2011" shows Italy as highly infected only as far as bots are concerned, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf (published April 2012), and the independent report by HostExploit shows Italy scoring well on a "badness" scale (Germany and the Netherlands, for example get a worse score), http://hostexploit.com/downloads/viewdownload/7-public-reports/39-global-security-report-april-2012.html). These results are also graphically visible in here: http://globalsecuritymap.com/#nl

[57] Figures on cybercrime are difficult to assess, as the main providers of data are computer security companies such as Symantec or government entities like the postal police, as opposed to "third-party" sources. Nevertheless, Italy's rates appear to be slightly above the world average. See, Tiziana Moriconi, "Crimini online, i dati italiani" [Online Crime, the Italian Data], Daily Wired, November 23, 2010, http://daily.wired.it/news/internet/hacking-accordo-tra-symantec-e-polizia-postale.html; Alessandra Talarico, "Cybercrime. Italia vittima e carnefice: è il paese che più abbocca al phishing e tra i più attivi negli attacchi web based" [Cybercrime. Italy Victim and Victimizer: It Is the Country That Takes the Bait in Phishing and Is Among the Most Active in Web-Based Attacks], Key4Biz, April 22, 2010, http://www.key4biz.it/News/2010/04/22/eSecurity/cybercrime_botnet_spam_ebanking_social_network_spyware_adware_phishing.html. For a recognition of the professionalism of Italy's postal police, see Alessandra Talarico, "Lotta al cybercrime: avrà sede a Roma nuova task force Usa-Europa. Utilizzerà le tecnologie di Poste Italiane" [Fighting Cybercrime: A New U.S.-European Task Force Will Be Based in Rome. Will Use the Technologies of the Italian Post], Key4Biz, June 30, 2009, http://www.key4biz.it/News/2009/06/30/eSecurity/cybercrime_sicurezza_reti_European_Electronic_Crime_Task_Force_US_Secret_Service_Massimo_Sarmi.html.

[58] Critical infrastructure includes telecommunications networks, energy and water distribution systems, banking networks, and transportation and emergency services.

confidential information online in an apparent act of revenge for the arrest of group members in the United States and parts of Europe.[59]

[59] "'Anonymous' attacks Italian cyber police website," The Raw Story, July 25, 2011, http://www.rawstory.com/rs/2011/07/25/anonymous-attacks-italian-cyber-police-website/; "Hackers hit back with attack on Italian police," Agence France-Presse, July 25, 2011, http://www.google.com/hostednews/afp/article/ALeqM5h7VBHxIVebJWDKXPGW5UCq0l2Mnw?docId=CNG.1c9bc08f90c82172428a633d1b6e8077.9d1.

JORDAN

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	12	13
Limits on Content (0-35)	11	12
Violations of User Rights (0-40)	19	20
Total (0-100)	**42**	**45**

* 0=most free, 100=least free

POPULATION: 6.3 million
INTERNET PENETRATION 2011: 35 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Jordan, a small kingdom of about six million people, prides itself on offering relatively broad freedom to use the internet and officially blocks only one website. The Jordanian government's response to public protests in 2011 was relatively mild compared to neighboring countries. Moreover, the king and parliament passed a set of constitutional amendments that could improve human rights protections and free expression.

Nevertheless, restrictions on internet freedom exist and have increased since January 2011. News websites, which have become a vital source of information in a country where traditional media freedom is limited, often face pressure from state actors to delete articles deemed politically sensitive. In April 2012, a government council passed a resolution that could require online news websites to register with the government, a policy that if implemented risks curbing their independent reporting and analysis. Meanwhile, surveillance, physical attacks against bloggers and online journalists, and hacking attacks against prominent news websites also present a threat.

Internet access was first provided to Jordanians in 1995, and the Telecommunications Regulatory Commission (TRC) was created that year to oversee the medium.[1] The authorities quickly recognized the economic potential of the internet and actively promoted

[1] The TRC was established as a financially and administratively independent jurisdictional body through the Telecommunications Law (No. 13 of 1995) and a subsequent amendment (Law No. 8 of 2002).

the development of information and communication technologies (ICTs) in the kingdom.[2] As the number of internet users began to increase dramatically, the government stepped up both infrastructure expansion and monitoring. Although the authorities are aware of the need to develop the ICT sector for the country's economic survival and progress, they are nonetheless concerned about the internet's ability to empower citizens politically.

OBSTACLES TO ACCESS

According to the International Telecommunication Union (ITU), 35 percent of the Jordanian population accessed the internet in 2011, or about 2.1 million people.[3] The TRC estimated the number of users in early 2012 to be much higher, at 3.3 million people, or about 50 percent of the population.[4] Given the large number of people getting online at cybercafes and offices, most users have access to broadband rather than dial-up connections.[5] Most internet users are young people ranging in age from 15 to 24.[6] Nonetheless, the medium, once seen as a tool for trivial entertainment and the exchange of scandalous or banned information, has grown into a vital instrument for business and an important forum for public discussion.

Mobile phone use has also expanded rapidly and by the end of 2011, the number of subscriptions was over 7.4 million, exceeding the total population.[7] Since 3G services were first launched in mid-2010, the number of subscribers has grown to over one million (about one-sixth of the population) between the two largest operators, Zain and Jordan Telecom.[8] Observers anticipate this number will further grow in 2012 upon implementation of a tax exemption for the purchase of smartphones and the launch of 3G services by another provider, Umniah.[9]

---

[2] Privacy International, "Jordan," *Silenced: An International Report on Censorship and Control of the Internet*, 2003, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-103564.

[3] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[4] Telecommunications Regulatory Commission of Jordan's official website [in Arabic], http://www.trc.gov.jo/index.php?option=com_content&task=view&id=1942&lang=arabic.

[5] Ibid.

[6] Mohammad Ghazal, "News websites most popular destination for Jordanian Internet users—study," The Jordan Times, March 22, 2012, http://jordantimes.com/news-websites-most-popular-destination-for-jordanian-internet-users----study.

[7] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[8] ITU, "Jordan Telecom to invest JOD50 million in 3G," news release, June 29, 2011, http://www.itu.int/ITU-D/ict/newslog/Jordan+Telecom+To+Invest+JOD50+Million+In+3G.aspx; ITU, "Smartphone tax exemption drives 3G growth (Jordan)," news release, January 19, 2012, http://www.itu.int/ITU-D/ict/newslog/Smartphone+Tax+Exemption+Drives+3G+Growth+Jordan.aspx.

[9] ITU, "Smartphone tax exemption drives 3G growth (Jordan)," news release, January 19, 2012, http://www.itu.int/ITU-D/ict/newslog/Smartphone+Tax+Exemption+Drives+3G+Growth+Jordan.aspx.

Expansion of fixed-line internet access has been hampered by the cost of computers and connectivity. For several years, internet connection fees were considered high relative to neighboring countries and the cost of living. Prices have decreased, reportedly upon direct orders from the king, but complaints about the quality of service persist. Monthly internet subscription prices currently range from 10 Jordanian Dinars (JD) (US$14) for the speed of 1 Mbps to about 25 JD (US$35) for the speed of 2 Mbps for uploads and 10 Mbps for downloads. These charges are typically twice as much for subscriptions in an office setting. By comparison, the average monthly income in Jordan is about US$500.[10] Customers often claim that connection speeds fluctuate and do not correspond to what they pay for. Meanwhile, internet access in remote areas remains poor, as almost all companies concentrate their operations and promotions in the capital, Amman.

The ICT sector is bound by Law No. 13 of 1995 and its amendment, Law No. 8 of 2002. The law endorses free-market policies and principles, and governs licensing and quality assurance.[11] Citizens and businesses can obtain internet access through privately owned service providers, and no special state approval or registration is required, but traffic must still flow through a government-controlled telecommunications hub. As of November 2011, there were 16 active internet service providers (ISPs) in Jordan, though licenses have been granted to over 20 companies.[12] The market is dominated by Umniah, Zain, and Jordan Telecom, the local affiliate of France Telecom's Orange brand. The formerly state-owned Jordan Telecom controls the fixed-line network and provides access to all other ISPs providing ADSL services, thereby centralizing most of the connection to the international internet.

The TRC is the main body overseeing the ICT sector. It is governed by the Telecommunications Law, which proscribes its financial and jurisdictional independence and the need to ensure no prior conflicts of interest among its five board members.[13] In May 2011, the Council of Ministers appointed Mohammad Taani to head the TRC.[14] The TRC is generally seen as independent and fair in its decision making, though it coordinates policy with the government.

[10] World Bank, "Gross national income per capita 2011, Atlas method and PPP," World Bank Databank, 2011, accessed July 18, 2012, http://databank.worldbank.org/databank/download/GNIPC.pdf.

[11] "Jordan," *One Social Network With A Rebellious Message,* Arabic Network for Human Rights Information, 2009, http://www.openarab.net/en/node/1618.

[12] ITU, *ICT adoption and prospects in the Arab region,* Connect Arab Summit 2012, pg. 57, http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-AR-2012-PDF-E.pdf.

[13] The Telecommunications Regulatory Commission of Jordan, *Chapter III*, http://www.trc.gov.jo/index.php?option=com_content&task=view&id=20&lang=english.

[14] Telecommunications Regulatory Commission of Jordan, *Mohammad Al Taani, Chairman of the Board of Commissioners/CEO*, http://www.trc.gov.jo/index.php?option=com_content&task=view&id=126&Itemid=1079&lang=english.

LIMITS ON CONTENT

Although the Jordanian government does not engage in extensive blocking of websites, other restrictions on online content exist. Behind-the-scenes pressure to delete content continues and in 2012 the parliament adopted amendments that require news websites to register with the government. Meanwhile, online tools—particularly news websites and the social-networking site Facebook—have played an important rule in mobilizing public protests to oppose restrictions to free expression and call for broader political reforms.

In a 2009 meeting with journalists, government officials pledged to refrain from issuing legislation to censor online content. Indeed, outright blocking of websites by the authorities is rare. The only permanently blocked website is the U.S.-based *Arab Times* newspaper, which often takes a critical tone toward Arab regimes and their leaders.[15] In 2008, the authorities began blocking access to up to 600 websites on internal government networks, claiming such measures were necessary to prevent public service employees from wasting time online. The inclusion of key Jordanian news websites among those blocked raised concerns that the purpose was also to limit government employees' access to independent information.[16] In a positive development, the administration of Prime Minister Marouf al-Bakhit that came into office in February 2011 reversed this policy, enabling access for government employees to all websites.

More common in Jordan is for website owners to remove material after receiving informal complaints via telephone from government officials, members of the security services, party leaders, lawmakers, journalists, and ordinary users. In several cases over the past two years, websites that refused such requests faced reprisals. For example, in February 2011, one of the country's most popular news websites, *Ammon News*, was hacked and temporarily disabled after its editors refused to comply with security agents' demands to remove a statement by 36 prominent Jordanian tribesmen calling for democratic and economic reforms. Among other actions, the hackers deleted the joint statement, which represented a politically sensitive development given such groups' historic support for the monarchy.[17] In another incident in March 2012, the Jordanian Royal Court pressured the website of the *al-Arab al-Yawm* newspaper to delete an article titled, "We will not live in a stupid man's robe," which criticized the government's handling of corruption and protests in the city of al-

[15] A test by Freedom House in February 2012 confirmed that the website remains inaccessible. See also, "Jordan," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/jordan.
[16] Arab Archives Institute, "Fear of Freedoms: King Insists on Freedoms, Government Resists," news release, December 6, 2008, http://www.ifex.org/jordan/2008/12/09/capsule_report_despite_advances/; "Public Employees Wasting Time on the Internet," The Jordan Times, August 5, 2010, http://www.jordantimes.com/index.php?news=28938.
[17] "In Jordan, website hacked after running sensitive statement," Committee to Protect Journalists, February 9, 2011, http://cpj.org/2011/02/in-jordan-website-hacked-after-running-sensitive-s.php.

Tafila.[18] In other cases, news websites have had to deal with waves of angry comments from the public after tackling sensitive issues, as readers pressure them to respect traditions.

Throughout 2011, debate continued over whether and how the government might extend the application of the Press and Publications Law (PPL), which governs and often restricts traditional media, to the online sphere. In January 2010, the Court of Cassation ruled that websites and electronic media must comply with the PPL.[19] However, implementing the decision was complicated by the fact that most Jordanian online news outlets are hosted on servers outside of the country due to cost, thereby placing them beyond the jurisdiction of domestic courts.[20] In August 2011, both houses of parliament passed amendments to the PPL to provide online news outlets with the choice to register with the government in exchange for certain benefits, or remain unregistered.[21] Among the benefits cited were guaranteed access to government officials, invitations to press conferences, and opportunities to receive public funding via advertisements. In addition, registered online news outlets and their staffs would only be subject to fines for content violations, whereas employees of unregistered websites risk imprisonment under the penal code, security legislation, and libel laws. Despite the government's efforts to lure independent websites into registering, as of March 2012, very few had done so. Thus, in April 2012, the Higher Judicial Council's Law Interpretation Bureau issued a decision classifying news websites as publications that should be subject to the same regulations as print media, including registering with the Press and Publications Department.[22] As of mid-2012, the government was considering legislation that would further formalize such an obligation.[23]

Among other implications, this regulatory change could affect the financial viability of online news websites as the PPL prohibits foreign investment in newspapers, a provision that could now apply to online news outlets as well. Meanwhile, unconfirmed reports emerged of government agencies in early 2012 pressuring advertisers to avoid certain news websites in an effort to limit the sites' income.[24] There have also been some initial reports of security or government officials offering encouragement—and possibly material support—to

[18] International Freedom of Expression Exchange (IFEX), "Royal Court orders newspaper to remove critical article from website," news release, March 26, 2012, http://www.ifex.org/jordan/2012/03/26/article_censored/.
[19] Hani Hazaimeh, "Court Ruling Threatens Press Freedom—Activists," Jordan Times, January 15, 2010, http://www.jordantimes.com/?news=23196.
[20] Daoud Kuttab, "Jordan's News Sites' 'Voluntary' Registration Law Will Not Work," The Huffington Post, August 4, 2011, http://www.huffingtonpost.com/daoud-kuttab/jordans-newssites-volunta_b_917809.html.
[21] Law No. 17, Article 49, 2011.
[22] Higher Judicial Council Bureau for Interpreting the Law, "Resolution No. 2 for the year 2012," [in Arabic], April 9, 2012, www.jc.jo/القانون بتفسير الخاص الديوان عن الصادرة القرارات/2640.
[23] Hani Hazalmeh, "Press law 'not sacred', open to change under Dome," The Jordan Times, August 2, 2012, http://jordantimes.com/press-law-not-sacred-open-to-change-under-dome.
[24] "Campaign on websites and the government refuses to license" [in Arabic], Allofjo, May 30, 2012, http://www.allofjo.net/index.php?page=article&id=29643.

journalists to establish news websites favorable to the government that would compete with the increasingly influential, and often critical, existing online outlets.[25]

The threat presented by restrictive laws and financial penalties in the PPL, combined with an awareness of extensive content monitoring, has a chilling effect on expression online. Bloggers and news website owners often complain directly or indirectly about their inability to post news freely due to monitoring. Many practice self-censorship and rarely cross the standard red lines, particularly concerning material that could be perceived as harmful to national security, national unity, the country's economy, or the royal family.

The country's approximately 200 news websites and their political analysis are an increasingly important source of information for many Jordanians, who feel they report information unavailable from print and broadcast media. A study released by the market research firm Ipsos in March 2012 found that around 70 percent of internet users accessed news websites, making it the most popular area of online interest, surpassing music and sports.[26] Three news websites—*Sarayanews*, *Khaberni*, and *Ammon News*—were among the top 20 most visited websites in the country in March 2012.[27]

Blogs in Jordan, which initially contributed to residents' discovery of the internet as a source of uncensored information, seemed to have lost some of their influence in relative terms in 2009 and 2010. Blogs regained their importance as an avenue for debate on political and social issues in 2011, as people used a wide range of new media tools to share information and organize protests. The most well-known blogs are produced by journalists seeking more freedom to post their views without their editors' censorship. A growing number of blogs are written in Arabic, a shift from several years ago, when most were bilingual or in English.

Web 2.0 applications and sites—including global platforms like Facebook, the microblogging service Twitter, and the video-sharing site YouTube—are freely available and very popular, particularly among younger Jordanians. The number of Facebook users in Jordan in March 2012 exceeded two million, representing over one-third of the country's population.[28] The microblogging website Twitter has garnered a smaller following. According to one social media analyst, by the end of May 2011, there were approximately 50,000 Twitter users in Jordan, of which only 15,000 were active, posting several times a

[25] "Liberal Press: government seeks to break the power forward positions" [in Arabic], JO24, May 29, 2012, http://www.jo24.net/index.php?page=article&id=5179.
[26] "News websites most popular destination for Jordanian Internet Users," Zawya.com, accessed September 18, 2012, http://www.zawya.com/story.cfm/sidZAWYA20120323115500/News_websites_most_popular_destination_for_Jordanian_Internet_users (subscription required).
[27] "Top Sites in Jordan," Alexa Web Information Company, accessed March 27, 2012, http://www.alexa.com/topsites/countries/JO.
[28] "Jordan Facebook Statistics," Social Bakers, accessed March 28, 2012, http://www.socialbakers.com/facebook-statistics/jordan.

week.[29] Several local social media tools had previously gained popularity, but in June 2011, the Jordanian microblogging site WatWet shut down, unable to compete with Twitter.[30] Besides average citizens using these tools to communicate, several ministers and government officials, including the Minister of Information, have established Facebook and Twitter accounts to communicate with the public. Queen Rania Al Abdullah has also been known to use Facebook and Twitter from time to time.

Facebook played a particularly important role in 2011 mobilizing youth to participate in protests calling for political reform. Throughout the year, numerous demonstrations took place, gathering thousands of people. In March 2011, a group calling itself Youth of March 24 organized a protest camp in a central square in Amman via Facebook. They demanded the prime minister's resignation, parliamentary reforms, and the prosecution of corrupt officials. That night, police attempted to disperse the youth, cutting off electricity at the location. Meanwhile, a group of people believed to be government loyalists began throwing rocks at the protesters as police reportedly stood by, resulting in over 30 people being injured.[31] The organizers had prepared for potential clashes, however, designating people in advance to document any violent incidents. As a result, images and video clips of the attack were taken, uploaded, and quickly circulated online.[32]

VIOLATIONS OF USER RIGHTS

In October 2011, responding to public pressure and street protests that began in January, King Abdullah II approved over 40 constitutional amendments that had been passed by both houses of parliament. The amendments include creation of a constitutional court (Article 58-61), an explicit prohibition on torture (Article 8), and the restriction of the State Security Court's jurisdiction only to crimes of treason, espionage, and terrorism (Article 110).[33] Several amendments touched directly or indirectly on internet freedom. Specifically, terms such as "mass media" and "other means of communication," which likely encompass online media, were added to provisions that both protect freedom of expression and allow

[29] Mohammad Ghazal, "Twitter study points to declining happiness, but users don't plan to stop," The Jordan Times, December 29, 2011, http://jordantimes.com/twitter-study-points-to-declining-happiness-but-users-dont-plan-to-stop.
[30] "On Shutting Down WatWet," Tootcorp.com, July 2011, http://tootcorp.com/2011/07/on-shutting-down-watwet/ (site discontinued).
[31] "Clashes break out at Jordan anti-government protest," BBC News, March 25, 2011, http://www.bbc.co.uk/news/world-middle-east-12857360.
[32] Yahia Shukkeir, *Jordan: 2011 Internet rights and democratization,* Global Information Society Watch, 2011, http://www.giswatch.org/en/country-report/social-mobilisation/jordan; Hadeel Gbon and Abdullah Dividend, "Dozens injured in a sit-in after a new attack of 'thugs'" [in Arabic], Alghad, March 25, 2011, http://alghad.com/index.php/article/422946.html.
[33] Ali al-Rawashdah, "Jordan approves constitutional amendments," Al-Shorfa, October 5, 2011, http://al-shorfa.com/cocoon/meii/xhtml/en_GB/features/meii/features/main/2011/10/05/feature-01.

for its limitation during periods of emergency (Article 15). With regards to the right to privacy, the requirement of a judicial order was added as a precondition for censorship or confiscation of telephonic and other means of private communication (Article 18).[34] For the Constitutional Court to come into effect, additional legislation is required, which had not been completed as of May 1, 2012.

Despite constitutional protections, there remain several laws that hinder free expression and access to information. These include the Jordan Press Association Law (1998), the penal code (1960), the Defense Law (1992), the Contempt of Court Law (1959), the Protection of State Secrets and Classified Documents Law (1971), and the Press and Publications Law (1999). An Access to Information Law was enacted in 2007, but it contains a number of restrictions.[35] In September 2011, the elected lower house of parliament passed an amendment to the country's Anti-Corruption Law, which would penalize the publication or dissemination of allegations of corruption without proof with fines ranging from 30,000 to 60,000 dinar (US$42,000-US$84,000).[36] However, in January 2012, the upper house of parliament rejected the controversial article when passing the law, following analysis by a new committee chosen after the change in government, advocacy efforts by civil society groups, and resignation threats by the board of the Jordan Press Association.[37]

Defamation remains a criminal offense under the penal code. A series of amendments to the law enacted in 2010 abolished imprisonment as a punishment for libeling ordinary citizens, but increased the fine (up to 10,000 dinars or US$14,000) and jail sentences (from three months to two years) for libel committed against public servants and government officials, contrary to international practice of greater lenience for criticism of elected or appointed officials.[38]

[34] Constitution of Jordan, 1952, http://www.mpil.de/shared/data/pdf/overview_amendments.pdf; "Jordan," Max Planck Institute for Comparative Public Law and International Law, last updated May 4, 2012, http://www.mpil.de/ww/en/pub/research/details/know_transfer/constitutional_reform_in_arab_/jordanien.cfm.

[35] For example, the law bars public requests for information involving religious, racial, ethnic, or gender discrimination (Article 10), and allows officials to withhold all types of classified information, a very broad category (Article 13) Arab Archives Institute, "Summary of the Study on Access to Information Law in Jordan," June 2005, http://www.alarcheef.com/reports/englishFiles/accessToInformation.pdf.

[36] Yahya Shakir, "Article 23 of the Anti-Corruption Law aimed at burying the opposing views in the bud" [in Arabic], Alarabalyawm, http://alarabalyawm.batelco.jo/pages.php?articles_id=17077;

[37] "Jordan journalists protest anti-corruption bill," Khaleej Times, September 28, 2011, http://www.khaleejtimes.com/darticlen.asp?xfile=data/middleeast/2011/September/middleeast_September568.xml&section=middleeast; Wael Jaraysheh, "Senate Returns Controversial Anti-Corruption Law, Dodging Deliberations Again," Ammon News, December 8, 2011, http://en.ammonnews.net/article.aspx?articleNO=14876; "Jordanian Senate Rejects Article 23 of the Anti-Corruption Law," SKeyes News, January 16, 2012, http://www.skeyesmedia.org/en/News/Jordan/Jordanian-Senate-Rejects-Article-23-of-the-Anti-Corruption-Law.

[38] IREX, "Introduction to News Media Law and Policy in Jordan," May 2011, pg 38, http://www.irex.org/sites/default/files/Media%20Law%20and%20Policy%20Primer%20(English).pdf.

The parliament passed a new cybercrime law in August 2010. The law, which proscribes penalties for cybercrimes such as hacking and online identity theft, also contains several provisions that could be easily used to suppress free online expression. For example, the new law prohibits posting any information on the web already not available to the public concerning national security, foreign affairs, the national economy, and public safety. Nevertheless, following protests by civil society, several more egregious provisions related to defamation and police searches without a warrant were removed by royal decree in September.[39]

For the most part, Jordan's leadership has not made use of these laws to severely punish domestic political opponents, though some online commentators have faced legal harassment.[40] In a troubling development, since early 2011, several online journalists have been brought before the military-dominated State Security Court (SSC) on charges related to their writings. In July 2011, Jordanian journalist Alaa' Fazzaa' was arrested for "working to change the constitution by unlawful means" after he reported about a Facebook group supporting reinstatement of Prince Hamza, King Abdullah's half-brother, as crown prince.[41] He was released several days later. During the year, Fazzaa' also faced prosecution for an article he authored on the news website *Khabarjo* in which he accused senior officials of inappropriately allowing convicted business tycoon Khalid Shahin to leave the country.[42] The charges against Fazzaa' were later dropped as part of a general amnesty.[43]

In April 2012, Jamal al-Muhtaseb, the publisher and owner of the *Gerasa News* website, was charged by the SSC with "opposing the ruling system," after the site published an article alleging that the Royal Court had directed a parliamentary committee not to refer a former minister's corruption case to trial.[44] The SSC ordered that Muhtaseb be held in pre-trial detention for 14 days.[45] The article's author, Sahar al-Muhtaseb, was also arrested but was

[39] International Freedom of Expression Exchange (IFEX), "Government yields to protests, modifies cyber crimes law," news release, September 3, 2010, http://ifex.org/jordan/2010/09/03/cyber_crimes_law/; Official Website of the Prime Ministry of the Hashemite Kingdom of Jordan [in Arabic], http://www.pm.gov.jo/arabic/index.php?page_type=gov_paper&part=3&id=5056.

[40] Oula Farawati, "Jordan's News Websites Running for Legal Cover," Menassat, March 11, 2009, http://www.menassat.com/?q=ar/comment/reply/6143.

[41] James M. Dorsey, "Assad Criticism Isolates Iran, Fails to Tackle Key Issues," MidEast Posts, September 8, 2011, http://mideastposts.com/2011/08/09/assad-criticism-isolates-iran-fails-to-address-key-issues/.

[42] AFP, "Jordan frees journalist held for 'undermining throne," Google News, http://www.google.com/hostednews/afp/article/ALeqM5gqpn0B98i6cWhwxx2TJvrRGILmFg?docId=CNG.7e8c9b730d578a188e3f19c677e0e598.131.

[43] James M. Dorsey, "Assad Criticism Isolates Iran, Fails to Tackle Key Issues," MidEast Posts, September 8, 2011, http://mideastposts.com/2011/08/09/assad-criticism-isolates-iran-fails-to-address-key-issues/.

[44] "Jordanian journalist arrested over critical article," Committee to Protect Journalists, April 25, 2012, http://cpj.org/2012/04/jordanian-journalist-arrested-over-critical-articl.php.

[45] Muhtaseb was released on bail in mid-May after 21 days in detention, but the charges against him were still pending. See, "Journalist Freed on Bail After 21 Days in Custody, Still Faces Prosecution," Reporters Without Borders, May 14, 2012, http://en.rsf.org/jordan-journalist-to-be-tried-before-25-04-2012,42354.html.

released on bail the same day. No bloggers or online journalists were serving prison terms as of May 2012, as several previously detained writers were released following royal pardons.

Jordanians are careful when they talk on mobile phones and extra prudent about what they say at public meetings. This attitude has passed naturally to the internet, because it is believed that security services closely monitor online comments, documenting them by date, internet-protocol (IP) address, and location. In a 2010 case that strengthened these suspicions, a Jordanian college student Imad al-Ash was sentenced to two years in prison after security forces accused him of insulting the king in an instant message to a friend and of posting "controversial religious opinions" in public online forums;[46] he was subsequently released after a royal pardon.

Cybercafes, where users might otherwise write with relative anonymity, have been subjected to a growing set of restrictive regulations in recent years. Since mid-2010, operators have been obliged to install security cameras to monitor customers, who in turn must supply personal identification information before they use the internet. Cafe owners are required to retain the browsing history of users for at least six months.[47] Authorities claim these restrictions are needed for security reasons. Although enforcement is somewhat lax, the once thriving cybercafe business is now in decline due to the restrictions as well as the decrease in the cost of home connections. Despite these restrictions, some data protection provisions are in place. For example, the legislation that regulates the telecommunications sector prescribes fines and one month to one year in prison for the distribution of improperly obtained content from any internet or telephone communication.[48]

Since January 2011, incidents of intimidation and physical attacks against bloggers and staff of online news websites have notably increased. According to Human Rights Watch, in February 2011, unknown assailants attacked Basil al-Ukur, and threatened Samir al-Hiyari, executives at the popular news website *Ammon News*.[49] Although the reason for the attack is unclear, the timing suggested it may have been related to the website's coverage of protests in Amman calling for major economic and political reforms. The following month, Sami Zubaidi, a prominent columnist and editor at another news website *Amman Post* reported

[46]Ahmad Al-Shagra, "Jordanian Student Sentenced to 2 Years Over IM," The Next Web, July 19, 2010, http://thenextweb.com/me/2010/07/19/royal-ash-jordanian-student-sentenced-to-jail-for-2-years-over-im/.
[47] International Freedom of Expression Exchange (IFEX), "Cyber crime law attacks free expression; Internet cafés monitored," News Release, August 18, 2010, http://www.ifex.org/jordan/2010/08/18/cyber_cafe/; "Interior requires internet cafes to install surveillance cameras and keep internet visits for months" [in Arabic], Saraya News, June 3, 2010, http://www.sarayanews.com/object-article/view/id/23211.
[48] Law No. 13 of 1995 and its amendment, Law No. 8 of 2002. "Jordan," *One Social Network With A Rebellious Message,* Arabic Network for Human Rights Information, 2009, http://www.openarab.net/en/node/1618.
[49] Human Rights Watch, *World Report 2012: Jordan*, 2011, http://www.hrw.org/world-report-2012/world-report-2012-jordan.

that a member of parliament threatened him with physical harm.[50] In a more serious incident in February 2012, female blogger Enass Musallam was stabbed and her attacker indirectly referenced her political writings. The assault occurred shortly after she published a blog post criticizing Jordan's Prince Hassan for derisive comments he made about pro-reform protesters.[51] Jordanian authorities denied the attack was related to her blog post or activism, but Musallam reported being harassed by police and called a liar after filing a complaint.[52]

In addition to attacks on particular individuals, the offices of at least one news website were also targeted. In April 2011, six men raided the office of *Al-Muharrir* in Amman, beating one employee and destroying a computer. The men stormed the office of editor-in-chief Jihad Abu Baidar, threatening to kill him and burn down the workplace if he did not withdraw an article on an anti-corruption commission investigation of former chief of staff, General Khaled Jamil al-Saraira.[53] News websites and online writers also face intimidation by conservative readers, who have been known flood their comments sections with threatening messages in a bid to muzzle independent thought and free expression.

Popular news websites have also been subjected to hacking attacks after posting sensitive material or during times of social tension. As noted above, in February 2011, *Ammon News* had its website hacked after publishing a call for reform by tribal leaders. At first, content was deleted or manipulated, then users began being redirected to a page saying, "This site was hacked because you work against the security of Jordan." For several days, both the work and personal email accounts of editors were inaccessible.[54] The following month, the opposition Islamic Action Front reported that its site had also been hacked a day after the group called for the prime minister's ouster.[55] The staff of these websites accused Jordan's intelligence agencies of carrying out the attacks, but the government denied the allegations.

[50] Ibid.
[51] International Freedom of Expression Exchange (IFEX), "Blogger stabbed after criticizing royal family member," news release, February 27, 2012, http://www.ifex.org/jordan/2012/02/27/musallam_stabbed/.
[52] "In Jordan, blogger stabbed after criticizing the royal family," Committee to Protect Journalists, February 29, 2012, http://cpj.org/2012/02/in-jordan-blogger-stabbed-after-criticizing-the-ro.php.
[53] "CPJ condemns attack on office of news website," Committee to Protect Journalists, April 19, 2011, http://cpj.org/2011/04/cpj-condemns-attack-on-office-of-website.php.
[54] International Freedom of Expression Exchange (IFEX), "News website hacked after publishing sensitive statement," news release, February 9, 2011, http://www.ifex.org/jordan/2011/02/11/ammon_news_hacked/.
[55] "Jordan Islamist Opposition Says Website Hacked," France24, March 27, 2011, http://www.france24.com/en/20110327-jordan-islamist-opposition-says-website-hacked (link discontinued).

KAZAKHSTAN

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	16	15
Limits on Content (0-35)	22	23
Violations of User Rights (0-40)	17	20
Total (0-100)	**55**	**58**

* 0=most free, 100=least free

POPULATION: 17 million
INTERNET PENETRATION 2011: 45 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Kazakhstan's government regards the internet and other information and communication technologies (ICTs) as a potential source of growth in the quest for diversification of economy, which is highly dependent on extractive industries. With that goal in mind, the government has made efforts to liberalize the telecommunications sector and promote internet use by enhancing websites of state entities and facilitating the introduction of new data transfer technologies. At the same time, the authorities fear the internet's democratizing potential and have begun attempting to control citizens' access to information. In recent years, the authorities have tried to assert broader control over internet content, particularly on issues deemed threatening to the reputation of long-ruling President Nursultan Nazarbayev and on national security concerns.

Since January 2011, the environment for internet freedom has become precarious, catalyzed by the government's response to a number of bombings attributed to religious extremists and a state of emergency declared after violent clashes between oil strikers and police in the city of Zhanaozen in western Kazakhstan in December 2011.[1] As such, the past year and a half has witnessed the increased filtering of websites, revival of the block on the blog-hosting service LiveJournal, intensified surveillance at cybercafes, and some of the first serious physical assaults on bloggers and online journalists.

Senior officials have also been signaling that further restrictions may be in store. In

[1] "Kazakh authorities censor news on deadly clashes," Committee to Protect Journalists, December 20, 2011, http://cpj.org/2011/12/kazakh-authorities-censor-news-on-deadly-clashes.php.

September 2011, the general prosecutor was quoted as saying, "the question of control over social networks, over the internet, is a question of time…countries must join efforts to counter this evil." [2] Two months later, a key policy document on "Information Security until 2016" was approved by a presidential decree with the warning that the "wide use of social networks and blogs by the Kazakhstani population creates possibilities for their utilization with the aim of deliberately influencing the internal political situation." [3]

OBSTACLES TO ACCESS

Internet access has grown exponentially in Kazahkstan, increasing from a 3.3 percent penetration rate in 2006 to 45 percent in 2011, according to the International Telecommunication Union (ITU),[4] though official government statistics cite a penetration rate of over 53 percent as of the end of 2011.[5] Experts have questioned the official statistics, arguing that the authorities count users of fixed and mobile internet separately, even though many individuals access the internet via both mobile and fixed-line connections.[6] In terms of user demography, 57 percent are female and 62 percent are between the ages 25 and 34.[7]

A growing number of people prefer to go online from home, alongside continued access at public libraries, educational institutions, and workplaces. Internet speeds offered by the state-run operator Kazakhtelecom and private internet service providers (ISPs) have grown at a slow but stable pace. Prices remains relatively high for the majority of the population but have decreased in recent years,[8] with unlimited broadband access contracts starting from US$14 a month compared to the average monthly income of approximately US$670.[9] Internet packages for most fixed-line subscribers in Kazakhstan are broken into a two-tiered

[2] Interfax News Agency, "Юрий Чайка налетел на соцсети" [Yuri Chaika attacked social networks], September 14, 2011, http://www.interfax.ru/politics/txt.asp?id=207849.
[3] Presidential Decree #174, dated November 14, 2011, text published by Nomad.Su, December 6, 2011, http://www.nomad.su/?a=3-201112060038.
[4] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[5] "Количество интернет-пользователей в Казахстане увеличилось до 8,7 млн. человек" [Kazakhstan's internet users reach 8.7 million], Caspionet.kz, February 25, 2012, http://caspionet.kz/eng/business/Kolichestvo_internetpoljzovatelej_v_Kazahstane_previsilo_8_7_mln__chelovek_1330177496.html.
[6] "Insufficient level of Internet penetration…" [Недостаточно высокий уровень проникновения Интернета…], Zakon, May 8, 2010, http://www.zakon.kz/171765-nedostatochno-vysokijj-uroven.html.
[7] "Контент в Казнете" [Content in KazNet], Institute of Political Solutions, October 6, 2011, http://ipr.kz/kipr/3/1/56.
[8] "Минсвязи обещает дальнейшее снижение тарифов на интернет и услуги связи" [Ministry of communications promises further decrease of tariffs for internet and telecoms], Newskaz.ru, September 14, 2011, http://newskaz.ru/society/20110914/1887966.html.
[9] "Средние заработные платы" [Average Monthly Income], Mojazarplata.kz, accessed June 6, 2012, http://mojazarplata.kz/main/srednie-zarabotnye-platy.

system: access to information hosted inside the country is unlimited, but for content hosted outside, contracts usually have a quota on traffic. If the quota is exceeded, the connection speed slows down, though no extra fee is charged.

Mobile phone penetration is significantly higher than internet usage, with a penetration rate of over 142 percent in 2011, up from 51 percent in 2006.[10] Since the launch of 3G data packages and the lowering of prices in late-2010, a growing number of people have been accessing the internet on their mobile phones or tablet computers. The deployment of 3G services was under way throughout 2011, and the authorities announced plans in May to introduce 4G technologies in the near future.[11]

Since 2009, WiMAX networks have also become available in Kazakhstan, including those offering retail options. The number of free WiFi hotspots in public places in big cities has been growing, while cybercafes continue to enjoy a stable customer base, especially when they are part of a chain. Following government instructions, Kazakhtelecom has set up public hotspots and terminals within government agencies for public access without charge, but the stations only provide access to e-government services and websites.

Kazakhstan's ".kz" internet country code was introduced in 1994. Currently there are more than 66,000 domains registered in the Kazakhstani segment of the internet, dubbed KazNet, though only about 10,000 are active, and even fewer receive at least 100 visitors per day.[12] The government has initiated several programs to stimulate internet use, lower the digital divide, and expand e-government functions. This trend continued in 2011 with the launch of the Program on Development of Information and Communication Technologies in the Republic of Kazakhstan for 2010-2014.[13] In addition to expanding infrastructure to connect more citizens to the internet and mobile phone networks, the plan envisages growth of locally-produced and export-oriented ICT technologies and services.

Social-networking platforms and other Web 2.0 applications are increasingly popular in Kazakhstan. The government has invested substantial funding into creating local websites and online services, including a Kazakh video-hosting website and a national social network. Nevertheless, the most accessed online resources from Kazakhstan remain foreign ones,

[10] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[11] "План по высвобождению частот для 4G направлен в правительство Казахстана" [Plan of frequencies allocation for 4G is sent to the government], Today.kz, May 23, 2011, http://www.today.kz/ru/news/science/2011-05-23/44532.

[12] Chulpan Gumarova, "Количество – не значит качество" [Quantity does not mean quality], Kapital newspaper, January 18, 2012, http://www.kapital.kz/gazeta/biznes/4293-2012-01-18-16-50-32.html.

[13] Программа по развитию информационных и коммуникационных технологий в Республике Казахстан на 2010 – 2014 годы, [Program on Development of Information and Communication Technologies in the Republic of Kazakhstan for 2010-2014], September 29, 2010, http://mci.gov.kz/main/?option=com_content&task=view&id=661&Itemid=29.

especially Russia-based social-networking platforms like Mail.Ru and Vkontakte.ru, as well as the search engine portals, Google and Yandex. YouTube, Facebook, Wikipedia, and Twitter are also growing in popularity. The most visited Kazakh site (with a ".kz" domain) as of April 2012 was the multifunctional portal Nur.Kz, resting in 14th place.[14]

Web 2.0 applications have been periodically blocked in Kazakhstan in recent years, though the government has not always admitted their intent behind the restrictions. The international blog-hosting platform LiveJournal was blocked for over two years from October 2008 to November 2010 by the two largest ISPs, the state-owned Kazakhtelecom, and Nursat.[15] The impetus for the block was ostensibly to restrict access to politically sensitive content related to the President Nazarbayev's former son-in-law Rakhat Aliyev.[16] The website was unblocked in after the disputed blog was frozen by LiveJournal administrators.[17]

Access to LiveJournal was blocked again in August 2011, along with the Russian social-networking website Liveinternet.ru. This time, a court ordered the block under claims that some accounts on the platforms were disseminating religious extremism.[18] A LiveJournal spokeswoman stated that the company had never received any official notice from the Kazakhstan government identifying certain accounts as extremist and requesting their removal, an action the blog-hosting provider claimed it would take if the concerns were found to be legitimate. This contributed to suspicions that the government's claims of "religious extremism" were an excuse to block content deemed undesirable for political, not national security, reasons.[19] Liveinternet.ru was subsequently unblocked, but LiveJournal remained inaccessible from Kazakhstan as of mid-2012. In April 2012, the Yessil District Court of Astana upheld the block while considering an appeal made by blogger Anatoly Utbanov, who argued that the wholesale blocking of LiveJournal was disproportionate

[14] "Top Sites in Kazakhstan," Alexa, accessed April 29, 2012, http://www.alexa.com/topsites/countries/KZ.
[15] Karin Deutsch Karlekar, eds., "Kazakhstan," *Freedom of the Press 2009* (New York: Freedom House, 2008), http://www.freedomhouse.org/template.cfm?page=251&year=2009; Ardak Bukeyeva and Svetlana Isaeva, "Киберцензоры vs Интернет" [Cybercensors vs. Internet], Kursiv newspaper, April 29, 2010, http://www.kursiv.kz/arhiv/tendencii-arhiv/1195203514-kibercenzory-vs-internet.html.
[16] Rakhat Aliyev, Nazarbayev's former son-in-law, had served in top positions in the country's secret services and diplomatic service. He had large business and media holdings before definitively falling out of favor with the president and his family in 2008 after he had faced multiple charges of abduction, financial crimes and a coup attempt. Having fled abroad, Aliyev began airing inside information and allegations, in the traditional media and online, in an effort to discredit the president. Materials related to Aliyev have been systematically filtered, and republication of excerpts from his book "Godfather-in-law" is officially banned.[16] Many observers believe that Nazarbayev's conflict with Aliyev was the primary reason for the first blockage of LiveJournal in Kazakhstan, and also accelerated adoption of the internet-related legal amendments in 2009.
[17] Adil Nurmakov, "Kazakhstan: Livejournal Unblocked After 2 Years of Filtering," Global Voices Online, November 17, 2010, http://globalvoicesonline.org/2010/11/17/kazakhstan-livejournal-unblocked-after-2-years-of-filtering/.
[18] "Kazakhstan blocks websites to battle religious extremism," Neweurasia.net, September 9, 2011, http://www.neweurasia.net/media-and-internet/kazakhstan-blocks-websites-to-battle-religious-extremism/.
[19] "LiverJournal portal, several blogs suspended," IFEX, September 2, 2012, http://www.ifex.org/kazakhstan/2011/09/02/livejournal_suspended/.

punishment for just two extremist blogs. In response, a representative of the Ministry of Communication and Information lamented the country's inability to filter separate accounts, asserting that the technical capacity should be in place by July 2012.[20]

The blog-hosting platforms Blogger.com and Wordpress.com were also periodically filtered throughout much of 2011. In February 2011, a district court in Astana banned two Wordpress pages for disseminating content related to religious extremism, but this resulted in the blocking of the whole platform.[21] Currently, Kazakhstani users can only access the main page of Wordpress.com and Blogger.com but not the blogs hosted by the platforms. Users from Kazakhstan also persistently report trouble accessing some of the Google's other services, including the server Googleusercontent.com that hosts attachments sent in Gmail, the Picasa image bank, and Google Translate's URL translation function (which is also powered by Googleusercontent.com).[22] Google's search engine is accessible and is the second most visited website in the country.[23]

In in mid-December 2011, mobile phone and internet communications were cut off in the city of Zhanaozen, a town in western Kazakhstan, for several days. The shutdown occurred after clashes between striking oil workers and police that left 15 people dead and 100 injured. On December 16, the first day of the unrest, Kazakhstan users also reported being unable to access Twitter.[24] Kazakhtelecom released a statement denying any intentional blocking, instead citing possible technical problems on the side of website as the cause,[25] while the authorities blamed the blackout on the riots and arson, which had damaged communication lines and electricity intermissions.[26] The next day, the president declared a state of emergency and curfew in the city.[27] Some observers believed the blocks were a government attempt to prevent details of the unrest from spreading, including evidence of

[20] "Суд подтвердил законность блокировки ЖЖ" [Court confirmed legitimacy of LiveJournal's block], Zakon.kz, April 18, 2012, http://www.zakon.kz/4485779-sud-podtverdil-zakonnost-blokirovki-zhzh.html.

[21] Svetlana Glushkova, "Портал Вордпресс заблокировали из-за двух блогов" [Wordpress portal was closed because of two blogs], Azattyq.org, July 12, 2011, http://rus.azattyq.org/content/worldpress_kazakhtelecom_blocking_blog_/24262786.html.

[22] See Google Help forum thread (in Russian) at https://groups.google.com/a/googleproductforums.com/forum/#!category-topic/gmail-ru/?????-???????/dJV0yhvaG08, accessed January 24, 2012.

[23] "Top Sites in Kazakhstan," Alexa, accessed April 29, 2012, http://www.alexa.com/topsites/countries/KZ.

[24] Isabel Gorst, "State of emergency after Kazakhstan clashes," Financial Times, December 17, 2011, http://www.ft.com/cms/s/0/65d6044e-27f8-11e1-9433-00144feabdc0.html#axzz1kYUkrfn4.

[25] "В Жанаозене полностью отсутствует сотовая связь и доступ к сети Интернет" [There is no cellular communication and internet access in Zhanaozen], Zakon.kz, December 18, 2011, http://www.zakon.kz/4463391-v-zhanaozene-polnostju-otsutstvuet.html; "Казахтелеком" не блокировал доступ к сайтам 16 декабря" [Kazakhtelecom did not block access to websites on December 16], Nur.kz, December 17, 2011, http://news.nur.kz/203939.html.

[26] "МСИ разъяснило ситуацию со связью в Жанаозене" [Ministry of Communications and Information explained the situation with connectivity in Zhanaozen], Tengrinews.kz, December 17, 2011, http://tengrinews.kz/kazakhstan_news/204082/.

[27] Isabel Gorst, "State of emergency after Kazakhstan clashes," Financial Times.

officers opening fire on unarmed protestors.[28] Others believed the purpose was to prevent the deliberate spread of misinformation, as the official information confirming the clashes and victims was made public in the evening of the same day. Two days before the Zhanaozen riots, the parliament had adopted amendments and addenda to the Law of National Security, which reserve the government's right to forcibly suspend communications services during counter-terrorist operations or suppression of mass riots (Article 23.4).[29] The amendments came into force in January 2012.

The state owns 51 percent of Kazakhtelecom, the largest ISP, which holds a 70 percent share in the internet access market.[30] Another five operators are licensed to connect to the international internet, but they are required to channel at least part of their traffic through Kazakhtelecom's backbone network facilities infrastructure.[31] Over 100 other ISPs operate in Kazakhstan but have to purchase traffic via the above-mentioned six, making it difficult for them to compete in the market. Kazakhtelecom's dominance over information flow routes creates the conditions for systemic content filtering and surveillance.

As of early 2012, there are four mobile telephone providers in Kazakhstan, including three using the GSM standard (GSM Kazakhstan, Beeline, and TELE2) and one using CDMA (Altel). Kazakhtelecom used to hold a 49 percent stake in GSM Kazakhstan but sold its shares to the Finnish company TeliaSonera for US$1.5 billion in December 2011 as part of the company's asset restructuring strategy. [32] Beeline belongs to the Russian mobile operator Vimpelcom, which acquired the Kartel company and its K-Mobile system in 2005.[33]

Several bodies regulate the ICT sector, with the main regulators being periodically reorganized. The most recent shift in January 2012 gave the responsibility for the technology sector to the newly established Ministry of Transport and Communications, while entrusting information-related regulation to the Ministry of Culture and Information. Until that point, both functions were filled by the now dissolved Ministry of Communications and Information, whose head became the new Minister for Transport and Communications.

[28] "Kazakh Authorities Censor News on Deadly Clashes," Committee to Protect Journalists, December 20, 2011, www.cpj.org/2011/12/kazakh-authorities-censor-news-on-deadly-clashes.php.

[29] "Республики Казахстан О национальной безопасности Республики Казахстан" [The Law on National Security], Zakon.kz, July 10, 2012, http://online.zakon.kz/Document/?doc_id=31106860&mode=all.

[30] Kazakhstan Stock Exchange, http://www.kase.kz/ru/emitters/show/KZTK;
Kazakhtelecom presentation, "Kazakhtelecom JSC – national operator of telecommunications in Kazakhstan," 2011, pg. 22, accessed on January 24, 2012, http://www.telecom.kz/download/Presentacia1.pdf.

[31] OpenNet Initiative, "Country Profile: Kazakhstan," *Access Controlled*, accessed September 23, 2010, http://www.access-controlled.net/wp-content/PDFs/part2/007_Kazakhstan.pdf.

[32] "Казахтелеком" продал шведской компании долю в Kcell" [Kazakhtelecom sold its stake in Kcell to the Swedish company], Nur.kz, December 22, 2011, http://news.nur.kz/204394.html.

[33] "Kartel (K-Mobile) GSM Network Expansion, Kazakhstan," Mobilecomms Technology, accessed February 15, 2011, http://www.mobilecomms-technology.com/projects/kartel/.

The ".kz" country code is managed by a registry, the Kazakhstani Network Information Center (KazNIC), and the Kazakhstani Association of IT Companies. Both were created in 2004–05 as formally nongovernmental organizations, but in practice, they are believed to be under close control of the authorities and have been known to make politicized decisions on registration and de-registration of the ".kz" domain names.[34] The government has at various times demanded that any website with a ".kz" country domain physically host its servers on the territory of Kazakhstan. Such regulations were first introduced in April 2005, but the relevant authorities made little effort to enforce them.

In September 2010, the government declared its intention to fully enforce the regulation, prompting several controversies. The most prominent dispute took place in June 2011, when Google redirected all of the traffic from its localized Google.kz page to Google.com rather than comply with the demand to move its servers in-country, which it said would contribute to a "fractured internet" and ultimately harm Kazakh users.[35] Shortly after the dispute became public, the government retreated and the Kazkahstani Association of IT Companies explained that the rule applies only to domain names registered after September 7, 2010.[36]

LIMITS ON CONTENT

In the past, the Kazakhstan government's online censorship was often selective, sporadic, and inconsistent, but in 2011, it became more institutionalized and hermetic. In particular, filtering expanded from Kazakhtelecom to other ISPs, while the authorities sought to undermine the effectiveness of circumvention tools and the courts began using recently-passed laws on "religious extremism" to block websites.

According to the most recent testing conducted by the OpenNet Initiative (ONI) in 2010 on two principle ISPs, access was blocked—particularly by Kazakhtelecom—to some "opposition…websites, regional media sites that carry political content…selected social networking sites, [and] a number of proxy sites."[37] At the time, ONI found that censorship was often inconsistent because in some cases, blocks were only implemented by Kazakhtelecom. International news sites such as the BBC, Radio Free Europe/Radio Liberty (RFE/RL), and the New York Times and websites of international organizations such as Human Rights Watch and Freedom House are available.

[34] OpenNet Initiative, "Country Profile: Kazakhstan."
[35] "Changes to the open Internet in Kazakhstan," Official Google Blog, June 7, 2011, http://googleblog.blogspot.com/2011/06/changes-to-open-internet-in-kazakhstan.html.
[36] "Google.kz вернулся в Казахстан" [Google.kz returrned to Kazkahstan], Tengrinews.kz, June 15, 2011, http://tengrinews.kz/internet/190571/.
[37] OpenNet Initiative, "Country Profile: Kazakhstan."

A package of legislative amendments adopted in July 2009, which received significant domestic and international criticism, granted the state broad authority to block access to foreign online resources whose content is deemed to run counter to national laws. The amendments declared that the internet and all websites—referred to as "internet resources"—were to be considered media outlets without differentiating between news sites, blogs, chat rooms, etc. The amendments also granted the state the power to suspend and/or shut down websites hosted within Kazakhstan, including any website with content deemed to harm the interests of the public and the state. Publications involving classified information, extremist propaganda, and pornography can also be restricted. Moreover, under the amendments, all ISPs are required to ensure blockage of banned websites, and the owners of internet resources are responsible for any content, posted by themselves or other users, that is deemed illegal under Kazakhstan's civil, criminal, and administrative laws.[38] The law stipulated that filtering of websites could be applied only with a court decision, though this requirement is not always observed in practice. The amendments have resulted in tighter censorship, ending the phenomenon whereby users could still access pages blocked Kazakhtelecom via alternative operators.

For some time, the 2009 legal amendments stood unimplemented, but after a series of suicide bombings in 2011, several court decisions were issued ordering the blocking of websites for reasons of "religious extremism." In August 2011, a court decision blocked access to LiveJournal and 11 other websites based on claims that the websites or certain webpages were disseminating content with signs of religious extremism.[39] As of October 2011, access to 125 websites was blocked in Kazakhstan for carrying religious extremist content and terrorism propaganda, and 168 more were awaiting a court decision, according to the nation's Security Council spokesperson.[40]

Despite these legal precedents, the filtering of websites without court decisions continues. In March 2010, the Computer Emergency Response Team (CERT) was established in Kazakhstan and operates as a governmental body under the Ministry of Communications. In contrast to many of its foreign counterparts, whose mandate is restricted to address only technical incidents, Kazakhstan's CERT also aspires to fight "destructive content" and "political extremism" by blacklisting and banning certain sites.[41] In March 2010, when

[38] "Парламент принял закон, усиливающий контроль над интернет-ресурсами в Казахстане" [Parliament adopted law to increase control over internet resources in Kazakhstan], Zakon.kz, June 24, 2009, http://www.zakon.kz/141606-parlament-prinjal-zakon-usilivajushhijj.html.

[39] "Kazakhstan blocks websites to battle religious extremism," Neweurasia.net, September 9, 2011, http://www.neweurasia.net/media-and-internet/kazakhstan-blocks-websites-to-battle-religious-extremism/.

[40] "В Казахстане закрыли доступ к 125 сайтам" [Kazakhstan closed access to 125 websites], Tengrinews.kz. October 1, 2011, http://tengrinews.kz/kazakhstan_news/198106/.

[41] "В Казахстане начались проверки "неправильных" сайтов" [Checks of 'undue' websites started in Kazkahstan], Nur.kz, March 1, 2010, http://news.nur.kz/144920.html.

probed about the transparency of their work, a CERT spokesperson said that the team's activity, including its criteria for blacklisting and the lists of blocked websites, is considered secret.[42]

One of the most notable cases of extralegal blocking has been the restrictions placed on the main website of *Respublika*, an opposition weekly paper known for its criticism of the government, which was blocked for most Kazakh users throughout 2011. The blocking was implemented without court order, and in fact, both the government and Kazakhtelecom executives have denied censoring *Respublika*, attributing its inaccessibility to the website's own technical problem. The publication, financed by Mukhtar Ablyazov (a fugitive businessman and former bank owner now living in self-imposed exile somewhere in Europe), uses social networks extensively to disseminate its journalistic content and regularly updates readers on available anonymizers and other circumvention tools. The website of satellite TV channel K+, also financed by Ablyazov, is inaccessible from Kazakhstan as well.

In another example of extralegal filtering beginning in early 2011, anonymizing tools were increasingly being filtered in Kazakhstan, though no court decision had been issued against them. Many users wishing to circumvent censorship instead switched to browsers designed by the Opera Corporation,[43] whose traffic compression feature initially meant to facilitate browsing with slow connections but now enables users to access blocked websites.

Since early 2009, there has also been an increase in self-censorship and content removal implemented by companies hosting online information, with many websites disabling comments to their articles.[44] With the 2009 internet-related amendments coming into force, most online content providers intensified their moderation practices to monitor and censor content that could expose them to legal repercussions. The self-censorship environment solidified further following the July 2010 adoption of a law granting President Nazarbayev the status of "Leader of the Nation," which essentially places any criticism of him and his family under the umbrella of threats to national security or reputation.

The 2008 blocking of LiveJournal, at the time the most popular blogging platform in Kazakhstan, generated significant changes to the country's blogosphere.[45] There were no

[42] "Служба реагирования на компьютерные инциденты рассказала о своей работе" [Computer emergency response team told about its work], Zakon.kz, March 25, 2010, http://www.profit.kz/articles/001196/.
[43] "Web browser that bypasses big brother a Kazakh hit," Reuters, April 13, 2010, http://www.reuters.com/article/2010/04/13/us-kazakhstan-internet-browser-idUSTRE63C37N20100413.
[44] Carl Schreck, "Kazakhstan Puts Pressure on Bloggers," The National, August 25, 2009, http://www.thenational.ae/apps/pbcs.dll/article?AID=/20090825/FOREIGN/708249847/1140.
[45] SUP Media, "LiveJournal in Figures. Autumn 2007," presentation, November 30, 2007, http://www.sup.com/stat_autumn07.pdf.

major local blogging platforms at the time. Since then, Yvision.kz has emerged as the most popular Kazakhstan-based blog-hosting platform, with over 60,000 users as of December 2011, most of them blogging in Russian. Noticing the emerging market for blog-hosting platforms, several other blogging projects have emerged since then, but few have succeeded in garnering a significant and active membership, thus leaving Yvision.kz in a dominant position. As a whole, the local blogosphere remains a relatively small community with room to grow.

The Kazakh blogosphere is dominated by the younger generation, but recent years have witnessed broader engagement of professionals, journalists, academics, members of parliament and other public figures, particularly on social networks. A 2011 survey by JSC Kazkontent found that 37 percent of respondents used social-networking sites, and that 38 percent published or read blogs and took part in forums.[46] In 2011, as political activists began to more vigorously use social media to spread their message, the authorities responded by sometimes relying on popular, yet relatively loyal, bloggers to engage in propaganda campaigns, inviting them on "blogger tours," such as the tours to Baikonur Cosmodrome for the launch of the second Kazakh satellite in July 2011 and to Zhanaozen after the riots in December 2011. Both the government and bloggers deny having financial ties to each other.

In an effort to counter criticism of the blocking of LiveJournal and to demonstrate a willingness to engage with citizens online, officials have started maintaining their own blogs in recent years. The website of every government body and local administration is required to have a blog. The website Blogs.egov.kz is called "the official blogging platform for high-ranking Kazakh officials" and is home to the blog of Prime Minister Karim Masimov.[47] Masimov is also an active Twitter user, setting a trend for other government officials to use the microblogging service to reach citizens, and news agencies increasingly quote officials' Twitter posts in their coverage.

Many candidates in the 2011 presidential and 2012 parliamentary elections set up Facebook and Twitter accounts for their campaigns, and the degree of their involvement in online debates grew significantly compared to previous years. This did not appear to affect the results much, however, as Nazarbayev won over 95 percent in elections that international observers found to be seriously flawed. In advance of parliamentary polls in January 2012, more politicians, especially those belonging to the radical, nationalist opposition party

[46] "Обзор казахстанского Интернет-рынка 2007-11" [Review of Kazakhstani internet market in 2007-11], Kazkontent, report, April 14, 2011. http://kzcontent.kz/rus/kaznet_3/12.
[47] Adil Nurmakov, "Kazakhstan: Prime Minister Launched Blog," Global Voices, January 16, 2009, http://globalvoicesonline.org/2009/01/16/kazakhstan-prime-minister-launched-blog/.

Rukhaniyat (Spirituality) who were disqualified from the vote in December 2011, used Facebook to win new supporters and advocate their platform.

Another important incident during the year involved coverage of the oil workers' strike in Zhanaozen in December 2011 that ended in violent clashes. Initially, the government and state-run media sought to place full blame for the violence on protestors, but then footage of police firing on unarmed protestors was recorded and uploaded to the YouTube, ultimately forcing the authorities to admit that the police had contributed to the violence and to put several officers on trial.[48] The government tried over 30 strikers with organizing the unrest based on charges some observers deemed unfair, particularly amidst reports of beatings and torture of detainees. Despite the positive role played by online tools in this instance, some observers cited negative effects as well, including the viral spread of rumors and manipulative misinformation over blogs and social networks, particularly over Twitter and Facebook.

Overall, civil society activists and the blogging community lack coordination and an understanding of one another's needs. This, in addition to the low level of civic consciousness and political literacy, results in limited political online activism in Kazakhstan. On the other hand, in areas of non-political activism—such as environmental advocacy (like the campaign against construction of ski resort in the nature reserve near Almaty[49]) and charitable campaigns (for example, fundraising for the disabled on blogosphere and social-networking sites)—social media has repeatedly made a difference.

VIOLATIONS OF USER RIGHTS

The Kazakhstan constitution guarantees freedom of the press, but it also provides special protection for the president. In practice, the authorities use various legislative and administrative tactics to control the media and limit free expression. Since 2008, they have also taken steps to change the legal landscape for the media. Under pressure from the Organization for Security and Cooperation in Europe (OSCE) ahead of Kazakhstan's presidency of the organization, a few amendments aimed at liberalizing media legislation were adopted in February 2009.[50] Although the amendments reduced some bureaucratic obstacles, they did little to contribute to broader political liberalization.

[48] "Kazakh police on trial over Zhanaozen violence," BBC, April 27, 2012, http://www.bbc.co.uk/news/world-asia-17867171; Hugh Williamson, "Kazakhstan: Letter to the Prosecutor General regarding the December events in Khanaozen and Shetpe," Human Rights Watch, February 1, 2012, http://www.hrw.org/news/2012/02/01/kazakhstan-letter-prosecutor-general-regarding-december-events-zhanaozen-and-shetpe.

[49] See campaign's website at http://k-zh.kz/, which features its representations in social networks.

[50] Human Rights Watch, "Human Rights in Kazakhstan."

In 2010, the parliament passed a law granting President Nazarbayev the status of "Leader of the Nation," which attached criminal responsibility to any damage done to his image, including public insults or distortion of his private biographical facts, among other provisions. More broadly, defamation remains a criminal offense and Kazakh officials have a track record of using libel to punish critical reporting.

Although cases of imprisonment of journalists or human rights defenders have occurred in recent years, no bloggers were prosecuted or jailed in 2011 and early 2012. However, as online journalists and bloggers sought to cover the aftermath of violent clashes in Zhanaozen alongside their colleagues from traditional media outlets, several individuals were detained, threatened, or assaulted. In December 2011, Ilya Azar, a journalist from the Lenta.ru news website was detained for four hours and forced to delete recorded interviews.[51] A few days later, blogger and activist Murat Tungishbayev was reportedly assaulted by police in the Magistau region who held a pistol to his head after he uploaded video footage to YouTube showing local residents holding a rally to protest the crackdown. He was released when other journalists rushed to the scene.[52] In a separate but related incident in October 2011, journalists and a cameraman from the online TV and production studio Stan.tv were assaulted by unknown assailants with baseball bats when visiting west Kazakhstan to report on the oil workers' strike that had been ongoing for several months prior to the violence that broke out in December.[53] In that instance, the authorities launched an investigation into the assault, identifying two suspects now reportedly wanted by police.[54]

In another incident of apparent harassment against Stan.tv, its office was visited by inspectors from the sanitary and epidemiology authorities in August 2011 who claimed that their antennas were emitting "inappropriate levels of … electromagnetic radiation" and posed a threat to the health of nearby residents. The following month, a court ruled that the station would have to stop using the antenna or shut down their production studio. Editors from the station claimed, however, that local residents said they had been pressured by police to write letters complaining about Stan.tv and that the inspections were part of an effort to discourage their independent reporting.[55] The office continued its operations after

[51] "Kazakhstan: Ensure Independent Probe Into Clashes," Human Rights Watch, December 18, 2011, http://www.hrw.org/news/2011/12/18/kazakhstan-ensure-independent-probe-clashes; "Kazakh authorities censor news on deadly clashes," Committee to Protect Journalists, December 20, 2011, http://cpj.org/2011/12/kazakh-authorities-censor-news-on-deadly-clashes.php.

[52] Ibid; "На станции Шетпе избит блогер Мурат Тунгишбаев" [At Shetpe station blogger Murat Tungishbaev beaten], Azattyq.org, December 18, 2011, http://rus.azattyq.org/archive/news/20111218/360/360.html?id=24425730.

[53] "Attack on StanTV journalists caused by their activity – Stan-production," KazTAG, October 27, 2011, http://www.kaztag.kz/en/top-news/71426.

[54] "В розыск объявлены двое подозреваемых в нападении на журналистов Стан ТВ" [Two suspects wanted for attack on Stan TV journalists], Aktau-News, November 9, 2011, http://aktau-news.kz/?p=7600.

[55] "Decision of court of first instance by suit of sanitary-epidemiologic station of Almaly district to LLP «Stan Prodaction» has been affirmed," Adilsoz.kz, December 15, 2011, http://www.adilsoz.kz/en/newsen/decision-of-court-of-first-instance-by-suit-of-sanitary-epidemiologic-station-of-almaly-district-to-llp-stan-prodaction-has-been-affirmed; "Online TV Station in Kazakhstan

complying with the court's demands to pay a fine of around US$350, dismantle its antenna (which was also used to access internet), and opt to use landline access "at the cost of their technical preferences."[56]

Throughout 2011, the issue of copyright enforcement online was a point of heated debate among the government, users, industry representatives, and other stakeholders. In January 2012, the president signed a new law on amendments and addenda in the legislation governing intellectual property rights that criminalizes the illegal use of copyrighted material (punishable by one year in prison) and the organized distribution of such material through a file-sharing hub (punishable by five years in prison).[57] Critics argue that the law's formulations are vague and its punishments harsh, leaving room for selective and arbitrary enforcement, including against civil society groups or opponents of the government. Prior to the new law coming into force in February 2012, already in June 2011, the authorities shut down a popular torrent-tracking website and detained two of its owners.[58] Initially, it appeared that they may face criminal charges, but in the end, the dispute was settled without such punishment, though the owners' computer equipment was confiscated. After the law came into force, the number of torrent-tracking sites dropped dramatically, and users turned to similar sites based outside Kazakhstan, contributing to a general slowing of internet traffic because of the upsurge in international bandwidth use.[59]

On December 30, 2011, the government issued a decree tightening surveillance in cybercafes. Under the decree, cybercafe owners are obliged to gather the personal information of customers and retain their online activities and browsing history. This information is to be retained for no less than six months and can be accessed by "operative-investigatory bodies."[60] The decree also bans the use of circumvention tools in cybercafes. As of February 2012, parts of the decree have begun to come into force, including two provisions that require the installation of video surveillance equipment and filtering software in cybercafes, generating some backlash from both users and cybercafe owners.[61] It remains unclear how these regulations might apply to public WiFi access points.

Ordered to Stop Using Antennas," RFERL.org, September 15, 2011, http://www.rferl.org/content/online_tv_station_in_kazakhstan_ordered_to_stop_using_antennas/24329843.html; "Unhealthy Kazakh journalism, or an unhealthy attack on Kazakh journalist?" NewEurasia.net, October 5, 2011, http://www.neweurasia.net/media-and-internet/unhealthy-kazakh-journalism-or-an-unhealthy-attack-on-kazakh-journalism/.

[56] Email interview with Burzhan Musirov, director of Production Studio Stan TV Ltd., June 13, 2012.

[57] See full text of the law published by the Kazakhstanskaya Pravda newspaper's website on January 12, 2012, http://kazpravda.kz/_pdf/jan12/200112law.pdf, accessed January 24, 2012; Nate Schenkkan, "Kazakhstan: Could Copyright Crackdown Be Next Frontier in Curbing Dissent?" Eurasianet.org, February 14, 2012, http://www.eurasianet.org/node/64998.

[58] "Создателям популярного торрент-трекера грозит уголовная ответственность" [Creators of popular torrent tracker may face criminal charges], Ktk.kz, June 2, 2011, http://www.ktk.kz/ru/news/video/2011/06/02/12789.

[59] Nate Schenkkan, "Kazakhstan: Could Copyright Crackdown Be Next Frontier in Curbing Dissent?"

[60] See, "Rules of rendering internet access services," adopted by the governmental decree #1718 on December 30, 2011, http://medialawca.org/old/document/-11242.

[61] "В интернет-клубы теперь будут пускать только с удостоверением личности" [Internet clubs will demand IDs],

It is difficult to track or verify efforts by the National Security Committee (KNB) or other agencies to monitor internet and mobile phone communications. However, a series of regulations approved in 2004 and updated in 2009 oblige telecom operators (both ISPs and mobile phone providers) to retain records of users' online activities, including phone numbers, billing details, internet protocol (IP) addresses, browsing history, protocols of data transmission, etc., including via installation of special software and hardware.[62] Providers must store user data for two years and grant access to "operative-investigatory bodies" when sanctioned by a prosecutor.[63] Furthermore, SIM card registration is required for mobile phone users at the point of purchase under the Civil Code; however, the requirement is not tightly enforced, and SIM card vendors view the registration as optional.[64]

The administrators of several opposition-related or independent news websites such as *Respublika*, *Kub*, and *Zonakz* that are blocked in Kazakhstan have reported suffering sporadic distributed denial-of-service (DDoS) cyberattacks since 2009.[65] In July 2011, a news and analysis website Guljan.org, established just two months earlier by the former editor-in-chief of the popular newspaper *Svoboda Slova*, reported being targeted by DDoS attacks that were crippling the site.[66] Although many suspect that regime actors were behind the attacks, their origin has been neither independently confirmed nor investigated by the police or CERT, whose responsibility it is to address such incidents.

Zakon.kz, January 25, 2012, http://www.zakon.kz/kazakhstan/4469529-takie-pravila-okazanija-uslug-dostupa-k.html.

[62] Ksenia Bondal, "Следи за базаром - нас слушают" [Watch out, we are watched], Respublika, republished by Zakon.kz, November 5, 2009, http://www.zakon.kz/top_news/152528-objazyvaet-li-ais-i-knb-sotovykh.html.

[63] See, "Rules of rendering internet access services," adopted by the governmental decree #1718 on December 30, 2011, and the Law on operative-investigatory activities, dated September 15, 1994, http://www.minjust.kz/ru/node/10182.

[64] "Сотовая связь: абонент не определен и опасен" [Cellular: caller is uncertain and dangerous], Ipr.kz, June 21, 2011, http://www.ipr.kz/kipr/3/1/51#.T7t40tx1BLc.

[65] "Интернет-СМИ «Фергана.Ру», Zona.kz и «Республика» были атакованы неизвестными хакерами почти одновременно" [Internet Media 'Fergana.ru,' Zona.kz and 'Respublika' Are Attacked by Unknown Hackers Almost Simultaneously], Fergana.ru, February, 20, 2009, http://www.ferghana.ru/news.php?id=11348.

[66] "Website of Gulzhan Ergalieva was Blocked by Kazakhstan DDoS attacks," Adilsoz.kz, July 21, 2011, http://www.adilsoz.kz/en/newsen/website-of-gulzhan-ergalieva-was-blocked-by-kazakhstans-ddos-attacks/; Rachel Van Horn, "Central Asia: Censorship 3.0 and the Struggle for Online Free Speech," Eurasianet.org, November 7, 2011, http://www.eurasianet.org/node/64461.

KENYA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Free**
Obstacles to Access (0-25)	12	10
Limits on Content (0-35)	9	7
Violations of User Rights (0-40)	11	12
Total (0-100)	**32**	**29**

* 0=most free, 100=least free

POPULATION: 43 million
INTERNET PENETRATION 2011: 28 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Kenya continues to experience growth in the information and communication technology (ICT) sector as demonstrated by the increasing number of internet users, mobile phone subscribers, and broadcasting stations in 2011. The Global Internet Speed Report released in March 2012 ranked Kenya after Ghana as the second country in Africa with the highest internet speed.[1] Nevertheless, lack of infrastructure, high costs, and low purchasing power—which was exacerbated in 2011 when high inflation put pressure on disposable incomes—still hamper connectivity for many Kenyans.

The internet was introduced in Kenya in 1993, and the first commercial internet service provider (ISP) began operating in 1995.[2] Mobile phones were introduced in 1992 but only became widely available and affordable after the country's telecommunications industry regulator, the Communications Commission of Kenya (CCK), was established and two service providers, Safaricom and Kencell, were licensed in 1999.[3]

Since 2008, there have been no confirmed incidents of government filtering or interference with online communication. However, in March 2012, the CCK announced its intention to set up a surveillance system aimed to monitor private emails, citing a rise in cyber security

[1] "Top 10 African Countries With Fastest Broadband Speed [REPORT]," TechLoy, March 12, 2012, http://techloy.com/2012/03/12/africa-top-broadband speed/.
[2] Francisca Mweu, "Overview of the Internet in Kenya," International Telecommunication Union (prepared for African Internet & Telecom Summit, Banjul, The Gambia, June 5-9, 2000), http://www.itu.int/africainternet2000/countryreports/ken_e.htm.
[3] Export Processing Zones Authority, *Kenya's Information &Communications Technology Sector 2005* (Nairobi: Export Processing Zones Authority, 2005), http://www.epzakenya.com/UserFiles/File/ictKenya.pdf.

threats as justification.[4] The installation of the internet traffic monitoring equipment known as the Network Early Warning System (NEWS) will be set up by International Telecommunication Union (ITU) experts and is expected to be operational in mid-2012.

OBSTACLES TO ACCESS

Kenya is one of Africa's fastest growing internet markets with internet penetration increasing from 7.5 percent in 2006 to 28 percent in 2011.[5] Much of this growth can be attributed to increases in mobile internet connections, improved internet bandwidth capacity,[6] and intensified promotions on social media applications by mobile operators.[7]

The mobile phone subscription rate in Kenya also increased from 60 percent in mid-2010 to 71.3 percent in December 2011, with 28.1 million mobile phone subscriptions, according to the CCK.[8] This is due to the growing popularity of mobile handsets as a medium of communication in addition to increasing popularity of value-added services such as data and internet, entertainment, and mobile money transfer. Mobile subscriptions on GPRS/EDGE and 3G networks continued to show an upward trend in 2011,[9] closing the year with 6.1 million subscriptions.[10] Further, CCK reports indicate that mobile data/internet subscriptions represent 99 percent of total internet subscriptions, an indication that the mobile handset has become a popular mode of accessing internet.[11]

While internet penetration continues to increase across the country, there is a large disparity in access between rural and urban areas. In most urban areas, the rate of access is above 15 percent, whereas penetration is less than 3 percent in some rural areas.[12] The spread of internet to underserved areas is hampered by high operation and maintenance costs, especially due to the lack of electricity, high license and spectrum fees, limited access to roads, and poor security against vandalism for the infrastructure deployed.[13]

---

[4] Mark Okuttah, "CCK sparks row with fresh bit to spy on internet users," Business Daily, March 20, 2012, http://www.businessdailyafrica.com/Corporate+News/CCK+sparks+row+with+fresh+bid+to+spy+on+Internet+users+/-/539550/1370218/-/item/1/-/4gnwl5/-/index.html.

[5] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[6] International Telecommunication Union (ITU), "Measuring the Information Society," 2011.

[7] CCK, "Quarterly Sector Statistics Report, 2nd Quarter, October-December 2011/2012," 22.

[8] Ibid., 8.

[9] CCK, "Quarterly Sector Statistics Report, 1st Quarter, July-Sept 2011/2012," http://www.cck.go.ke/resc/downloads/SECTOR_STATISTICS_REPORT_Q1_11-12.pdf.

[10] CCK, "Quarterly Sector Statistics Report, 2nd Quarter, October-December 2011/2012," 21.

[11] CCK, "Quarterly Sector Statistics Report, 1st Quarter, July-Sept 2011/2012," 19.

[12] CCK, "Analysis of 2010 ICT Survey released in September 2011," http://www.cck.go.ke/resc/downloads/ANALYSIS_OF_THE_NATIONAL_ICT_SURVEY_2010.pdf.

[13] CCK, "Study on ICT Access Gaps in Kenya 2011," http://www.cck.go.ke/news/downloads/Access_Gaps_Final_Report.pdf.

The impediments to ICT infrastructural development partly explain the disproportionately high concentration of internet subscribers in Kenya's two largest cities, Nairobi and Mombasa. Both the government and private sector are working to remedy the disparity between rural and urban access through the introduction of "digital villages" and Pasha (Swahili for "inform") Centers, which are small public access sites similar to cybercafes.[14] In April 2010, Kenya's ICT Board began granting loans to entrepreneurs to set up Pasha Centers equipped with five computers and an internet connection in each of Kenya's 210 constituencies.[15] By September 2011, 37 Pasha Centers had been approved.[16] From the private sector, the telecommunications company Safaricom aims to set up 500 digital villages across the country, and 147 centers have been established as of early 2012.[17] However, owners of both digital villages and Pasha Centers complain of high tariffs, and the ICT Board's promise to provide Pasha owners with a year of free internet connectivity is yet to materialize.[18]

Competition is present in most segments of the telecommunications sector as a result of the country's open market-based licensing process instituted in 2008, though Safaricom still dominates mobile phone services with nearly 68 percent of the market as of September 2011.[19] Increased competition among providers have decreased tariffs on mobile-cellular services, and in early 2011, the telecom Airtel sparked a price war by reducing voice call, text messaging, and termination fee rates, prompting Safaricom and Orange to follow suit.[20]

Under the Communications Amendment Act passed in January 2009, responsibility for the regulation of both broadcast and online media was passed from the Media Council to the CCK. While the 1998 Kenya Communications Act formally enshrines the CCK's independence, most of the body's commissioners are government appointees, and the appointment process is not sufficiently open or transparent.[21] Further, a 2009 CCK customer satisfaction survey found some concern among respondents who believe that the CCK does not work independently, is controlled by "outside forces," and is biased towards

[14] "Kenya Investing Ksh 16.3 Billion in Rural ICT," *Information Policy* (blog), July 30, 2009, http://www.i-policy.org/2009/07/kenya-investing-ksh163-billion-in-rural-ict.html.
[15] Kenya ICT Board, "About PASHA," March 11, 2010, http://www.ict.go.ke/index.php?option=com_content&view=article&id=160&Itemid=182.
[16] Warigia Bowman, "Digital Villages," 2011, accessed January 10, 2012, http://www.kictanet.or.ke/?p=2716.
[17] Ibid.
[18] Ibid.
[19] CCK, "Quarterly Sector Statistics Report, 1st Quarter, July-Sept 2011/2012."; Macharia Kamau, "Safaricom raises concerns over competition rules," Standard Media, http://www.standardmedia.co.ke/InsidePage.php?id=2000008960&cid=14.
[20] Duncan McLeod, "Inside Kenya's brutal mobile price war," Tech Central, January 19, 2011, http://www.techcentral.co.za/inside-kenyas-brutal-mobile-price-war/20445/.
[21] Open Society Foundations, "Public Broadcasting in Africa Series: Kenya," 2011, 65, http://www.afrimap.org/english/images/report/MAIN%20report%20final%20web%20res.pdf.

some players in the market.[22] There is no evidence that the opinions from the survey were significantly different in 2011 and early 2012.

The CCK has yet to make any decisions affecting the internet, thus its autonomy and professionalism in making determinations on the topic remain to be seen. Two draft bills—the Media Council Bill 2011 and Independent Communications Commission of Kenya Bill 2010—aimed at aligning the CCK and Media Council under Kenya's 2010 Constitution are undergoing internal review and stakeholder consultation as of early 2012.[23]

Access providers have formed organizations such as the Kenyan ISP Association, the Telecommunications Service Providers of Kenya, and the Kenya Cybercafe Owners to lobby the government for better regulations, lower costs, and increased efforts to improve computer literacy.

LIMITS ON CONTENT

The government does not employ technical filtering or any administrative censorship system to restrict access to political or other content. Citizens are able to access a wide range of viewpoints, with the websites of the British Broadcasting Corporation (BBC), the U.S.-based Cable News Network (CNN), and Kenya's *Daily Nation* newspaper being the most commonly accessed online news outlets.[24] Despite concerns over the use of the internet to propagate hate speech during the post-election violence in late 2007 and early 2008, and fears that the authorities might use this to justify imposing greater controls on online content, no such restrictions have been introduced. Nonetheless, in January 2012, the National Integration Cohesion Commission (NCIC) announced that one of the new areas of focus for the commission's work will be to monitor hate speech on the internet ahead of Kenya's next general elections, which have been postponed from August 2012 to March 2013.[25]

Individual internet users generally seem comfortable with expressing themselves freely online. Some mainstream media organizations, commentators, and bloggers practice limited self-censorship,[26] but this is mainly due to business implications. For example, in July 2010

[22] "Customer Satisfaction and Perception Survey – 2009," Ace Research & Field Management Services, accessed January 10, 2012, http://www.cck.go.ke/consumers/downloads/Customer_Satisfaction_Report2009.pdf.
[23] "Bill Tracker," Commission for the Implementation of the Constitution, http://www.cickenya.org/bill_tracker?page=1.
[24] Victor Juma, "Mobile Internet on Course to Becoming Top Earner for Firms," Business Daily, April 22, 2010, http://allafrica.com/stories/201004210995.html.
[25] Moreen Majiwa, "NCIC Monitoring Social Media for Hate Speech," Mzalendo, March 26, 2011, http://www.mzalendo.com/tag/mzalendo-kibunja/.
[26] Interview with Rebecca Wanjiku, online journalist, January 3, 2010.

one blogger had to take down a post critical of a mobile provider because the company he worked for was a contractor at the mobile firm. The mobile firm called the blogger's supervisor, who subsequently gave the blogger an ultimatum to either take down the post or be fired.[27]

Print outlets, television, and radio continue to be the main sources of news and information for most Kenyans, though there are increasing efforts to extend mainstream news to online platforms. Kenyans have unrestricted access to the social-networking site Facebook, the video-sharing site YouTube, and the blog-hosting site Blogger, all of which rank among the ten most popular sites in the country.[28] All major television stations now use YouTube to rebroadcast news clips and have accounts on Facebook and Twitter.

Kenya is known to be the birthplace of Ushahidi.com (Swahili for "testimony"), the crowdsourcing website that was created in the aftermath of the country's disputed 2007 presidential election to document and map eyewitness reports of violence around the country, which were collected via text messages. The Ushahidi open source software and platform has since become a popular tool for social activism and citizen journalism around the world.

The internet continues to be an important platform for political debate and mobilization around critical issues such as the rising cost of living and insecurity affecting ordinary citizens.[29] For example, the Unga (Flour) Revolution protests against rising food and fuel prices throughout 2011 were organized largely through Twitter, Facebook and other websites. In July 2011, a demonstration against Kenya's Minister of Education over unaccounted funds from the Free Primary Education Fund was also organized through text messages, Twitter, and Facebook.[30] Nevertheless, the Unga Revolution protests did not translate into a reduction of food prices, and the Minister of Education did not resign, reflecting the limits of ICT activism in affecting change in Kenya.

Digital media has revolutionized the way that human rights groups in Kenya network and share information.[31] For example, groups such as Bunge La Mwananchi (People's Parliament) used to meet in person to organize events; today, they mobilize its members and discuss issues primarily through listservs and on Facebook. In February

[27] Interview conducted during the 2011 Bloggers Association of Kenya (BAKE) meeting.
[28] Alexa, "Top Sites in Kenya," accessed January 24, 2012, http://www.alexa.com/topsites/countries/KE.
[29] Kenfrey Kiberenge, "More Food Protests Expected in Nairobi," The Standard, April 23, 2011, http://www.standardmedia.co.ke/?id=2000033874&cid=4&articleID=2000033874.
[30] Grace Githaiga, "Technological advancement: new frontiers for Kenya's media?" in Pudderphatt et al., *A New Frontier, An Old Landscape* (United Kingdom: Global Partners and Associates, November 2011), 194, http://participatorymedia.lab.asu.edu/files/NewFrontierOldLandscape.pdf.
[31] Larry Diamond, *In the Spirit of Democracy* (New York: Henry Holt and Company LLC, 2008).

2012, Mzalendo.com re-launched its portal designed to allow citizens to communicate with their representatives in parliament and rate their services. The website is expected to play a key role in online debates, and Mzalendo comments are currently moderated to guard against abuse.[32]

VIOLATIONS OF USER RIGHTS

Freedom of expression is enshrined in Article 33 of Kenya's Constitution and includes the right to seek, receive, or impart information and ideas. The right, however, does not extend to propaganda, hate speech, incitement to violence, and advocacy of hatred. Criminal defamation laws with penalties of at least Ksh 400,000 (approximately US$4,680) remain on the books,[33] waiting to be repealed or amended to conform to Kenya's 2010 Constitution. Existing laws that are in conflict with any article of the 2010 Constitution will be declared unconstitutional.[34]

While defamation cases are occasionally brought against journalists in traditional media, jurisprudence is now catching up online with a few legal actions being taken against internet users in recent years. An example is that of blogger Dennis Itumbi, who in April 2012 accused blogger Robert Alai of defamation through what he considered malicious tweets. Itumbi is seeking compensation, an apology, and a retraction of "similar prominence and or any other remedies, the court may deem fit,"[35] grounding his case on the premise that bloggers "have to be responsible for what we say on social media."[36]

In January 2009, the government passed a controversial Communications Amendment Act despite warnings from civil society groups that it could hinder free expression. The Act established that any person who publishes or transmits obscene information in electronic form commits an offense. It also outlines other forms of illegality associated with the use of ICTs.[37] The prescribed punishments include up to KSh 200,000 (approximately US$2,340) in fines and two years' imprisonment.

[32] Rebecca Wanjiku, "Kenyan Government Takes Cautious Approach Toward Social Media," PC World, March 2, 2012, http://www.pcworld.com/article/251194/kenyan_government_takes_cautious_approach_toward_social_media.html.
[33] Chapter 36: The Defamation Act, Laws of Kenya, Revised edition 2009 (1972), http://www.kenyalaw.org/Downloads/Acts/Defamation%20Act%20(Cap.36).pdf.
[34] Article 4 of Kenya's 2010 Constitution.
[35] "Journalist Itumbi sues blogger Alai," The Star, April 13, 2012, http://www.the-star.co.ke/national/national/71340-journalist-itumbi-sues-blogger-alai.
[36] Dennis Itumbi, "Why I am moving to court against a blogger," DennisItumbi.com (blog), March 18, 2012, http://www.dennisitumbi.com/?p=297.
[37] Republic of Kenya Office of Public Communications, "The Kenya Communications (Amendment) Act 2009," accessed February 15, 2011, http://www.communication.go.ke/Documents/media.pdf.

As of early 2012, however, many laws such as the 2009 Communications Amendment Act are undergoing internal review and stakeholder consultation. The aim is to repeal or amend them in order to bring them in conformity with Kenya's new Constitution passed in 2010.[38] The Freedom of Information Bill and the ICT Sector Policy Guidelines 2011[39] are some of those undergoing internal review. The process is being spearheaded by the Commission for the Implementation of the Constitution.[40]

Surveillance of the internet and mobile phones has become a growing concern in Kenya over the past year. In March 2012, the CCK announced its intention to set up a surveillance system aimed to monitor private emails, citing a rise in cyber security threats.[41] The regulator has notified telecom service providers on the need to cooperate with the installation of the internet traffic monitoring equipment known as the Network Early Warning System, which will be set up by International Telecommunication Union (ITU) experts and is expected to be operational in mid-2012. This is being viewed as a breach of Article 31 of Kenya's Constitution, which grants citizens the right to privacy, including preventing infringement of "the privacy of their communication."

One potential case of online surveillance was reported in March 2012, when blogger Dennis Itumbi was arrested on suspicions that he had hacked the International Criminal Court (ICC) website. While no evidence was produced to prove Itumbi guilty, it was suspected that his communications had been monitored.[42] However, he was never arraigned in court and was released after questioning, pending further investigations.

In June 2010, the CCK announced a requirement for all mobile phone subscribers to register their SIM cards with their service providers. By September 2011, approximately 60 percent of users had registered, and in April 2012, the authorities extended the deadline to August 2012 to allow everyone to register.

There were no reports of extralegal intimidation of journalists, bloggers, or other ICT users by state authorities or any other actor in 2011. Furthermore, ICT users in Kenya have not been subject to widespread technical violence; however, in early 2012, 103 Kenyan

[38] "Bill Tracker," Commission for the Implementation of the Constitution," http://www.cickenya.org/bill_tracker.
[39] Ministry of Information and Communications website: http://www.information.go.ke/index.php?option=com_content&task=view&id=392&Itemid=535.
[40] "Bill Tracker," Commission for the Implementation of the Constitution."
[41] Mark Okuttah, "CCK sparks row with fresh bit to spy on internet users," Business Daily, March 20, 2012, http://www.businessdailyafrica.com/Corporate+News/CCK+sparks+row+with+fresh+bid+to+spy+on+Internet+users+/-/539550/1370218/-/item/1/-/4gnwl5/-/index.html.
[42] Cyrus Ombati, "Kenya Police go to Hague over hacking," The Standard, March 26, 2012, http://www.standardmedia.co.ke/?id=2000054909&cid=&articleID=2000054909.

government websites were defaced by an Indonesian hacker,[43] and cyber security threats have become a growing concern to the CCK in recent years.[44]

[43] Lilian Nduati, "Massive cyber attack hits 100 State websites," Daily Nation, January 17, 2012, http://allafrica.com/stories/201201180434.html.
[44] Mark Okuttah, "CCK sparks row with fresh bit to spy on internet users," Business Daily, March 20, 2012.

KYRGYZSTAN

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access (0-25)	n/a	13
Limits on Content (0-35)	n/a	10
Violations of User Rights (0-40)	n/a	12
Total (0-100)	**n/a**	**35**

* 0=most free, 100=least free

POPULATION: 5.7 million
INTERNET PENETRATION 2011: 20 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

The current state of internet freedom in Kyrgyzstan must be understood in the context of the aftermath of events in 2010, which included the violent overthrow of President Kurmanbek Bakiev's regime, as well as ethnic clashes between the Kyrgyz and Uzbek population that led to over 400 deaths. Shortly before Bakiev's ousting, political pressure on the media, both traditional and online, intensified. The video portal Stan.tv was closed as punishment for covering opposition meetings,[1] the country's largest online portal that was serving as the main platform for political discussions was shut down,[2] and all internet service providers (ISPs) were forced to cut off their connections to the international internet in order to prevent information from leaking out.[3]

However, after Bakiev's removal in April 2010, these restrictions were lifted and the flow of information returned to normal. In 2011, the environment was relatively favorable to internet freedom, as the interim government was stable and presidential elections in October 2011 were deemed competitive, though flawed. Despite such improvements, internet access remains limited primarily to urban areas and state bodies initiated several attempts in 2011 to block websites. As of April 2012, however, only one blocking order against the Central Asian news website Ferghana News (Ferghana.ru) had been implemented by the state-run ISP, KyrgyzTelecom. Meanwhile, ethnic relations remained tense and several

1 "Newspaper suspended, TV station raided in Kyrgyzstan," Committee to Protect Journalists, April 2, 2010, http://cpj.org/2010/04/newspaper-suspended-tv-station-raided-kyrgyzstan.php.
2 "Страна, устремленная в будущее… Кыргызстан-2010. Хроника событий" [The country directed to the future… Kyrgyzstan-2010. Chronicle of events], August 30, 2010, http://pda.kabar.kg/kabar/full/18890.
3 "Блокировка продолжается"[Blocking goes on], Namba.kg (blog), April 6, 2010 http://blogs.namba.kg/post.php?id=470.

individuals involved in websites advocating for Uzbek rights were physically attacked during the year.

OBSTACLES TO ACCESS

Access to information and communications technologies (ICTs) has grown in Kyrgyzstan in recent years, with internet penetration being among the highest in Central Asia, though still low by global standards. According to the International Telecommunications Union (ITU), internet penetration rate in 2011 stood at 20 percent, an increase from 12.3 percent in 2006.[4] The State Telecommunication Agency under the Government of Kyrgyzstan (STA) reported a notably higher figure as of October 2011, of 1.9 million people, or about 35 percent of the population.[5] However, a USAID-funded survey by M-Vector Research Agency in 2011 found that only 16 percent of respondents reported ever using the internet.[6] Among them, 51 percent were located in the capital Bishkek and 32 percent in Osh, the country's second largest city. By contrast, only 5 percent of rural respondents reported ever going online, reflecting the urban-rural divide in penetration. Cybercafes are a particularly popular means of obtaining access, with over one-third of internet users reporting that they had accessed the internet at such a venue.[7]

Fixed-broadband access, via either fiber-optic cables or DSL, is accessible mainly in the capital Bishkek, with broadband in the provinces provided only by the state-run KyrgyzTelecom. Broadband speeds range from 24 Mbps for DSL to 100 Mbps for the FTTx (fiber to the x) network, which is well-developed in Bishkek. The government has launched a CDMA450 mobile telephone and broadband network to expand telecom infrastructure into more rural areas, though it has only become partially active. CDMA450 phones have become popular in rural areas with more than 30,000 subscribers as of November 2011; however, only 600 subscribers actually access the internet through their phones, reflecting a low digital literacy rate among rural users.[8]

4 International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

5 Report of the State Communication Agency under the government of Kyrgyz Republic for 10 months of 2011, by request of the public fund, Civil Initiative on Internet Policy (CIIP).

6 "Media Consumption & Consumer Perceptions Baseline Survey," M-vector Consulting Agency, April 2011, http://m-vector.com/upload/news/media_survey_eng/Part1Researchoverviewweng.pdf.

7 Ibid.

8 Information obtained from the former top management of Kyrgyztelecom.

Mobile phone penetration is significantly higher in Kyrgyzstan with a penetration rate of nearly 105 percent in 2011.[9] Mobile phone companies claim that their networks cover 90 percent of the populated territory in the country, thus opening the possibility of internet use for most people as mobile web access expands. At the end of 2010, Beeline (one of the largest mobile phone carriers) launched a 3G network that currently covers the whole country. Another large firm, Megacom, launched its own 3G network in January 2012 in Bishkek and reported plans to cover the entire country within six months. Meanwhile, Saimatelecom launched a 4G network covering Bishkek and some suburbs. With the rollout of these mobile broadband networks, the number of mobile web users had reached an estimated 20,000 as of early 2012.

Despite the spread of ICT infrastructure across the country in recent years, the price of internet access remains beyond the reach of much of the population. As an indication of the limited access among lower income brackets, the M-Vector study noted above found that only 8 percent of internet users with an average monthly income of less than 7,500KGS (about US$160) use the internet, while about 40 percent of those with an income under 30,000 KGS (about US$640) do.[10] Moreover, given high poverty rates in rural areas, accessing the internet is not a high priority for many people.[11] Individuals living in rural areas largely rely on mobile phone internet access because the fixed-line infrastructure is very underdeveloped. Such service costs on average between US$40 and US$750 per gigabyte for mobile internet access; by comparison, the average monthly income per capita is US$190.[12] A lack of equipment and low computer literacy also render internet use difficult for many people in rural areas. Prices for unlimited data plans, which are primarily available in the capital, are more affordable, ranging from US$5 to US$100 per month for fixed-line broadband, depending on speed and download volume.[13]

Differing tariffs for accessing domestic versus international content are in place by fixed-line internet providers but not via mobile phone. All fixed-line operators charge about ten times less in fees or even none for internal traffic compared to international traffic. Mobile phone operators do not make this distinction in their data plans and charge the same for accessing information, wherever it may be hosted.

9 International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

10 "Media Consumption & Consumer Perceptions Baseline Survey," M-vector Consulting Agency.

11 In rural areas, about 60 percent of the population lives below the poverty line, while in cities, this number is about 30 percent. Source: "USAID Local Development Program," USAID Kyrgyz Republic, accessed September 17, 2012, http://ldp.kg/en/tasks/chas-sector/sectors/agriculture/meat/.

12 World Bank, "Gross national income per capita 2011, Atlas method and PPP," World Bank Databank, 2011, accessed July 18, 2012, http://databank.worldbank.org/databank/download/GNIPC.pdf.

13 The information is obtained by comparisons of tariff plans from the sites of ISPs.

Many social media outlets such as YouTube, Facebook, and Twitter are freely available. However, some international blog-hosting services are subjected to filtering from upstream providers based in Kazakhstan. Three of Kyrgyzstan's four first-tier ISPs are linked to the international internet via Kazakhstan and its state-run provider Kazakhtelecom; the fourth connects through Russia.[14] As a result, when the Kazakhstan government blocks websites, they also become inaccessible in Kyrgyzstan. Among the resources blocked in Kazakhstan are the blog-hosting service Livejournal, the news website Newsland.ru, and some Google services. Nevertheless, ISPs in Kyrgyzstan are not required to use government-owned channels to connect to the international internet and can establish their own. In 2010, the state-owned ISP KyrgyzTelecom completed the construction of a fiber-optic cable connection to China, but it has yet to begin functioning.[15]

Kyrgyzstan's telecommunications sector is relatively liberalized and competitive compared to other countries in the region. There are four first-tier ISPs. The state-owned KyrgyzTelecom is the largest ISP with a market share of about 60 percent, and it oversees infrastructure deployed throughout Kyrgyzstan. The other three first-tier ISPs (Elcat, Megaline, and Saimatelecom) are privately-owned. The largest among them is Megaline, which provides broadband service in Bishkek. In addition to the first-tier providers, there are 61 licensed second-tier ISPs, though only 15 are active.

There are six mobile phone operators providing voice and data services via a variety of technical standards. The two largest competitors with nearly equal market share are Megacom and Beeline. Megacom was nationalized in 2010 amidst the political upheaval. In January 2012, a court ruled that 51 percent of Megacom's shares should be returned to the owners who possessed the company before individuals affiliated with the ex-president came to unlawfully own it.[16]

The main body regulating the ICT industry, including radio spectrum allocation, is the State Telecommunication Agency under the Government of Kyrgyzstan (STA), which is a government body that contains a director and 137 members. The director and his two deputies are appointed by the prime minister.[17] Some facets of its work have been criticized, such as inefficient and non-transparent allocation of radio frequencies and restrictions on wireless mesh internet networks. Another problematic issue has been the requirement that communication devices (including computers, modems, and wireless access points) must be

14 "Coverage area of internet service providers in Bishkek," Tilekus.com (blog), accessed September 17, 2012, https://sites.google.com/site/tilekus/projects/internet-in-central-asia/internet-providers-in-kyrgyzstan.

15 "Годовой отчет 2010, Кыргызтелеком" [Annual report 2010, Kyrgyztelecom], Kyrgyztelecom, accessed September 17, 2012, http://www.kt.kg/about_us/documents_and_tender/#ui-tabs-3.

16 Information obtained from a conversation with top management of Megacom. The decision has yet to be published officially.

17 "Regulation on the State Telecommunication Agency under the government of Kyrgyz Republic," passed by a Resolution of the government of KR № 124, as of 20.02.2012.

locally certified by the STA.[18] While this requirement is not systematically enforced, its selective application could serve as an instrument of political pressure and pretext for authorities to seize "uncertified" property, though this has not yet occurred.

LIMITS ON CONTENT

The Kyrgyzstan government does not significantly censor the internet, but some political and news websites have been sporadically blocked in the past. In 2011, there were several incidents of orders to block such content being issued, with only one block on Ferghana.ru implemented as of April 2012 (see below). This may be because television remains by far the dominant medium through which citizens obtain information about their country and thus censorship efforts have focused on broadcast media.[19] For example, in the run-up to the 2011 presidential elections, the government passed a statute placing stringent regulations on foreign television broadcasts related to the elections and imposing high fines for violations.[20] Given the difficulty of parsing content, television carriers chose to cut off access to most foreign television channels—whether they were Russian, American, or European—in order to avoid the fines. By comparison, the websites of broadcasters such as CNN, the BBC, or Russia Today remained available throughout the campaign. Online resources have not been affected by this statute as they are not considered to be mass media.

Nevertheless, there have been several incidents of government entities ordering blocks of online content, including at least one news website. In May 2011, a court in the Pervomaiski region issued a decision prohibiting the distribution of two books—*The Philosophy of Cruelty: Hour of the Jackal* and *The Philosophy of Cruelty: The Genocide Continues…* —and an accompanying video CD-ROM that documented the ethnic violence that occurred in June 2010. The books and videos, which flooded online video-sharing sites, sparked outrage in Kyrgyzstan because of their portrayal of the event as genocide against ethnic Uzbeks. The judge ruled the content illegal for inciting national hatred and banned its dissemination in Kyrgyz territory.[21] Later in June 2011, the Prosecutor General's Office ordered the blocking of the portals Yandex.ru, Mail.ru, and YouTube after having discovered that the sites

18 "Regulation on rules and procedure of mandatory certification of production."

19 According to the 2011 M-vector survey, TV still remains the primary source of information for 83.4 percent of the urban population and 93.5 percent of the rural population. Source: "Media Consumption & Consumer Perceptions Baseline Survey," M-vector Consulting Agency, April 2011.

20 According to the statute, all overseas channels during an election campaign can only be broadcasted from recorded sources and must not contain any information about candidates that can be considered as propaganda or that can discredit them. See Article 22 of the Constitutional Law № 68, "On elections of the President of Kyrgyz Republic and deputies of Jogorku Kenesh of Kyrgyz Republic," as of 02.07.2011.

21 "Суд вынес запрет на распространение книг «Час шакала» и «Час шакала-2» на территории Кыргызстана" [The court made the judgment to prohibit the distribution of books "Jackal Hour" and "Jackal Hour-2" on the territory of Kyrgyzstan], Kyrgyz Telegraph Agency (KirTAG), May 3, 2011, http://www.kyrtag.kg/?q=ru/news/5870.

contained the banned materials. The non-profit Civil Initiative on Internet Policy (CIIP) sent a letter to the management of these companies requesting that the material be removed from their sites to prevent a blanket block from being imposed. The management of Yandex.ru agreed to the request and removed the content, though the materials remain available on YouTube and Mail.ru as of mid-2012, and the blocking order was never carried out.[22]

In another case in June 2011, the parliament passed a resolution instructing the government to block the independent Central Asian news website Ferghana News (Ferghana.ru) also based on charges that its content could incite national strife.[23] In February 2012, the STA sent letters to all ISPs delineating the requirement to block the news website.[24] As of April 2012, only KyrgyzTelecom has implemented the blocking.[25]

Also in June 2011, a member of parliament suggested blocking Diesel Forum (Diesel.elcat.kg), the country's most popular online forum, claiming that it too was "inciting national strife."[26] The forum has been online for over ten years and is the most popular platform for discussion of a wide variety of issues, including political debates and criticism of the government. During the events of 2010, Diesel Forum was a key source of information for many citizens. Given the lack of evident rationale for the blocking suggestion, which sparked widespread opposition from the online community, the block was never implemented.

The government has also sought to restrict access to terrorism-related content. In November 2011, a top official in 10th department of the Ministry of Internal Affairs claimed that their unit for countering cyber-threats had identified 12 websites with terrorist and extremist content that were then blocked according to a court order.[27] Among the list of blocked websites was one belonging to the militant group Islamic Movement of Uzbekistan (furqon.com); however, according to Freedom House tests conducted in December 2011, the website remained accessible from most ISPs.

22 Videos can be found at: http://www.youtube.com/watch?v=vcgbMC7_LWU, and http://video.mail.ru/mail/uzbekbek1/268/269.html, accessed September 17, 2012.
23 "Resolution of Jogorku Kenesh," Kenesh.kg, June 17, 2011, http://kenesh.kg/RU/Pages/ViewNews.aspx?id=8&NewsID=2678.
24 "Пресс релиз Государственного агентства связи при Правительстве Кыргызской Республики" [Press-release of the State Telecommunication Agency under the government of Kyrgyz Republic], as of 22.02.2012.
25 "Independent News Website Partly Blocked in Kyrgyzstan," Radio Free Europe/Radio Liberty, February 22, 2012, http://www.rferl.org/content/independent_news_website_partly_blocked_in_kyrgyzstan/24492408.html.
26 "Депутат «Ар-Намыса» требует привлечь к уголовной ответственности форум «Дизель»" [The deputy of "Ar-namys" political party demands that the forum "Diesel" to be criminal proceedings taken against], Kloop.kg (blog), June 20, 2011, http://kloop.kg/blog/2011/06/20/deputat-ar-namysa-trebuet-privlech-v-ugolovnoj-otvetstvennosti-k-dizel-forum/.
27 "12 сайтов заблокировано на территории Кыргызстана за распространение слухов экстремистского характера" [12 sites have been blocked in Kyrgyzstan as spreading rumors of extremist kind], Kyrgyz Telegraph Agency (KirTAG), November 28, 2011, http://www.kyrtag.kg/?q=news/13260.

According to the legal requirements in place under the 2005 statute, "On Counteraction to Extremist Activities,"[28] the procedure by which a website can be blocked must first begin with a request to the prosecutor.[29] Then a review committee must be assembled consisting of representatives from different organizations (linguistic, religious, legal, etc.) that could confirm the extremist orientation of a site, though the committee members are appointed by the government, calling into question the committee's independence and level of objectivity. Once confirmation is granted, a court will issue a judicial decision to block the website. When implementing a blocking order, ISPs in Kyrgyzstan generally do so by blocking access to the website's internet protocol (IP) address. Should the IP address change, the website would become accessible again. Since there is no consistent monitoring of the status of blocks by the authorities, their effectiveness is limited. In a different dynamic, the Central Election Committee in July 2011 rejected several accreditation requests by internet-based news agencies to cover the presidential election campaign. The committee claimed that under Kyrgyz law, the online news sites were not considered "mass media" and that only mass media are permitted to cover election campaigns.[30] After criticism by local experts and international organizations such as the European Union,[31] Human Rights Watch,[32] and the Committee to Protect Journalists,[33] parliament reversed the decision the following month and allowed online information agencies to take part in election coverage.[34]

Self-censorship online exists to a degree, primarily as a result of government restrictions against the incitement of national hatred. All posts on forums are strictly moderated to limit this type of content, and online journalist or bloggers generally try to avoid issues concerning ethnic relations.

28 Dmitry Golovanov, "Kyrgyzstan: Extremism Outlawed," IRIS Merlin, August 2005, http://merlin.obs.coe.int/iris/2005/8/article26.en.html; "The statute on counteraction against extremist activities" as of, 20.02.2009.

29 Representatives of the 10th department explained the procedure to the author in a private interview in December 2011.

30 Kalicha Djamankulova, "Информационные агентства не допустили к предвыборной агитации" [Information agencies are not allowed to cover the presidential elections], Knews.kg, July 21, 2011, http://www.knews.kg/ru/vybory/1104.

31 Jeanne Khusainova, "Европейский союз: Информационные агентства в Кыргызстане должны использовать все законные возможности для отстаивания своих прав" [European Union: information agencies in Kyrgyztan should use all legal resources to assert their rights], 24kg.org, July 28, 2011, http://www.24kg.org/election2011/105863-evropejskij-soyuz-informacionnye-agentstva-v.html.

32 Jeanne Khusainova, "Human Rights Watch: ЦИК Кыргызстана должен аккредитовать информационные агентства для участия в предвыборной агитации" [Human Rights Watch: CEC of Kyrgyzstan has to accredit information agencies to cover the presidential elections], 24kg.org, August 5, 2011, http://www.24kg.org/election2011/106343-human-rights-watch-cik-kyrgyzstana-dolzhen.html.

33 Jeanne Khusainova, "Комитет по защите журналистов призывает ЦИК Кыргызстана позволить информационным агентствам участвовать в освещении выборов" [Committee to Protect Journalists appeals CEC of Kyrgyzstan for allowing information agencies to cover presidential elections], 24kg.org, July 28, 2011, http://www.24kg.org/election2011/105864-komitet-po-zashhite-zhurnalistov-prizyvaet-cik.html.

34 Askar Aktalov, "Жогорку Кенеш: «Информагентства имеют право принимать участие в предвыборной агитации»" [Jogorku Kenesh: information agencies have a right to cover the presidential elections], Knews.kg, August 16, 2011, http://www.knews.kg/ru/parlament_chro/1862/.

The Kyrgyz blogosphere is not well-developed. There are several popular blog-hosting platforms in Kyrgyzstan (such as Namba.kg, Kloop.kg, Diesel.elcat.kg, and Taboo.kg), but most blogs focus on entertainment, reprint reports from other news agencies, or simply contain a blogger's private thoughts on different issues. There are no particularly popular blogs specifically devoted to political or social issues. Most blogs are in Russian, though some are in the local Kyrgyz language, but the latter are not as popular as the former. The internet in general has become an important source of alternative information for users, but since it is primarily the wealthier segments of the population who can afford to consistently access the internet, the wealthy are the main active participants in online communities. Social media applications such as Facebook have not yet gained widespread popularity. As of March 2012, there were about 75,000 Facebook users in Kyrgyzstan, representing only about 3 percent of online users.[35]

Several online initiatives were launched in the run-up to the 2011 elections, including the website Politmer.kg created to allow Kyrgyz citizens to monitor the campaign promises made by the presidential candidates, and the crowd-sourcing website Map.inkg.info created to document and map out election violations. During pre-election debates, some forum topics were created to collect questions for the candidates.

VIOLATIONS OF USER RIGHTS

Following the violent overthrow of President Bakiyev in 2010, a new constitution was approved by referendum in June 2010, which strengthens the power of parliament vis-à-vis the president. Article 31 of the constitution guarantees the right to freedom of thought, expression, speech, and press. Article 29 provides constitutional protections over privacy, including private correspondences (by phone, mail, electronic or others), and forbids the collection or dissemination of confidential information without an individual's consent. Nevertheless, the judiciary is not independent and remains dominated by the executive branch. Corruption among judges, who are underpaid, is also widespread, hindering the fairness of decisions in freedom of expression cases as well as others.[36]

In July 2011, the government decriminalized libel to bring legislation in line with the new constitution. Nevertheless, "insult" remains a criminal offense. Officials have long used libel charges to stifle critical media but have not applied these against bloggers to date.[37] The

35 "Kyrgyzstan Facebook Statistics," Social Bakers, accessed March 2012, http://www.socialbakers.com/facebook-statistics/kyrgyzstan.
36 Aili Piano (ed.), "Kyrgyzstan," *Freedom in the World 2012*, http://www.freedomhouse.org/report/freedom-world/2012/kyrgyzstan.
37 "OSCE Hails Kyrgyzstan Decision to Discriminate Libel," The Telegraph, July 19, 2011, http://www.telegraph.co.uk/news/worldnews/asia/kyrgyzstan/8648135/OSCE-hails-Kyrgyzstan-decision-to-decriminalise-

criminal code contains several provisions (Articles 299 and 299-1) that prohibit "inciting national, racial, religious or inter-regional hostility." As noted above, the government has sought to apply these provisions in some cases to restrict nonviolent political speech. Nevertheless, there have been no cases of an individual being punished for views or information published online.

All traditional media outlets must register with the government. In June 2011, the Prosecutor General's Office[38] proposed amending the statute that regulates mass media[39] to include internet news websites as a form of mass media, requiring them to have a license and to operate with the same responsibilities as traditional media outlets. In January 2012, an expert from the Government Office seconded the recommendation.[40]

There are currently no restrictions on anonymous communication on the internet. Websites do not need to register, encryption software is freely available, and real-name registration to post content online is not required. Furthermore, registration for prepaid SIM cards is optional; however, post-paid SIM cards, which are rarely used, do require registration with a passport.

The director of the Ministry of Internal Affairs claimed in October 2011 that their department on countering cyber threats monitors online content with the aim of identifying provocative rumors and then determining who is behind them.[41] This statement appears to be unfounded, however, as the ministry is known to lack personnel with sufficient technical qualifications for such work.

Nevertheless, several scandals in 2010 and 2011 revealed the abuse of equipment for intercepting communications. While the scandals involved the interception of phone communications, the equipment can also be applied to the internet. One such scandal involved a phone conversation between two members of a provisional government regarding the fraudulent appropriation of US$1 million.[42] A subsequent study from June 2011 by the

libel.html.

38 "Генпрокуратура Кыргызстана предлагает «законодательно к СМИ отнести интернет-издания и сайты, зарегистрированные в зоне kg»" [Prosecutor General's Office suggests "to legalize internet agencies and sites, registered in .kg zone, by inclusion them in the list of mass-media"], 24.kg, June 6, 2011, http://www.24.kg/community/101891-genprokuratura-kyrgyzstana-predlagaet.html.

39 The law, "On mass-media," June 16, 2008, http://www.medialaw.kg/?q=node/9.

40 Nurzada Tynaeva, "Эксперт Аппарата правительства предлагает разработать новый закон «О СМИ», чтобы регулировать информагентства" [The expert of the Government Office suggests to work out the new statute on mass-media to regulate information agencies], Knews.kg, January 17, 2012, http://www.knews.kg/ru/parlament_chro/9145/.

41 "Программисты 10-го управления МВД КР вычисляют распространителей слухов по Интернету" [The programmers of the 10th department of the Ministry of Internal Affairs determine the spreaders of rumors in Internet], October 25, 2011.

42 Video of recorded phone conversation can be viewed at: http://www.youtube.com/watch?v=zGKUrgGkyzg.

non-profit CIIP analyzed the legislative framework surrounding interception and its enforcement. It concluded that there were many gaps in the law that enabled interception equipment to be used, and even abused, without sufficient oversight.[43] In April 2011, the parliament passed a decision to switch off all interception equipment deployed on the premises of mobile phone operators.[44] According to reports by members of parliament from September 2011, however, the equipment continues to function.[45] As of February 2012, the CIIP together with the Kyrgyz State Committee on National Security and several human right organizations were working to draft amendments to the statute on the Conduct of Investigations—the body responsible for regulating these issues—that would clarify the circumstances surrounding the use of interception and provide a more adequate legal framework.

Amidst ongoing ethnic tensions, in 2011, there were several reported instances of physical attacks or intimidation of members of minorities associated with news websites. In August, Sokhrukh Saipov, the editor and publisher of the news website UzPress, was brutally attacked, although it is unclear whether Saipov was attacked specifically for his online activities. Nevertheless, the website publishes content in three languages about the social and political challenges affecting ethnic Uzbeks in southern Kyrgyzstan.[46] In a separate incident in May 2011, followers of the nationalist Asaba party threatened non-ethnic Kyrgyz staff of the online news agency 24.kg.[47]

During 2011, there were no politically motivated cyberattacks reported in Kyrgyzstan, including in the run-up to the presidential elections. In 2005, however, the OpenNet Initiative recorded the extensive use of distributed denial-of-service (DDoS) attacks against opposition and news websites, demonstrating a precedent for such attacks.[48] In September 2011, there was one incident of the Kabar.kg government online news agency website being defaced by hackers, but this did not significantly obstruct its work. In March 2012, the social entertainment resource Namba.kg experienced a DDoS attack that was apparently part of an extortion attempt.[49] In the same month, the news agency Vesti.kg also reported a DDoS

43 "Анализ законодательства КР на соответствие применения СОРМ, – предварительное заключение" [Analysis of the Kyrgyz legislation, concerning lawful using of interception equipment -preliminary conclusion], Gipi.kg, accessed September 17, 2012, http://www.gipi.kg/archives/1743.

44 Resolution of Djogorku Kenesh № 332-V as of 15.04.2011, "On switching off mobile operators' lawful interception equipment."

45 "Дастан Бекешев: В Кыргызстане в компаниях сотовых операторов до сих пор действует система СОРМ" [Dastan Bekesev: Lawful interception equipment still keeps working in mobile operators in Kyrgyzstan], 24.kg, September 8, 2011, http://www.24.kg/parlament/108440-dastan-bekeshev-v-kyrgyzstane-v-kompaniyax.html.

46 "Independent Journalist Brutally Attacked in Kyrgystan," Committee to Protect Journalists, August 15, 2011, http://www.cpj.org/2011/08/independent-journalist-brutally-attacked-in-kyrgyz.php.

47 "World Report 2012: Kyrgyzstan," Human Rights Watch, accessed August 30, 2012 http://www.hrw.org/world-report-2012/world-report-2012-kyrgyzstan.

48 "Kyrgyzstan," OpenNet Initiative, December 18, 2010, http://opennet.net/research/profiles/kyrgyzstan.

49 As reported by the blog at: http://blogs.namba.kg/post.php?id=116481.

attack on its site,[50] presumably because they had been republishing articles from Ferghana.ru.

50 Anna Yalovkina, "Редактор "Ферганы": Трудно судить, связаны ли DDoS-атаки на "Фергану" и "Вести"" [Editor of *Fergana*: It's hard to judge whether DDoS attacks on Fergana and Vesti are related], Vg.kg, March 29, 2012, http://www.vb.kg/news/society/2012/03/29/183948_redaktor_fergany_trydno_sydit_sviazany_li_ddos_ataki_na_fergany_i_vesti.html.

LIBYA

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access (0-25)	n/a	18
Limits on Content (0-35)	n/a	9
Violations of User Rights (0-40)	n/a	16
Total (0-100)	**n/a**	**43**

* 0=most free, 100=least free

POPULATION: 6.5 million
INTERNET PENETRATION 2011: 17 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

The political unrest and armed conflict that occurred in Libya in 2011, which resulted in the death of Muammar al-Qadhafi after over 40 years in power, led to a dramatic regime change. The country shifted from being one of the world's harshest dictatorships to a post-conflict aspiring democracy. As of May 2012, the government of Libya was comprised of a National Transitional Council (NTC) formed during the conflict and an appointed interim government mandated to steer the country towards elections scheduled for July 2012, after which a new constitution will be drafted. These political changes were also reflected in the internet freedom landscape. As such, this report straddles three radically different periods: a highly restrictive environment under Qadhafi, a partial internet and telephone blackout for much of 2011, and a relatively open online information landscape since the rebel victory in October 2011.

Qadhafi's regime employed a wide range of tactics for suppressing freedom of expression online, including maintaining monopoly control over the internet infrastructure, blocking websites, engaging in widespread surveillance, and meting out harsh punishments to online critics. Such restrictions intensified as the revolt against Qadhafi's rule gained momentum in February 2011, culminating in an internet shutdown that affected most of the country and lasted until the liberation of Tripoli in August 2011.[1] Since Qadhafi's death in October 2011, a frenzy of self-expression online has erupted as Libyans seek to make up for lost

[1] Hayley Tsukuyama, "Welcome back to the Internet Libya," The Washington Post (blog), August 22, 2011, http://www.washingtonpost.com/blogs/faster-forward/post/welcome-back-to-the-internet-libya/2011/08/22/gIQArYrJWJ_blog.html.

time. Nevertheless, periodic electricity outages, residual self-censorship, and weak legal protections pose ongoing challenges to internet freedom.

Internet first became available at state institutions in Libya in the mid-1990s, during a time of international economic sanctions imposed following the Lockerbie bombing. This expanded to public access in 1998, though priority was given to multinational companies, people close to the government, and some individuals authorized to open cybercafes.[2] It was only after Qadhafi endorsed information and communication technologies (ICTs) in 2000 as a means of promoting economic opportunities for youth that use of the medium began to spread more widely.[3] Few restrictions were imposed on communications in the early years of access and evidence of censorship was anecdotal until around 2003. It was then that sanctions were lifted and the government became free to purchase surveillance and filtering equipment. Soon after, more systematic censorship emerged, particularly of opposition websites based overseas.

OBSTACLES TO ACCESS

When the internet became publicly available in Libya in 1998, prices were excessively high and access was limited to a small elite. After 2000, however, thousands of cybercafes sprouted up, even in desert towns, rendering the internet more widely available.[4] Over the following decade, Qadhafi's son, who was managing the state-run telecom operator, reduced prices, invested in a fiber-optic backbone network, and expanded ADSL, WiMAX, and wireless local loop technologies.[5] These measures brought the price for browsing down to 1LYD (US$0.75) per hour in cybercafes by 2004 and even lower in 2011 prior to the uprising.

Nevertheless, as of 2007, penetration remained at around 4 percent, according to the International Telecommunications Union (ITU). By 2011, this had grown to 17 percent or about 1.1 million users, though such statistics do not include the small number of people using unregistered satellite phones to get online.[6]

[2] "Report on Internet in Libya" [in Arabic], by a committee of experts for www.reallibya.org, 2004, http://www.mohamoon-daleel.com/montada/messagedetails.asp?p_messageid=3334 (site discontinued).
[3] Ibid.
[4] Gamal Eid, "Libya: The Internet in a conflict zone," The Arabic Network for Human Rights Information, 2004, http://www.anhri.net/en/reports/net2004/libya.shtml.
[5] "Libya – Telecoms, Mobile and Broadband," BuddeCom Focus Report, accessed August 30, 2012, http://www.budde.com.au/Research/Libya-Telecoms-Mobile-and-Broadband.html.
[6] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

Despite improved infrastructure and relatively low prices for accessing the internet at cybercafes, the cost for a home internet connection remains beyond the reach of a large proportion of Libyans, particularly those living outside major urban areas. As of early 2011, a dial-up internet subscription cost 10LYD per month (US$7), an ADSL one was 20LYD (US$15) for 7GB, and WiMax was 40LYD ($US30) for 10GB (after initial connection fees). By comparison, the average monthly income as of early 2011 was about US$1,400, reflecting relatively high salaries in oil and gas firms. Those employed in the public sector, who comprise a large contingent of the Libyan workforce, earn an average income of only 250LYD (US$195).[7] As a result, the number of broadband subscriptions was relatively low, at around 70,000 or just over 1 percent in 2011.[8] As elsewhere, a VSAT connection was extremely expensive, running to hundreds of thousands of dinars. Limited computer literacy, particularly among women, has also been an obstacle. By contrast, with literacy rates at almost 90 percent and a wide range of websites and computer software available in Arabic, language has not been a significant barrier to access.[9]

Compared to the relatively low internet penetration rate, mobile phone use is ubiquitous. By 2008, penetration surpassed 100 percent of the population, including individuals possessing two phones. The growth in mobile phone use was largely due to its increasing affordability, as a second provider joined the market in 2003 and prices dropped dramatically. By 2011, the price of a prepaid SIM card from the main provider, Libyana, was only 5LYD (US$4), to which a user could then add minutes depending on market prices, which were generally affordable. Smartphones and 3G connectivity have been available since 2006, though the prohibitive cost of more upscale models impedes their wider dissemination.[10] Since 2008, Voice over Internet Protocol (VoIP) has been freely accessible.

During the conflict that erupted in 2011, purchasing a SIM card became very difficult. A thriving black market emerged as illegal immigrants and expatriates sold their SIM cards for around 50LYD (US$40) before departing the country because mobile phones were being confiscated or stolen at checkpoints. Since the end of the fighting in August 2011, the above-mentioned tariffs have largely resumed, despite calls from the public to reduce them. In an effort to quickly appease customers as the NTC develops its telecommunications policy, the interim government topped up the majority of Libyan mobile phone subscribers with a 100LYD (US$80) voucher on two major Muslim holidays. Since the end of February 2012,

[7] Over the past decade, the government experimented with a flexible pay scale, awarding different wages for different jobs. Thus, average salaries in the public sector varied greatly according to the year of hiring and type of contract. In the private sector, especially in oil and gas, they varied according to company, location, industry, experience and benefits. In April 2011, the Qadhafi government increased salaries for some public sector positions, so the average income there rose to about 350 LYD.
[8] ITU, "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011.
[9] "The World Bank World Development Indicators: Libya," The World Bank, http://data.worldbank.org/country/libya.
[10] "Libyana Introduces 3G Services for First Time in Libya," The Tripoli Post, September 26, 2006, http://www.tripolipost.com/articledetail.asp?c=2&i=311.

there has been a serious shortage of WiMAX modems, driving up the price of second hand devices.

The state-run General Posts and Telecommunications Company (GPTC) is the main telecommunications operator and is fully owned by the government. In 1999, the GPTC awarded the first internet service provider (ISP) license to Libya Telecom and Technology (LTT) as a subsidiary of the state-owned firm. At least seven other companies—including Modern World Communication, Alfalak, and Bait Shams—have also been licensed to provide internet services, but they are subordinate to the LTT, which retains monopoly control over Libya's gateway to the international internet.[11] The GPTC also owns the two mobile phone providers, Almadar and Libyana.

This government chokehold over the communications network became critical in 2011, as Qadhafi's forces strategically limited access to the internet and mobile phones beginning January 25.[12] Initially, there were rolling outages, then in March, as the uprising gained momentum, the entire country's international internet connection was shut off. Mobile phone connectivity also became erratic. Access did not fully resume until August 2011, though there were some openings for government traffic and in the liberated enclaves. When the government shut down the internet, it did not completely sever the connection to the outside world as occurred in Egypt, but used a more sophisticated method that took longer to detect. One technical expert likened it to turning off a tap: "the stream of traffic was slowed to a trickle, and then a few drips."[13] In addition, strictly Libyan-based websites, like the state-run press and LTT-based email accounts, remained accessible to the population for a few more days.

Meanwhile, in April 2011, engineers supporting the rebels who had gained control of the eastern enclave of Benghazi hijacked the government-run cell phone towers of Libyana in that part of the country. They took independent control of the mobile phone network, renaming it Free Libyana.[14] In June 2011, a fiber-optic connection to Egypt was enabled

[11] United Nations Economic Commission for Africa, "The Status of Information for Development Activities in North Africa," (paper presented at the twentieth meeting of the Intergovernmental committee of experts, Tangier, Morocco, April 13-15, 2005), http://www.uneca.org/na/Information.pdf; "Internet Filtering in Libya – 2006/2007," OpenNet Initiative, 2007, http://opennet.net/studies/libya2007; "Telecoms in Libya" [in Arabic], Marefa.org, accessed August 30, 2012, http://www.marefa.org/index.php/%D8%A7%D9%84%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA_%D9%81%D9%8A_%D9%84%D9%8A%D8%A8%D9%8A%D8%A7.

[12] "Project Cyber Dawn v1.0, Libya," The Cyber Security Forum Initiative, April 17, 2011, p. 20, http://www.unveillance.com/wp-content/uploads/2011/05/Project_Cyber_Dawn_Public.pdf

[13] James Cowie, "What Libya learned from Egypt," Renesys (blog), March 5, 2011, http://www.renesys.com/blog/2011/03/what-libya-learned-from-egypt.shtml

[14] Margaret Coker and Charles Levinson, "Rebels Hijack Gadhafi's Phone Network," Wall Street Journal, April 13, 2011, http://online.wsj.com/article/SB10001424052748703841904576256512991215284.html; Spencer Akerman, "How Libya's Rebels got their cell service back," Wired, April 13, 2011, http://www.wired.com/dangerroom/2011/04/how-libyas-rebels-got-their-cellular-service-back/

with the help of the United Arab Emirates (UAE) firm Etisalat, improving internet connectivity. As a result, internet browsing and mobile phone calls were available in that part of the country throughout the conflict. In November 2011, the networks of the eastern and western parts of the country were unified, though infrastructure repairs continue in some areas.[15]

Internet access via ADSL or WiMAX was free of charge in the eastern part of the country during the conflict and became free throughout Libya for those with functioning equipment from November 2011 until March 1, 2012. This considerably increased the number of users and hours spent online. Pricing structures then returned and as of May 1, 2012, internet was available via mobile phone, landline, and cable networks throughout Libya for those who had modems and SIM cards. The account connection fees of the Qadhafi era returned, while monthly subscription rates slightly decreased and data usage quotas were raised. Despite these changes, internet speeds in Libya remain extremely slow.[16]

Since the end of the conflict, there have been no government-imposed restrictions on connectivity, but problems remain due to damaged infrastructure. As important as harm done to the telecom sector has been the damage to the electricity grid, which some estimate at US$1 billion.[17] For example, from mid-December 2011 to the end of February 2012, the western parts of Libya experienced rolling blackouts due to the heavy demand on conflict-damaged infrastructure. Without electricity, internet connectivity became impossible.

Although a popular access point previously, the cybercafe industry was decimated due to the months-long internet shutdown that began in February 2011, with almost all venues closing. As a result, in early 2012, most people accessed the internet from their homes, hotel lobbies, and workplaces (particularly those working for foreign organizations or companies).

The post-conflict regulatory environment remains very unclear. The interim government has a Ministry of Communications, but it has expressed no clear vision for the future. During the Qadhafi era, decisions on licensing were made by the government-controlled GPTC. In 2006, the General Telecom Authority (GTA) was formed with plans announced that it would be followed by a new regulator in 2009. At the time of the 2011 uprising, it remained unclear whether the GTA had come into existence, though some suspected it had been formed and mandated to oversee the monitoring of online activities.

[15] Fozia Mohamed, "Libya 2011: A Seminal Year Through Citizen Media," GlobalVoices, January 9, 2012, http://globalvoicesonline.org/2012/01/09/libya-2011-a-seminal-year-through-citizen-media/

[16] "Beyond LTT: The State of Libya's Internet," Kifah Libya, May 20, 2012, http://www.kifahlibya.com/2012/05/20/tech-beyond-ltt-the-state-of-libyas-internet/.

[17] "Cost of last year's damage to electricity industry put at $1bn," The Libya Herald, March 28,2012, http://www.libyaherald.com/cost-of-last-years-damage-to-electricity-industry-put-at-1-bn/.

LIMITS ON CONTENT

From 1998 to 2003, there was little blocking of online content in Libya, perhaps because the government did not see it as threatening or because most users were not inclined to visit overseas opposition websites.[18] In 2003, the government changed its attitude and Moussa Koussa, head of the Libyan Intelligence Agency at the time and a close Qadhafi aid, was tasked with monitoring and restricting the influence of opposition websites. Initially, a code of conduct approach was taken and cybercafes were instructed to install stickers by each computer warning customers not to visit websites that might negatively impact so-called national security or public morals. The aim was to instill fear in users, prompting them to self-censor political discourse.

Soon after, the government began blocking access to certain websites, a phenomenon that became noticeable in 2004. Initially, Arabic language content was targeted, though later European languages were censored as well. The blocking was sporadic rather than constant, perhaps in order to allow the government to plausibly deny it was deliberately censoring.

A reformist effort initiated in 2006 and led by Qadhafi's British-educated son Saif al-Islam resulted in a more lenient internet filtering regime,[19] and new websites adopting a critical position on corruption were launched and accessible.[20] The most recent testing by the OpenNet Initiative (ONI) in 2008-2009 indeed revealed a slight reduction in filtering. Censorship primarily targeted opposition websites like those of the National Front for the Salvation of Libya and Libya Watanona. According to ONI, filtering was done via IP blocking at the international gateway controlled by the LTT and users received a time out message rather than an alert acknowledging access was being denied by the government.[21] The reformist experiment ended in June 2009 with the nationalization of several privately owned outlets linked to Saif al-Islam. From then on, conditions for internet freedom rapidly declined. Cyber dissidents were arrested and imprisoned,[22] though blocking did not dramatically increase.

The government also passed a rule in 2006 mandating that websites registered under the ".ly" domain not contain content that is "obscene, scandalous, indecent or contrary to Libyan

[18] Doug Saunders, "Arab social capital is there – it's young and connected," The Globe and Mail, March 5, 2011, http://www.theglobeandmail.com/news/world/doug-saunders/arab-social-capital-is-there-its-young-and-connected/article1930770/.
[19] "Libya," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/libya.
[20] IREX,"Media Sustainability Index – Middle East and North Africa," *Media Sustainability Index 2008* (Washington D.C.: IREX, 2008), 25, http://www.irex.org/system/files/MENA_MSI_2008_Book_Full.pdf.
[21] "Internet Filtering in Libya – 2006/2007," OpenNet Initiative, 2007, http://opennet.net/studies/libya2007.
[22] Ismael Dbarra, "Internet in Libya: Everyone is rebelling against continued blocking and censorship," Elaph (Arabic), March 5, 2009, www.elaph.com/Web/politics/2009/3/415948.htm.

law or Islamic morality."[23] This rule appears to still be in effect under the interim government, which has not yet abolished it, but has not enforced it either.[24]

Since the rebels' victory in August 2011, all previously blocked websites, including those of Israeli newspapers, have become accessible again. Under the interim government, there have been no reports of website blocking or pressure to delete content. However, many Qadhafi-era government webpages containing information on laws and regulations from before the uprising are inaccessible, as is the online archive of formerly state-run Libyan newspapers. Some of these websites may have become defunct after the officials running them were ousted or fees to hosting providers were left unpaid, but others were likely deliberately taken down when the revolutionaries came to power.

As of May 2012, social media applications like the video-sharing website YouTube, the social-networking platform Facebook, and the microblogging service Twitter were freely accessible. YouTube had previously been blocked under the Qadhafi regime beginning in January 2010. Observers suspected the restriction was in response to the circulation of a video showing demonstrations by family members of detainees killed at the notorious Abu Salim prison, as well as footage of members of the Qadhafi family at luxurious parties.[25] Due to the split in the network during the conflict, YouTube was available in eastern regions beginning in April 2011, while it became accessible in the western parts in November 2011 after internet connectivity was restored. Other social media applications like Facebook and Twitter were blocked for a few weeks beginning in February 2011, shortly before the entire internet was cut off.[26]

Under Qadhafi, the highly repressive environment and fear of harsh punishments for critical speech contributed to extreme self-censorship by internet users. The Qadhafi regime was fairly explicit about what forms of speech were off limits. In a February 2011 text message sent to mobile phone users throughout the country, the regime warned citizens not to challenge the government stance on the application of Islamic law, the security and stability of Libya, the country's territorial integrity, and Qadhafi's persona.

By early 2012, the environment had loosened considerably and freedom of expression was flourishing. Still, a sizable number of Libyan bloggers and online journalists continue to practice some degree of self-censorship due to the fluid and uncertain political situation.

[23] "Internet Filtering in Libya – 2006/2007," OpenNet Initiative.
[24] "Regulations," Libya ccTLD, accessed August 30, 2012, http://nic.ly/regulations.php.

[25] "Watchdog urges Libya to stop blocking websites," AFP, February 4, 2010, http://www.google.com/hostednews/afp/article/ALeqM5gMqNCaIpcd74x_33F16sT_6IDriw.
[26] "Libya Blocks Facebook, Twitter and Aljazeera.net," ArabCrunch, February 18, 2011, http://arabcrunch.com/2011/02/libya-blocks-facebook-twitter-and-aljazeera-net.html.

There are few mechanisms in place to hold the interim government to account should they abuse their power. In addition, given the already tense and violent environment, many bloggers choose not to touch on social taboos like rape or tribal conflicts. Many also avoid publishing content critical of the 2011 revolution. Such unseen pressures contribute to an atmosphere of less than complete freedom.[27]

Blogging first emerged in Libya in 2003—with even Qadhafi launching his own blog in 2006 (www.alqathafi.org)—though the number of blogs based inside the country remained meager compared to other Arab countries.[28] Since the start of the revolution in February 2011, however, the contingent of blogs written by those inside Libya has notably increased. Under Qadhafi, most Arabic language blogs in Libya focused on poetry and storytelling, while some English language ones occasionally ventured into veiled criticism. Criticism of the regime mainly came from bloggers and websites based outside the country, who would sometimes post letters or comments from individuals in-country, thereby giving them a platform for free expression but protecting their identities.[29]

Libyans in the diaspora used social media to spread the word and show support for the February 17 "day of anger" that launched the revolution. A large number of Libyans inside the country responded, changing their surname on Facebook to "Libya" in a symbolic protest against Qadhafi's regime.[30] As of the first quarter of 2011, there were about 64,000 active Twitter accounts of Libyans based in-country and almost 200,000 people's Facebook activity was abruptly interrupted when Libya became disconnected from the internet in March.[31] Even so, prior to the revolution, most of the content on these social networks related to personal affairs rather than political activism due to the atmosphere of fear and self-censorship.

Once the uprising began, online media, blogs, and social networks played a visible role amplifying the voices of those inside the country, often via bloggers based in the diaspora. People in the eastern parts of the country, where internet access was available, uploaded videos and tweeted updates about what was happening. From the western parts, however,

[27] Tracey Shelton, "Libya's media has its own revolution," Global Post, March 18, 2012, http://mobile.globalpost.com/dispatch/news/regions/africa/120301/libya-media-revolution-newspapers-television-radio-journalism-free-speech.
[28] Claudia Gazzini, "Talking Back: How Exiled Libyans use the web to push for change," Arab Media Society, February, 2007, 3, http://www.arabmediasociety.com/articles/downloads/20070312142030_AMS1_Claudia_Gazzini.pdf.
[29] "Libya 2011: A Seminal Year Through Citizen Media," Global Voices, January 9, 2012, http://globalvoicesonline.org/2012/01/09/libya-2011-a-seminal-year-through-citizen-media/.
[30] "Project Cyber Dawn v1.0, Libya," The Cyber Security Forum Initiative, April 17, 2011, p. 14, http://www.unveillance.com/wp-content/uploads/2011/05/Project_Cyber_Dawn_Public.pdf.
[31] Racha Mourtada and Fadi Salem, "Civil Movements: the Impact of Facebook and Twitter, Dubai School of Government," Dubai School of Government, May 2011, Vol 1, No. 2, p. 5, http://www.dsg.fohmics.net/en/publication/Description.aspx?PubID=236&PrimenuID=11&mnu=Pri.

there was an eerie silence, except for a small number of individuals who had sophisticated equipment or physically carried content across the border into Tunisia.[32]

By comparison, since the fall of Qadhafi's regime, Facebook, Twitter and other digital media have grown in popularity and been used to mobilize Libyans for activism around a variety of causes. By April 2012, Facebook use had doubled to around 400,000 people, and the social networking tool was the most visited website in the country.[33] Bloggers, online journalists, and other users have vocally expressed a diverse range of visions for the post-Qadhafi political order, the interim government and other topics, though lingering self-censorship remains. People have also turned to Facebook to learn the latest news about upcoming events and some have used mass text message campaigns to rally support in the run-up to elections scheduled for mid-2012. Websites related to the Amazigh minority, whose language was banned under Qadhafi, are now flourishing.

VIOLATIONS OF USER RIGHTS

During the Qadhafi era, Libya's media environment was among the most tightly controlled in the world. Several laws provided for freedom of speech, but these protections were typically offset by vague language restricting the same freedoms. For example, the 1969 Libyan Constitutional declaration and the 1988 Green Charter for Human Rights both guarantee freedom of speech and opinion but also note that these must be "within the limits of public interest and the principles of the Revolution."[34] A new press law was discussed in 2007, but never realized.[35] A Telecommunications Law was discussed in 2010 but not officially put into effect and its draft is no longer available online. The judiciary was not independent.

Meanwhile, several laws authorized harsh punishments for those who published content deemed offensive or threatening to Islam, national security, territorial integrity, or the reputation of Qadhafi. The penal code called for imprisonment or the death penalty for anyone convicted of disseminating information critical of the state or the "Leader of the Revolution." The 1972 Publications Act imposed fines and up to two years in prison for a variety of violations, including libel, slander, and "doubting the aims of the revolution."[36]

[32] "Libya: Bloggers Between Dictatorship and War," Global Voices, August 21, 2011, http://globalvoicesonline.org/2011/08/21/libya-bloggers-between-dictatorship-and-war/.
[33] "Libya Facebook Statistics," Socialbakers, accessed April 10, 2012, http://www.socialbakers.com/facebook-statistics/libya; "The Top Sites in Libya," Alexa, accessed April 10, 2012, http://www.alexa.com/topsites/countries/LY.
[34] IREX, "Media Sustainability Index – Middle East and North Africa," *Media Sustainability Index 2008* (Washington D.C.: IREX, 2008), 27, http://www.irex.org/system/files/MENA_MSI_2008_Book_Full.pdf.
[35] IREX, "Media Sustainability Index – Middle East and North Africa," *Media Sustainability Index 2006/2007* (Washington D.C.: IREX, 2009), 33, http://www.irex.org/system/files/MENA%20MSI%202007%20Book.pdf.
[36] Freedom House, "Libya," *Freedom of the Press 2011*, http://www.freedomhouse.org/report/freedom-press/2011/libya.

Particularly egregious was a law on collective punishment, which allowed the authorities to punish entire families, towns, or districts for the transgressions of one individual.[37] Because of their vague wording these laws could be applied to any form of speech whether transmitted via the internet, mobile phone, or traditional media.

As of May 2012, these laws remained on the books. However, in what many viewed as a positive sign for the future, the NTC in August 2011 published a Draft Constitutional Charter for the Transitional Stage, intended to fill the gap before full elections and a new constitution come into effect. Article 13 of the Draft Charter guarantees "freedom of opinion for individuals and groups, freedom of scientific research, freedom of communication, liberty of the press, printing, publication and mass media."[38]

Under Qadhafi's rule, several internet users and online journalists were detained, prosecuted, and in some cases, killed, for disseminating or accessing information deemed undesirable by the regime. For example, in June 2005, Daif al-Ghazal, a former journalist for a pro-government news outlet who then began contributing stories critical of the authorities to overseas news websites, was abducted and tortured to death in custody.[39] In February 2011, as anti-government protests were getting off the ground, Qadhafi forces arrested several online activists, including the director and editor-in-chief of *Irassa*, an independent news website, and blogger Mohamed al-Hashim Masmari, who had posted videos online and given interviews to foreign media.[40] They are believed to have been released when the rebels liberated Benghazi. In an incident that gained international attention, Mohammed al-Nabbous, a citizen journalist who had launched an online live broadcast of events called Libya al-Hurra TV, was killed by Qadhafi-linked snipers in March 2011 while reporting on a battle near Benghazi.[41]

Although there is less fear of government repression in the post-Qadhafi era than previously, threats still remain. In March 2012, Sharifa Alfisa, an outspoken female independent

[37] IREX, "Media Sustainability Index – Middle East and North Africa," *Media Sustainability Index 2005* (Washington D.C.: IREX, 2006), 36, http://www.irex.org/system/files/MENA_MSI_2005-Full.pdf.
[38] "Draft Constitutional Charter for the Transitional Stage," Project on Middle East Democracy, August 2011, www.pomed.org/wordpress/wp-content/uploads/2011/08/Libya-Draft-Constitutional-Charter-for-the-Transitional-Stage.pdf.
[39] "Opposition journalist Daif Al Ghazal tortured to death," IFEX, June 6, 2005, http://www.ifex.org/libya/2005/06/06/opposition_journalist_daif_al_ghazal/.
[40] "Attacks on media continues across Middle East," Committee to Protect Journalists, February 2, 2011, http://cpj.org/2011/02/attacks-on-media-continue-across-middle-east.php; "Protestors take over state radio in Libya," Global Journalist, February 23, 2011, http://www.globaljournalist.org/freepresswatch/2011/02/libya/protesters-take-over-state-radio-in-libya/.
[41] "Journalists under attack in Libya: the tally," Shabab Libya, May 3, 2011, http://www.shabablibya.org/news/journalists-under-attack-in-libya-the-tally; Elizabeth Flock, "Libyan citizen journalist Mohammed Nabbous killed in fighting in Benghazi," The Washington Post (blog), March 21, 2011, http://www.washingtonpost.com/blogs/blogpost/post/libyan-citizen-journalist-mohammed-nabbous-killed-in-fighting-in-benghazi/2011/03/21/AB2rcA8_blog.html.

journalist writing for a number of online Libyan news sites, was abducted and beaten under mysterious circumstances in Benghazi by unidentified individuals.[42] She was released a couple of days later. Unconfirmed reports circulated that she was investigating the murder of General Abdulfatah Younis in which the NTC and Islamist militias are alleged to be implicated.[43] Others claimed she was kidnapped on suspicion of being pro-Qadhafi.[44]

Even under Qadhafi, there were few restrictions on anonymous communication over the internet, such as requiring user registration, perhaps because of other measures the authorities used to monitor users. However, customers were required to present identification when purchasing a SIM card.

Most Libyans had always suspected that the government was engaging in widespread surveillance of online communications. Beginning in 2009, cybercafe owners were required to sign binding commitments with the authorities to monitor those accessing the internet on their premises, including via installation of special software. However, the full extent of the Qadhafi regime's monitoring of Libyans' private communications became evident only after the liberation of Tripoli.[45] Indeed, it appeared that the regime had almost deliberately chosen to focus on surveillance rather than censorship as its main tactic for controlling online communications and curbing internet activism. State of the art equipment from foreign firms such as the French company Amesys,[46] and possibly the Chinese firm ZTE, were sold to the regime, enabling intelligence agencies to intercept communications on a nationwide scale and collect massive amounts of data on both phone and internet usage.[47] *Wall Street Journal* correspondents who visited an Internet Monitoring Center after the regime's collapse reported finding a storage room lined floor-to-ceiling with dossiers of the online activities of Libyans and some foreigners with whom they communicated.[48] According to current and former staff of LTT, as the rebellion gained momentum, the regime sought to ramp up surveillance and disable opposition websites. Among other measures adopted, the government reportedly recruited hackers from China and Eastern Europe to take down opposition websites and social media platforms, as well as generate malware to compromise activists' computers.[49] Extensive efforts were also made to develop

[42] "Story of the abduction of Sharifa Alfisa" [in Arabic], Law of Libya (forum), March 28, 2012, http://www.lawoflibya.com/forum/showthread.php?t=18618.
[43] Maha Ellawati, "Freed journalist still unable to talk," Libya Herald, March 29, 2012, http://www.libyaherald.com/?p=3697
[44] "Story of the abduction of Sharifa Alfisa" [in Arabic], Law of Libya (forum).
[45] Matthieu Aikins, "Jamming Tripoli: Inside Moammar Gadhafi's Secret Surveillance Network," Wired, May 18, 2012, http://www.wired.com/threatlevel/2012/05/ff_libya/6/.
[46] Ivan Sigal, "Libya: Foreign Hackers and Surveillance," Global Voices, October 27, 2011, http://advocacy.globalvoicesonline.org/2011/10/27/libya-foreign-hackers-and-surveillance/.
[47] Ibid.
[48] Paul Sonne and Margarent Coker, "Firms Aided Libyan Spies," The Wall Street Journal, August 30, 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html.
[49] Sasa Milosevic, "Serbia: Gaddafi's Cyber Army Oppose Rebels and NATO," Global Voices, March 30, 2011, http://globalvoicesonline.org/2011/03/30/serbia-gaddafis-cyber-army-oppose-rebels-and-nato/

the capacity to eavesdrop on Skype and VSAT connections. According to these LTT employees, the government even obtained backdoor access to Thuraya satellite phones, which were widely perceived as a secure means of communication.[50]

While many Libyans would like to believe that such widespread surveillance has ceased under the interim government, uncertainties remain. Given the lack of an independent judiciary or procedures outlining the circumstances under which the state may conduct surveillance, there is little to prevent the government or security agencies from resuming the practice. Some suspect that it has been activated to target those with an anti-Islamist agenda. During an interview on al-Hurra TV in March 2012, the Minister of Telecommunications stated that such surveillance had been stopped because the interim government wanted to respect the human rights of Libyans. An organization representing IT professionals in Libya refuted his remarks in an online statement, claiming those working in the telecom sector report that the surveillance system has been reactivated. Such allegations could not be independently verified, however.[51]

During the Qadhafi era, opposition websites like Libya Our Home (www.libya-watanona.com), those affiliated with the Muslim Brotherhood, and ones belonging to minorities like the Amazigh (www.tawalt.com) were periodically hacked, with the government widely suspected of being behind the attacks.[52] In 2009, a wave of such attacks targeted prominent opposition websites. They were found to have been carried out by a Libyan based in the United States, believed to be connected with the regime.[53] Another attack was reported in January 2011 against the opposition website al-Manara after it had posted videos of early anti-Qadhafi protesters in Bayda and al-Mostakbal.[54]

[50] Ibid.
[51] "Libya Telecom" Facebook post [in Arabic], March 31, 2012 at 7:16am, https://www.facebook.com/LibyaTelecom/posts/201142566662920.
[52] "Internet Filtering in Libya – 2006/2007," OpenNet Initiative, 2007, http://opennet.net/studies/libya2007
[53] Ismael Dbarra, "Internet in Libya: Everyone is rebelling against continued blocking and censorship" [in Arabic], Elaph, March 5, 2009, www.elaph.com/Web/politics/2009/3/415948.htm.
[54] Amira Al Hussaini, "Libya: Gaddafi wages war on the internet as trouble brews at home, "Global Voices, January 17, 2011, http://globalvoicesonline.org/2011/01/17/libya-gaddafi-wages-war-on-the-internet-as-trouble-brews-at-home/.

MALAYSIA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	9	10
Limits on Content (0-35)	11	14
Violations of User Rights (0-40)	21	19
Total (0-100)	**41**	**43**

* 0=most free, 100=least free

POPULATION: 29 million
INTERNET PENETRATION 2011: 61 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

The Malaysian government's active encouragement of internet and mobile phone access has resulted in a steady growth in the use of such media since the first internet service provider (ISP) was inaugurated in 1992. By 2011, internet penetration had reached over 60 percent of the population. In the watershed general elections of March 2008, the ruling National Front (BN) coalition lost its two-thirds parliamentary majority for the first time since 1969, and the use of the internet for political mobilization was widely perceived as contributing to the opposition's electoral gains.[1] Many observers then sensed that the government and ruling coalition had recognized the potential political impact of the internet and had therefore grown more determined to control it.

Such fears have not materialized, for the most part, though some restrictions have increased. Since early 2011, there has been a notable drop in the number of bloggers arrested and one notorious security law was repealed, but other troubling infringements on internet freedom have emerged. Prominent online news outlets and opposition-related websites have faced cyberattacks at politically critical moments, and legal amendments rendering intermediaries liable for seditious comments posted by other users were passed in April 2012. In addition, there has been a palpable increase in the presence of "cybertroopers," online commentators paid by the government and political parties to attack opponents through blogs and social media. Nevertheless, citizens continue to communicate via advanced web applications, online news websites, and social-networking services, and in July 2011, internet users

[1] "Malaysia's Uneasy Dance with the Web," Asia Sentinel, August 17, 2010, http://asiasentinel.com/index.php?option=com_content&task=view&id=2645&Itemid=178.

documented a police crackdown on peaceful protesters that was downplayed by the more tightly-controlled traditional media.

OBSTACLES TO ACCESS

Internet penetration in Malaysia is among the highest in Asia, reaching as many as 17.5 million users—or 60 percent of the population—by mid-2011, according to official figures and the International Telecommunications Union (ITU).[2] Malaysians can access the internet through home connections, their workplaces, mobile phones, or cybercafes. In April 2012, Kuala Lumpur's municipal government introduced a new policy to require businesses acquiring a food and beverage license to provide free or low cost WiFi service.[3] Cybercafes play an important role in bridging the urban-rural connectivity gap. Nevertheless, there remains an acute digital divide in the country, with more than 80 percent of internet users living in urban areas as of 2010,[4] and significantly lower penetration rates in more sparsely populated states in East Malaysia, where most residents belong to indigenous groups. To narrow this gap, by 2011, the government had reportedly established around 250 Community Broadband Centers nationwide and distributed nearly 500,000 netbooks to students and low income citizens in rural and suburban areas.[5]

Mobile phone use has also increased significantly in recent years, surpassing the country's total population in 2011, resulting in less of an urban-rural divide compared to internet connectivity. By the end of 2011, the number of subscribers was 36.6 million, indicating some individuals had multiple phone lines.[6] Mobile internet access is available and generally affordable. By mid-2011, there were about 10 million 3G subscribers and 2.9 million

[2] "Rural Broadband Initiatives in Malaysia," Ministry of Information Communication and Culture Malaysia, September 21, 2011, http://www.scribd.com/doc/68533475/Rural-Broadband-Initiatives-in-Malaysia; "Fixed line and broadband penetration rate hit 81%," Star Online, December 13, 2011, http://thestar.com.my/news/story.asp?file=/2011/12/13/parliament/10085852&sec=parliament; International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[3] Choong Mek Zhin, "DBKL to make it a requirement for restaurants to provide Wi-Fi services," Star Online, January 9, 2012, http://thestar.com.my/metro/story.asp?file=/2012/1/9/central/10210201&sec=central.

[4] "Malaysian Internet Usage Driven Primarily by People in Central Region," ComScore, October 7, 2010, http://www.comscore.com/Press_Events/Press_Releases/2010/10/comScore_Expands_Segmentation_Capabilities_in_Malaysia.

[5] "Rural Broadband Initiatives in Malaysia," Ministry of Information Communication and Culture Malaysia.

[6] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

broadband mobile users;[7] approximately 20 percent of Malaysians aged 20-24 reportedly accessed the internet via their mobile phones.[8]

The lack of high-quality infrastructure in many parts of the country remains the primary obstacle to improved connectivity.[9] In response, the Malaysian government has prioritized the development of broadband internet infrastructure. Broadband usage has increased significantly since 2007, with household penetration surpassing 60 percent by early 2012.[10] Nevertheless, the infrastructure remains insufficient to meet growing demand.[11] In March 2010, the government launched a National Broadband Initiative, which introduced five programs to expedite expansion of broadband internet and mobile phone coverage. Some programs were implemented in cooperation with formerly state-owned Telekom Malaysia, the country's largest telecommunications company, which retains a monopoly over the fixed-line network.[12] In addition, the introduction of wireless WiMAX technology since 2008 has enabled provision of broadband services to regions that are difficult to reach via cable connections; four WiMAX providers were in operation as of mid-2010.

Under the 1998 Communication and Multimedia Act (CMA), a license is required to own and operate a network facility. There are 25 ISPs operating in the country, most of them privately-owned. There have not been any reported denials of ISP license applications, but the licensing process could serve as a means of control, and the owners of major ISPs and mobile phone service providers often have connections to the government. Of the two largest ISPs, TMnet and Jaring, the former is a subsidiary of the privatized national phone company Telekom Malaysia, and the latter is wholly owned by the Ministry of Finance. Maxis Communications, the largest mobile phone service provider, was founded by Ananda Krishnan, who also owns the largest satellite broadcaster and enjoys close ties to former Prime Minister Mahathir Mohamad. Two new mobile phone providers have joined the market since 2008: YTL Communications and Umobile, both of whose owners are closely associated with the ruling party. In recent years, some local authorities have introduced

[7] "Rural Broadband Initiatives in Malaysia," Ministry of Information Communication and Culture Malaysia; "Communications and Multimedia Pocketbook of Statistics," Malaysian Communications and Multimedia Commission, 2011, http://www.skmm.gov.my/attachment/Pocket%20Book/Q3_2011_Eng.pdf.

[8] "Malaysian Internet Usage Takes Off in 2010," Nielsen Wire, April 25, 2011, http://blog.nielsen.com/nielsenwire/global/malaysian-internet-usage-takes-off-in-2010/.

[9] "Your 10 Questions for Dr. Mohamed Awang Lah," Star Online, May 22, 2010, http://biz.thestar.com.my/news/story.asp?file=/2010/5/22/business/6298179&sec=business.

[10] Pia Ruffino, "Malaysia to reach 60 per cent broadband penetration target," Asia Pacific FutureGov, March 11, 2011, http://www.futuregov.asia/articles/2011/mar/11/malaysia-reach-60-cent-broadband-penetration-targe/; "Communications and Multimedia Pocketbook of Statistics," Malaysian Communications and Multimedia Commission, 2011; "Malaysia among top 3 in economic impact of internet study," New Straits Times, February 1, 2012, http://www.nst.com.my/latest/malaysia-among-top-3-in-economic-impact-of-internet-study-1.40267#ixzz1lfi2fVQj.

[11] MCMC, "Broadband Meter: Subscribers and Users,"MyConvergence, March 2010, http://myconvergence.com.my/main/images/stories/SpecialEdition/pdf/MyConBumper_p97_BBMeter.pdf.

[12] Sira Habu and Shaun Ho, "RM 1 Billion Initiative to Promote High-Speed Broadband Usage," Star Online, March 25, 2010, http://thestar.com.my/news/story.asp?file=/2010/3/25/nation/5931577&sec=nation.

restrictions on cybercafe licensing to curb the mushrooming of venues offering access to illegal online activities like gambling. In some regions, this has also made it difficult for legitimate cybercafes to open, limiting the internet access opportunities for a broad range of users.

Regulation of the internet falls under the purview of the Malaysian Communications and Multimedia Commission (MCMC), which is overseen by the minister of information, communications, and culture. Both the MCMC and the ministry are guided by the CMA, which gives the information minister a wide range of licensing and other powers. The government appoints MCMC commissioners, although three out of the six commissioners represent non-governmental entities, currently all from the private sector.[13] Since 2008, the process for appointing members of the MCMC advisory board has become more transparent and participatory, involving consultations with diverse stakeholders and the inclusion of civil society members on the board. In past years, the MCMC had emerged as a driving force in efforts to curtail online speech. However, since early 2011, such aggressiveness subsided, possibly to avoid controversy ahead of elections to take place before April 2013.

LIMITS ON CONTENT

The Malaysian government does not employ any known filtering technology to actively block websites, though the authorities have taken other measures to restrict the circulation of certain information. A provision of the CMA explicitly states that nothing in the act "shall be construed as permitting the censorship of the Internet." The Bill of Guarantees of the Multimedia Super Corridor (MSC), an information technology development project, also promises no censorship of the internet. Throughout 2011, officials, including Prime Minister Najib Razak, repeatedly reinforced their commitment not to censor the internet.[14] However, in April 2012, the parliament passed an amendment to the 1950 Evidence Act that holds intermediaries liable for content posted by anonymous users, raising concerns that this would damper free expression online and open the door to selective, politically motivated prosecutions.

Incidents of website blocks have occasionally been reported. In May 2011, the MCMC sent a memo to ISPs requesting that they block access to 10 file-sharing websites (including Pirate

[13] Malaysian Communications and Multimedia Commission, "Commission members," http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=1.

[14] Melissa Chi, "PM vows no Internet censorship despite FB, Twitter influence," Malaysia Today, February 12, 2011, http://www.malaysia-today.net/mtcolumns/newscommentaries/38089-pm-vows-no-internet-censorship-despite-fb-twitter-influence; Kal Kamel, "No Internet censor, but bloggers must know where to draw the line: Malaysian Prime Minister," Grey Review, April 25, 2011, http://www.greyreview.com/2011/04/25/no-internet-censor-but-bloggers-must-know-where-to-draw-the-line-malaysian-prime-minister/; Clara Chooi, "Najib repeats promise of no Internet censorship," the Malaysian Insider, April 24, 2011, http://www.themalaysianinsider.com/malaysia/article/najib-repeats-promise-of-no-internet-censorship/.

Bay and Megavideo) in an effort to crackdown on copyright violations. The memo cited Section 263 of the CMA alongside the copyright law as the basis for the requested blocking.[15] In addition, many government-linked companies and public universities restrict access for their students and employees to certain sensitive websites, such as the independent online news outlet Malaysiakini.

Although there is no significant technical blocking, there have been cases of administrative efforts to remove content from the internet. The MCMC has been known in the past to track online discussions and then instruct bloggers or online news outlets to remove content perceived as overly critical of the government. Procedures surrounding such requests are generally nontransparent. The energy, water, and communications minister reported in September 2008 that the MCMC had formed a panel to monitor websites and blogs that was composed of representatives from the police, attorney general's office, and the Home Ministry. Although this mechanism appears to be somewhat active, there were no controversial incidents reported in 2011 and early 2012, as there had been in 2009 when the MCMC directed Malaysiakini to take down two videos from its website.[16]

In January 2011, a top Home Ministry official announced that the government was considering amending the Printing Presses and Publications Act (PPPA) to expand its scope to online content, including possibly to posts on blogs, the social-networking site Facebook, or the video-sharing platform YouTube.[17] The PPPA is one of several laws that restrict freedom of expression among traditional media, in part by requiring news outlets to obtain annual ministerial permission for their continued publication. The statement immediately prompted a strong outcry from parliament members,[18] news websites,[19] and a range of Malaysian civil society groups.[20] The government appears to have subsequently abandoned the proposal.

[15] "Pirate Bay, MegaUpload & Others Blocked By Government Order," Torrent Freak (blog), June 9, 2011, http://torrentfreak.com/pirate-bay-megaupload-others-blocked-by-government-order-110609/.

[16] The videos showed Muslim demonstrators marching with a cow's head to protest the relocation of a Hindu temple. Malaysiakini's editor-in-chief, Steven Gan, refused to comply with the order, stating that his outlet had no ill intentions in posting the videos. The MCMC forwarded the case to the attorney general, urging that Malaysiakini be prosecuted for failing to comply with the removal order. Should the attorney general pursue the case, Malaysiakini faces a potential fine of up to 50,000 ringgits (US$14,300), and Gan could receive up to a year in prison. As of May 2012, the attorney general had not yet made a final decision whether to pursue the or not. This was the only reported case of its kind. See, Reporters Without Borders, "Malaysiakini Website Refuses to Bow to Censorship," news release, September 24, 2009, http://en.rsf.org/malaysia-malaysiakini-website-refuses-to-24-09-2009,34575.

[17] "Publications Act to be amended to address loopholes," Star Online, January 26, 2011, http://thestar.com.my/news/story.asp?file=/2011/1/26/nation/7873307&sec=nation.

[18] Jerrenn Lam, "Malaysia: Amending the law to censor internet?" Global Voices (blog), February 15, 2011, http://globalvoicesonline.org/2011/02/15/malaysia-amending-the-law-to-censor-internet/.

[19] Steven Gan, "A killer blow to online media," Malaysiakini, January 26, 2011, http://www.malaysiakini.com/news/154538.

[20] International Freedom of Expression eXchange (IFEX), "Civil society groups oppose government plan to impose Internet censorship," news alert, February 2, 2011, http://www.ifex.org/malaysia/2011/02/02/opposition_to_censorship/.

In a more troubling development, in April 2012, the parliament passed an amendment to the 1950 Evidence Act that holds intermediaries liable for seditious content posted anonymously on their networks or websites.[21] This would include hosts of online forums, news outlets, and blogging services, as well as businesses providing WiFi services.[22] The amendment also holds liable the person whose name is attributed to such content or who owns the computer it was sent from, whether or not they were indeed the author, thereby presuming guilt and shifting the burden of proof to the accused.[23] The legal change was pushed through hurriedly, but garnered significant public backlash after its passage. As of early May 2012, the amendment had yet to come into effect. Civil society and lawyers' groups were mobilizing efforts to pressure the government to delay its entrance into the official gazette.[24]

The level of self-censorship appears to have remained consistent compared to previous years. Although the repeated prosecution of bloggers has caused some online writers to exercise greater caution, critical commentary and exposés of official misconduct have a regular presence in online discourse. The authorities discourage free expression on "red-line" issues such as Islam's official status, race, royalty, and the special rights enjoyed by *bumiputera* (ethnic Malays and other indigenous people, as opposed to the ethnic Chinese and Indian minorities).

Expanded internet access has led to the emergence of a vibrant blogosphere, and an increasing number of Malaysians are turning to the internet as their main source of news. Advanced web applications like YouTube, Facebook, and the microblogging application Twitter are freely accessible and their use has grown dramatically in recent years. In early 2012, Facebook, YouTube, and Google's blog-hosting service Blogger were among the top five most visited websites, while Malaysiakini was ranked 14th and the more pro-government *Star Online* was ranked 20th.[25] An October 2011 study by the digital analytics company ComScore found that Malaysians over the age of 15 spent approximately one-third of their time on social-networking services.[26] By May 2012, there were just over 12 million

[21] Eva Galperin, "This Week in Internet Censorship: Points system for Weibo, Activist Released in Bahrain, Censorship in Malaysia, Ethiopia, and More," Electronic Frontier Foundation, May 31, 2012, https://www.eff.org/deeplinks/2012/05/week-internet-censorship-points-system-weibo-activist-released-bahrain-censorship.
[22] Teoh El Sen, "Paktan seeks to halt new Evidence Act," Free Malaysia Today News, June 28, 2012, http://www.freemalaysiatoday.com/category/nation/2012/06/28/pakatan-seeks-to-halt-new-evidence-act/.
[23] Parliament of Malaysia, *Act to amend the Evidence Act 1950*, 2012, http://www.parlimen.gov.my/files/billindex/pdf/2012/DR162012E.pdf.
[24] The amendment reportedly came into effect in June 2012. See, Edwin Yapp, "Evidence Act amendments, a slippery slope," Digital News Asia, May 24, 2012, http://www.digitalnewsasia.com/node/165.
[25] "Top Sites in Malaysia," Alexa Web Information Company, accessed January 25, 2012, http://www.alexa.com/topsites/countries/MY.
[26] "Social Networking Accounts for One Third of All Time Spent Online in Malaysia," ComScore, October 17, 2011, http://www.comscore.com/Press_Events/Press_Releases/2011/10/Social_Networking_Accounts_for_One_Third_of_All_Time_Spent_Online_in_Malaysia.

Facebook users in the country, reflecting about 70 percent of internet users and more than 40 percent of the total population.[27] There were at least 1.6 million estimated Twitter users by the end of 2011.[28] Almost all prominent politicians and civil society groups, including those representing ethnic minorities, blog or tweet regularly, and many also have a presence on Facebook. English and Malay are the dominant blogging languages.

The government seems to have decided that it is preferable to engage with and rebut online criticism than to censor it. Prime Minister Najib Razak blogs and is an ardent Facebook user, boasting over one million followers.[29] He and other government representatives have used websites and social media to directly communicate with citizens. The police force, for example, has Facebook and Twitter accounts where officers provide updates on policing activities and occasionally respond to accusations of abuse by members of the public.[30]

Some such engagement has taken a more manipulative turn, however. Notably, since 2010 there has been a palpable increase in the number of "cybertroopers" used by political parties to generate favorable content on their behalf or to post information harmful to their opponents' reputation. Both government and opposition sources have confirmed that bloggers and other online commentators are paid to influence internet content,[31] though it appears that the resources available to the ruling coalition are greater. Concerns have also been raised that large sums of public funds have been used toward this purpose. The prime minister's National Front (BN) party, for example, reportedly has its own Unit Media Baru, a group of bloggers paid to improve the party's image online. In February 2012, the government admitted paying international PR firm FBC Media 83.8 million MYR (US$26.5 million) to boost Prime Minister Najib's image abroad via programming on the British Broadcasting Corporation (BBC) and CNBC.[32] Other reports have indicated that as much as US$55,000 per month had been promised to FBC Media for online campaigns, including ones involving bloggers based in the United States.[33] The impact of the government's efforts

[27] Lim Yung-Hui, "Facebook Hits 70% Penetration Rate in Malaysia," Forbes, December 20, 2011, http://www.forbes.com/sites/limyunghui/2011/12/20/facebook-hits-70-penetration-rate-in-malaysia/.
[28] "Lead Generation and Internet Marketing in Malaysia," MVF Global, accessed September 18, 2012, http://www.mvfglobal.com/malaysia.
[29] Najib Razak's Facebook page, accessed July 19, 2012, www.facebook.com/najibrazak; Najib Razak's blog, "1Malaysia," accessed July 19, 2012, http://www.1malaysia.com.my/.
[30] Polis Diraja's Facebook page, http://www.facebook.com/PolisDirajaMalaysia.
[31] Joanna Yap, "PRS' cyber-troopers ready for coming polls," Boreno Post Online, March 22, 2012, http://www.theborneopost.com/2012/03/22/prs-cyber-troopers-ready-for-coming-polls/; Lim Guan Eng, "Najib's new army of cyber troopers with a history of dirty tricks is proof that the 13th general election will be the dirtiest election yet," DapMalaysia, November 21, 2011, http://dapmalaysia.org/english/2011/nov11/lge/lge1414.htm.
[32] Mariam Mokhtar, "Sorry no cure, BBC," Free Malaysia Today News, February 17, 2012, http://www.freemalaysiatoday.com/category/opinion/2012/02/17/sorry-no-cure-bbc/; "BBC's worldwide apology exposes Malaysian govt's image," Harakah Daily, February 13, 2012, http://en.harakahdaily.net/index.php/berita-utama/4376-bbcs-worldwide-apology-exposes-malaysian-govts-image.html
[33] "New Revelations Link FBC Media to BN's Dirty Tricks Blogging Campaigns—Latest Expose!" Sarawak Report, August 7, 2011, http://www.sarawakreport.org/2011/08/dirty-tricks-new-revelations-link-fbc-media-to-bns-blogging-campaigns/.

remains unclear, however, as observers noted that the opposition retained the upper hand in the blogosphere at the end of 2011.[34]

Online news sources and social media have emerged as effective tools for political mobilization and challenging the government's grip on traditional media. This was especially evident before, during, and after a July 2011 rally calling for electoral reforms, greater government transparency, and reduced corruption. The protest was organized by the Coalition for Free and Fair Elections (Bersih 2.0)—whose Facebook page had 200,000 fans—and drew tens of thousands of people to the streets, despite warnings of a government crackdown. The authorities responded harshly and arrested over 1,500 protestors, though most were quickly released. Mainstream media downplayed police brutality or distorted the protestors' largely peaceful behavior in an effort to justify the assault. By contrast, social media were flooded with images of police firing teargas and water cannons, chasing and arresting demonstrators, or wearing riot gear as they face off with protestors.[35] According to one blogger, nearly 900,000 tweets with relevant hashtags were circulated and 1,600 videos were uploaded to YouTube,[36] including one posted by Malaysiakini that showed police beating a participant.[37] Within one week of the incident, a Facebook petition calling for the prime minister's resignation had garnered 200,000 supporters. In the run-up to general elections in 2013, the influence of online news and social media is expected to further increase.

VIOLATIONS OF USER RIGHTS

Malaysia's constitution provides citizens with "the right to freedom of speech and expression," but allows for limitations on this right. The government exercises tight control over print and broadcast media through restrictions on licensing and the use of the Official Secrets Act (OSA), the Sedition Act, and harsh criminal defamation laws to penalize journalists and other critics. Violations of these laws are punishable by several years in prison.

[34] Tedewin Ngumbang, "Barisan Nasional Unit Media Baru Will Wallop Opposition a PBB YB Boasted!" Borneo Warrior (blog), September 27, 2011, http://borneo-warrior.blogspot.com/2011/09/barisan-nasional-unit-media-baru-will.html; Nawawi Mohamad, "Money and infighting in Umno: Even the cyber-troopers have to play it 'smart,'" Malaysia Chronicle, May 19, 2012, http://malaysia-chronicle.com/index.php?option=com_k2&view=item&id=33361:money-and-infighting-in-umno-even-the-cyber-troopers-have-to-play-it-smart&Itemid=2.

[35] "Police Beating," YouTube video, :53, posted by "malaysiakini," July 9, 2011, http://www.youtube.com/verify_age?next_url=/watch%3Fv%3DZqCmcF7pZZI; Jerrenn Lam, "Malaysia: Bersih 2.0 Rally Rattles the Government," Global Voices (blog), July 11, 2011, http://globalvoicesonline.org/2011/07/11/malaysia-bersih-2-0-rally-rattles-the-government/.

[36] Joshua Ongys, "Statistics on Bersih 2.0 Rally – Malaysia 9 July 2011," Joshuaongys.com (blog), July 9, 2011, http://joshuaongys.com/2011/07/bersih-2-0-rally-malaysia-9-july-2011-online-social-media-statistics-youtube-facebook-twitter/.

[37] "Police Beating," YouTube video, :53, posted by "malaysiakini," July 9, 2011.

With regard to online expression, the government has repeatedly circumvented protections afforded by the MSC Bill of Guarantees and the CMA,[38] carrying out arbitrary arrests and launching investigations against internet users under the older, more restrictive laws that had principally been applied to traditional media. In some cases, the government has relied in prosecutions on the CMA itself and its broadly worded Section 233, which bans content deemed "indecent, obscene, false, threatening, or offensive."[39] In 2009 and 2010, several individuals were arrested and charged with sedition for comments posted in blogs[40] or for alleged threats made on Facebook.[41] In 2011, fewer such cases reported and several earlier prosecutions were discontinued. Nevertheless, defamation cases against bloggers that involved disproportionate requests for damages threatened to chill online expression.

In September 2011, Prime Minister Najib Razak raised hopes at home and abroad when he announced that the government would abolish or amend some of the country's harsh security laws, like the Internal Security Act (ISA).[42] Indeed, in April 2012, several important changes were made to the legal framework surrounding freedom of expression and national security. The ISA, which allowed for detention without trial and had been used in the past to detain bloggers, was abolished. That same month, the Security Offenses (Special Measures) Act (SOA) was passed to replace it, though as of May 2012, it had yet to come into effect. The new law provides several improved protections to detainees. These include requiring police to immediately inform a detainee's family and reducing to 28 days the maximum amount of time that someone can be held without charge or being brought before a judge.[43] The law also includes a provision explicitly stating that "no person shall be arrested and detained…solely for his political belief or political activity."[44] Despite these improvements, the law also includes restrictive provisions absent in its predecessor. For example, it grants wide-ranging powers for the Public Prosecutor—and in emergency situations, the police—

[38] Multimedia Super Corridor (MSC), "MSC Malaysia 10-Point Bill of Guarantees," accessed November 16, 2010, http://www.mscmalaysia.my/topic/MSC+Malaysia+Bill+of+Guarantees; MCMC, "Communications and Multimedia Act 1998," accessed November 16, 2010, http://www.skmm.gov.my/index.php?c=public&v=art_view&art_id=43.

[39] Reporters Without Borders, "Malaysiakini Website Refuses to Bow to Censorship," news release, September 24, 2009, http://en.rsf.org/malaysia-malaysiakini-website-refuses-to-24-09-2009,34575.

[40] Charles Ramendran, "Bomb Threat by Blogger," Sun2Surf, January 13, 2010, http://www.sun2surf.com/article.cfm?id=42322.

[41] G Vinod, "PAS Member: I Did Not Threaten to Kill Saiful," Free Malaysia Today, May 19, 2010, http://www.freemalaysiatoday.com/fmt-english/news/general/5771-pas-member-i-did-not-threaten-to-kill-saiful.

[42] "Najib announces major changes in controversial laws as Malaysia Day gifts," Star Online, September 16, 2011, http://thestar.com.my/news/story.asp?file=/2011/9/16/nation/20110916070850&sec=nation; James Hookway, "Malaysian Leader Opens Door for Reforms," The Wall Street Journal, September 16, 2011, http://online.wsj.com/article/SB10001424053111903927204576571934144265052.html?mod=WSJASIA_hpp_MIDDLETopNews; "Malaysia Repeals Security Act and Emergency Provisions," Freedom House, http://www.freedomhouse.org/article/malaysia-repeals-security-act-and-emergency-provisions.

[43] Parliament of Malaysia, *Security Offences (Special Measures) Act 2012*, accessed September 18, 2012, http://www.parlimen.gov.my/files/billindex/pdf/2012/DR152012E.pdf.

[44] Ibid.

to intercept communications without the need for a court order in cases involving security offenses.[45]

While the SOA focuses primarily on security offenses, the government also made changes to the penal code that could allow for punishment of political speech, specifically adding a new criminal offense of "any activity detrimental to parliamentary democracy." Civil society groups raised concerns that this broadly defined term could be construed to include criticism of parliament, government officials, or particular policies, rendering such expression punishable with jail time. The law minister stated in an interview, however, that the provision would not be applied for nonviolent activities.[46] Meanwhile, other laws previously used to detain bloggers, such as the OSA and Sedition Act, remain in place.

In 2011, a number of bloggers faced legal harassment, intimidation, fines, and brief periods of detention. No bloggers were imprisoned at year's end, though several had charges pending against them. Among them was Raja Petra Kamarudin, a blogger and founder of *Malaysia Today* who fled into exile in 2009 to avoid sedition charges.[47] Although some charges against him were dropped, he reportedly continues to be the subject of various police investigations due to his criticism of the government from abroad. [48]

Bloggers have also been arrested on charges of sedition after posting remarks critical of the monarchy. In 2009 and 2010, there were at least ten such cases, but only one ended in conviction.[49] In 2011, the number of such detentions dropped dramatically, though at least one such incident occurred. In March 2011, blogger Mohd Nur Hanief Abdul Jalil was arrested for referencing on his blog allegations of a sex scandal involving the Sultan of Selangor and a celebrity model.[50] He was investigated under the Sedition Act by police and

[45] Ibid.
[46] Shahanaaz Habib, "A matter of trial and error," Star Online, April 22, 2012, http://thestar.com.my/news/story.asp?file=/2012/4/22/nation/11153338&sec=nation.
[47] Teh Eng Hock, "Raja Petra Can't Be Tried in Britain," Star Online, May 26, 2010, http://thestar.com.my/news/story.asp?file=/2010/5/26/nation/6340987&sec=nation.
[48] K Kabilan, "RPK: 1Malaysia Will Be Najib's Downfall," Free Malaysia Today, May 25, 2010, http://politicalwatchmalaysia.blogspot.com/2010/05/rpk-1malaysia-will-be-najibs-downfall.html; "Perkasa Makes Police Report Against Raja Petra," Malaysia Today, January 7, 2010, http://malaysia-today.net/mtcolumns/newscommentaries/29452-perkasa-makes-police-report-against-raja-petra.
[49] Centre for Independent Journalism, "Debate on Royal Powers Draws Attacks and Threats; Bloggers Ahiruddin Attan and Jed Yoong Questioned by Police," International Freedom of Expression eXchange (IFEX), March 4, 2009, http://www.ifex.org/malaysia/2009/03/04/capsule_report_debate_on_royal/; Centre for Independent Journalism, "Six People Charged with 'Insulting' Royalty Online," International Freedom of Expression eXchange (IFEX), March 16, 2010, http://www.ifex.org/malaysia/2009/03/16/six_people_charged_with_insulting/; International Freedom of Expression eXchange (IFEX), "Government Hounds Bloggers That Criticise Royalty," news alert, March 25, 2009, http://www.ifex.org/malaysia/2009/03/25/government_hounds_bloggers_that/.
[50] Hanief, Malaysia: Tong Taik Umno (blog), Hanief.blogspot.com.

MCMC officials. No charges were pressed, however, and he was released within 24 hours.[51] Sedition charges against blogger Khairul Nizam Abdul Ghani from 2010 were also still pending as of May 2012.[52]

More common in 2011 were disproportionate defamation suits filed against bloggers. In July 2011, a Kuala Lumpur court ordered blogger and opposition party member Amizudin Ahmat to pay 400,000 MYR (US$130,000) in damages and legal costs to Minister of Information, Communications, and Culture Rais Yatim. Amizudin had posted on his blog allegations that Yatim had raped an Indonesian maid working in his home, copying the information from a news website.[53] Upon realizing the report's inaccuracy, the blogger deleted it and apologized to Yatim. The latter's continued pursuit of the case and the exorbitant punishment raised concerns of politically motivated intimidation.[54] In February 2011, the Japanese company Asahi Kosei filed a defamation suit for 10 million MYR (US$3.3 million) against activist Charles Hector, who authored blog posts about abuses of Burmese migrant workers at the firm's facility in Malaysia, drawing on a series of interviews conducted with employees.[55] In August, the case was settled out of court, with Hector promising to pay 1 MYR in damages and publish an apology in local media. Labor and human rights advocates criticized the outcome, speculating that Hector was left with no choice but to comply because of the high sums involved, although his investigation was legitimate.[56] In a more unusual case from June 2011, Fahmi Fazdil, a social commentator and aide to an opposition politician, was forced to apologize on Twitter 100 times as part of a settlement in a defamation case with Blulnc Media. The case related to a tweet Fazdil had sent in January claiming a pregnant friend employed by the company had been poorly treated.[57]

[51] "Blogger 'arrested' at midnight under Sedition Act," Malaysia Today, March 19, 2011, http://malaysia-today.net/mtcolumns/from-around-the-blogs/38903-blogger-arrested-at-midnight-under-sedition-act; "Blogger 'arrested' at midnight under Sedition Act," Uppercaise (blog), March 19, 2011, http://uppercaise.wordpress.com/2011/03/19/blogger-hanief-faces-sedition-probe/.

[52] "Malaysian Blogger Charged with Insulting Dead Sultan," China Post, January 31, 2010, http://www.chinapost.com.tw/asia/malaysia/2010/01/31/243065/Malaysian-blogger.htm; Sarban Singh, "Blogger pleads not guilty to insulting Johor royals (update)," Star Online, January 29, 2010, http://thestar.com.my/news/story.asp?file=/2010/1/29/nation/20100129170602&sec=nation.

[53] M. Mageswari, "Dr Rais sues blogger over rape allegation, May 6 for case management," Star Online, April 18, 2011, http://thestar.com.my/news/story.asp?file=/2011/4/18/nation/20110418160508&sec=nation.

[54] International Freedom of Expression eXchange (IFEX), "Opposition blogger ordered to pay exorbitant damages to minister," news alert, July 22, 2011, http://www.ifex.org/malaysia/2011/07/22/amizudin_defamation_suit/.

[55] International Freedom of Expression eXchange (IFEX), "Blogger on migrant workers' treatment faces company's defamation claim," news alert, June 24, 2011, http://www.ifex.org/malaysia/2011/06/24/charles_hector_lawsuit/.

[56] "Malaysian migrant workers' advocate pressured to accept settlement with electronics company," Clean Clothes Campaign, September 5, 2011, http://www.cleanclothes.org/news/malaysian-migrant-workers-advocate-made-to-accept-settlement-with-electronics-company; "Malaysia: Defamation case against human rights defender Charles Hector Fernandez ended with a settlement," World Organization Against Torture, August 26, 2011, http://www.omct.org/human-rights-defenders/urgent-interventions/malaysia/2011/08/d21400/.

[57] "Malaysian to tweet apology 100 times in Twitter defamation case," The Guardian, June 2, 2011, http://www.guardian.co.uk/world/2011/jun/02/malaysian-tweet-apology-defamation.

Some bloggers have faced legal harassment for content that most observers regarded as humorous satire. In September 2010, police arrested cartoonist Zulfiklee Anwar Ulhaque, better known as Zunar, under the ISA for publishing cartoons deemed insulting to the prime minister and his deputy. Zunar was quickly released and no formal charges were pressed.[58] He subsequently sued the government for unlawful detention.[59] In a positive development, a case filed against blogger Irwan Abdul Rahman in 2010 was dropped in March 2011.[60] The MCMC had charged Rahman with circulating false news over a satirical blog post claiming that Malaysia's main utility company was planning to sue the World Wildlife Fund for its Earth Hour initiative, in which individuals are requested to turn off all lights and electrical appliances for one hour.[61] A small number of other cases have involved content related to religion or corruption allegations.[62]

In recent years, the authorities have repeatedly hinted that they may take steps to register bloggers, though the idea has been set aside following protests by the blogging community and journalists. In December 2011, news emerged of a Computing Professionals Bill being considered.[63] If passed, the law would initiate registration with a government-appointed board of all computing and information technology (IT) professionals working on Critical National Information Infrastructure (CNII).[64] The sudden announcement caught many IT professionals off-guard, sparking confusion and anger.[65] Among the criticisms of the bill were the inclusion of minimum educational requirements as a prerequisite to registration and the

[58] "Malaysian Cartoonist Goes into Hiding After Sedition Arrest," RFI English, September 28, 2010, http://www.english.rfi.fr/asia-pacific/20100928-malaysian-cartoonist-goes-hiding-after-sedition-arrest.

[59] In July 2012, the High Court ruled that the police had acted unlawfully when confiscating 66 copies of a compilation of Zunar's cartoon, but that their detention of Zunar was legal. K. Pragalath, "Partial victory for cartoonist Zunar," Free Malaysia Today, July 31, 2012. http://www.freemalaysiatoday.com/category/nation/2012/07/31/partial-victory-for-cartoonist-zunar/. Tom Spurgeon, "CR Holiday Interview #7: Zunar," The Comics Reporter, December 27, 2010, http://www.comicsreporter.com/index.php/cr_holiday_interview_7_zunar/.

[60] International Freedom of Expression eXchange (IFEX), "Case against blogger withdrawn, but disturbing message prevails," news alert, March 18, 2011, http://www.ifex.org/malaysia/2011/03/18/case_dropped/.

[61] Reena Raj, "MM Editor Charged for Poking Fun at TNB," Malay Mail, September 2, 2010, http://www.mmail.com.my/content/48276-mm-editor-charged-poking-fun-tnb; Hafizah Hoze Rizal, "Blogger Hassan Skodeng's Case Set for March 15," Malay Mail, January 26, 2011, http://www.mmail.com.my/content/62051-blogger-hassan-skodengs-case-set-march-15.

[62] In August 2010, the right–wing group Perkasa lodged a complaint against blogger Helen Ang for authoring an article that questioned the position of Islam in Malaysia; as of May 2012, the case was still pending, but observers felt it was unlikely the attorney general would pursue it. "Perkasa Lodges Report Against Blogger," Malaysian Insider, August 9, 2010, http://www.themalaysianinsider.com/malaysia/article/perkasa-lodges-report-against-blogger/.

[63] Lim Yung-Hui, "Malaysian IT Community Response to Board of Computing Professionals Malaysia Bill 2011: Where's the Beef?," Forbes, December 12, 2011, http://www.forbes.com/sites/limyunghui/2011/12/12/malaysian-it-community-response-to-board-of-computing-professionals-bill-2011-wheres-the-beef/; Vijandren Ramadass, "Computing Professionals Bill 2011 – Draft," Lowyat.net (blog), December 9, 2011, http://www.lowyat.net/v2/index.php?option=com_content&task=view&id=5800&Itemid=2.

[64] "The Computing Professionals Bill 2011: An Orwellian "Big Brother"," Philosophy Politics Economics (blog), December 13, 2011, http://tonypua.blogspot.com/2011/12/computing-professionals-bill-2011.html

[65] Malaysians Against Board of Computing Professionals Bill Facebook Page, http://www.facebook.com/pages/Malaysians-Against-Board-of-Computing-Professionals-Bill/289002177811647.

broad definition of CNII to include not only banking and national security sectors, but also energy, transportation, health, and government.[66] Responding to the outcry, the Ministry of Science, Technology and Innovation claimed that registration would be voluntary.[67] As of May 2012, the bill had not yet been introduced to parliament.

The extent of government surveillance of the internet is unclear, but privacy protections are generally poor in Malaysia. As noted above, the new SOA allows for the interception of communications without a judicial order, at least in cases involving security offenses.[68] The authorities appear to be capable of identifying anonymous internet and mobile phone users with the help of service providers. Ongoing court cases indicate that police regularly gain access to the content of text messages from telecommunications companies, sometimes without needing to go through judicial channels. Beginning in 2007, all mobile phone users, including roughly 18 million prepaid users, were required to register as part of an effort to decrease rumor mongering, though the rule appears to have been weakly enforced. Users in cybercafes are not required to register.[69] A government plan to provide free email accounts to all citizens over the age of 18 was announced in 2011, prompting fears it would expand the government's ability to monitor people's online activities.[70]

Although bloggers and online journalists have been subject to arbitrary arrest, they generally do not face physical violence. However, independent online news outlets and some opposition-related websites continue to face distributed denial-of-service (DDoS) attacks, including at moments of crucial political importance. For example, the popular independent online news outlet Malaysiakini was rendered inaccessible by sustained DDoS attacks in April 2011, days before important state elections in Sarawak.[71] It was targeted again in July 2011 in the run-up to the Bersih 2.0 rally, but weathered them better thanks to a server upgrade.[72] Several other news websites and blogs were hit by attacks during those same periods.

[66] "Computing Professionals Bill 2011 Preliminary Analysis," Illegitimate Code (blog), December 10, 2011, http://illegitcode.wordpress.com/2011/12/10/computing-professionals-bill-2011-analysis/; Foong Cheng Leong & Joachim Leong, "Computing Professionals Bill 2011 – Ambiguity, Arbitrariness and Uncertainty," The Malaysian Bar, December 13, 2011, http://www.malaysianbar.org.my/legal/general_news/computing_professionals_bill_2011_ambiguity_arbitrariness_and_uncertainty.html.

[67] "MCA: Computing Professionals Bill will stifle talent growth," December 21, 2011, http://www.nst.com.my/local/politics/mca-computing-professionals-bill-will-stifle-talent-growth-1.22120 (site discontinued).

[68] Privacy International, *Privacy in Asia: Final Report of Scoping Project*, November 2009, https://www.privacyinternational.org/issues/asia/privacy_in_asia_phase_1_report.pdf.

[69] "Dec 15 Registration Deadline Stays: MCMC," Bernama, August 18, 2006, http://www.bernama.com/kpdnhep/news.php?id=214811&lang=en.

[70] Rebekah Heacock, "Malaysia: Government's Free E-mail Plan Met with Opposition," OpenNet Initiative, April 26, 2011, http://opennet.net/blog/2011/04/malaysia-governments-free-e-mail-plan-met-with-opposition.

[71] Mong Palatino, "Malaysia: Cyber Attacks Shut Down Independent News Website," Global Voices (blog), April 13, 2011, http://globalvoicesonline.org/2011/04/13/malaysia-cyber-attacks-shut-down-independent-news-website/.

[72] "Malaysiakini comes under DDOS attack," Malaysiakini, July 8, 2011, http://www.malaysiakini.com/news/169343.

Although the attacks have not been conclusively traced to the government, some observers believe they were either sponsored or condoned by Malaysian security agencies. Meanwhile, in June 2011, dozens of government websites were attacked shortly after the hacking group Anonymous threatened to target Malaysian government sites to protest media censorship and the blocking of file-sharing websites.[73]

[73] Kelly Goh & Austin Camoens, "Hacker group tells why it wants to attack Malaysian Govt portal," Star Online, June 14, 2011, http://thestar.com.my/news/story.asp?file=/2011/6/14/nation/20110614143743&sec=nation; "Hackers attack Malaysia government websites," BBC, June 16, 2011, http://www.bbc.co.uk/news/world-asia-pacific-13788817.

MEXICO

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	12	11
Limits on Content (0-35)	10	11
Violations of User Rights (0-40)	10	15
Total (0-100)	**32**	**37**

* 0=most free, 100=least free

POPULATION: 116 million
INTERNET PENETRATION 2011: 36 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/I USERS ARRESTED: No
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

In February 1989, the Monterrey Superior Studies Institute established Mexico's first internet connection.[1] Despite dramatic growth in internet penetration over the last 23 years, the majority of the population, particularly in rural areas, still lacks affordable access. This is largely due to infrastructural deficiencies and high prices resulting from ownership concentration in the telecommunications sector. On the other hand, mobile phones are widely available.

Once individuals are able to get online, the Mexican internet is predominantly free of censorship. While the blogosphere is not as influential as in other countries in the region, the social-networking site Facebook and the Twitter microblogging service have emerged as tools for citizen mobilization, including in response to drug-related violence and attacks on journalists. In 2011, for the first time, internet users became the target of such violence when four people were brutally killed in Nuevo Laredo between September and November, apparently in connection with their online writings. Separately, several new websites reporting critically about state governments have begun serving as important sources of information and forums for public discussion. However, as they gained prominence, the websites reported encountering harassment, discrimination, and cyberattacks that negatively affected their ability to operate.

[1] Network Information Center (NIC) Mexico, "History of NIC Mexico" [in Spanish], accessed November 16, 2011, http://www.nic.mx/es/NicMexico.Historia (site discontinued).

OBSTACLES TO ACCESS

Internet penetration in Mexico has notably increased in recent years, from approximately 20 percent of the population in 2006 to 36 percent by early 2012.[2] These figures remain low, however, for a country at Mexico's level of economic development and especially for a member of the Organization for Economic Cooperation and Development (OECD).[3] In addition, technological advancement has been uneven across the country, with a large percentage of users concentrated in Mexico City or other urban areas.[4] This digital divide is largely due to a lack of infrastructure as well as high prices. Thus, as of August 2011, only 21 percent of households had internet service,[5] and in May 2012, 54 percent of users reported accessing the web outside their home.[6] Nevertheless, cybercafes are generally easy to access in small cities, some small towns, and in areas frequented by tourists. No accurate statistics are available on the level of internet use among the indigenous population.

A lack of competition in the telecommunications sector has contributed to high prices and weakened incentives for the dominant companies to expand services to rural areas, leaving many parts of the country without connectivity. According to the National Institute of Geography and Statistics (INEGI), landline coverage in urban areas is only 50 percent, and in rural areas, this figure drops to 25 percent. As a result, broadband access is also limited. Although there are hundreds of independent internet service providers (ISPs) in Mexico,[7] the private company Teléfonos de México (Telmex) dominates the market for landlines and provides DSL broadband internet services for 8.7 million of the market's 10 million subscribers.[8]

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#. A study by AMIPCI based on interviews conducted in April-May 2012 supported this figure that there were 40.6 million users, about 35 percent of the population "Internet users in Mexico reach more than 40 million," [in Spanish] Mexican Internet Association (AMIPCI), May 17, 2012, http://www.amipci.org.mx/?P=articulo&Article=71.

[3] "Internet penetration in Mexico is still low" [in Spanish], Azteca Noticias, May 7, 2012, http://www.aztecanoticias.com.mx/notas/tecnologia/110807/penetracion-de-internet-en-mexico-es-baja-amipci.

[4] Of the 30.6 million users over the age of six, an estimated 25.6 million live in urban areas. Mexican Internet Association, *AMIPCI 2009 Report on Internet Users' Habits* [in Spanish], Mexican Internet Association (AMIPCI), May 2010, http://www.amipci.org.mx/estudios/temp/Estudiofinalversion1110-01989330012742874950B.pdf (site discontinued).

[5] "Internet penetration in Mexico" [in Spanish], Mexican Communication Magazine, March 29, 2011, http://mexicanadecomunicacion.com.mx/rmc/2011/08/18/la-penetracion-de-internet-en-mexico/#axzz1jqEkt6lM.

[6] Mexican Internet Association, *AMIPCI 2010 Report on Internet Users' Habits* [in Spanish], Mexican Internet Association (AMIPCI)

[7] James Thomasson, William Foster, and Laurence Press, *The Diffusion of the Internet in Mexico* (Austin: Latin American Network Information Center, University of Texas, 2002), http://lanic.utexas.edu/project/etext/mexico/thomasson/thomasson.pdf.

[8] Ibid.

Broadband subscriptions have enjoyed modest growth since 2009, increasing by 2.3 percent to reach 10.6 broadband subscribers per 100 inhabitants in 2011;[9] by comparison, the OECD average is 25.1.[10] There has been some reduction in the cost of a broadband connection, but it remains expensive for many Mexicans, ranging from 389 pesos (US$30) to 599 pesos (US$78) per month,[11] compared to the minimum monthly wage of 1,770 to 1,860 pesos (US$114 to US$126), depending on location.[12] Access from cybercafes is more affordable, ranging from 10 to 15 pesos (US$0.77 to US$1.15) per hour.

The Mexican government acknowledges the serious gaps in internet access and has shown willingness in recent years to address the problem. In April 2009, Congress approved a Law for the Development of an Information Society that explicitly recognizes the responsibility of the Mexican state to plan and promote access to information and communication technologies (ICTs).[13] In May 2010, the Department of Communications and Transportation announced an investment of 1.5 billion pesos (US$115.5 million) to extend internet access to neglected regions that private companies have deemed unprofitable.[14] The plan included efforts to create a national network of fiber-optic cables to connect outlying regions, and allow third parties to offer internet services.[15] However, three years later, achievements have been marginal, as evidenced by the statistics cited above.[16]

Six private companies provide most mobile phone services, though the Telmex subsidiary Telcel dominates with 70 percent market share.[17] Mobile phone access, according to the International Telecommunications Union (ITU), is significantly more widespread than internet use, with 94.6 million subscribers (82 percent of the population) as of the end of 2011.[18] The Competitive Intelligence Unit, a market research firm, estimates that the country will achieve 100 percent penetration in 2014.[19] A drop in prices for mobile phone

[9] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011.
[10] OECD Broadband Subscriptions data, June 2011.
[11] Ibid.
[12] "Minimum wage in Mexico" [in Spanish], Misalario.org, last modified February 20, 2012, http://www.misalario.org/main/tu-salario/salario-minimo/mexico-salarios-minimos.
[13] Special Committee of Congress for the Promotion of Digital Access to Mexicans, *Bill to Promote the Development of the Society of Information* [in Spanish], 2009, http://jmcane.files.wordpress.com/2009/04/ley-desarrollo-sociedad-de-la-informacion-mexico.pdf.
[14] "SCT Will Invest 1.5 Billion Pesos for the Internet" [in Spanish], El Universal, June 23, 2010, http://www.eluniversal.com.mx/notas/689775.html.
[15] James Thomasson, William Foster, and Laurence Press, *The Diffusion of the Internet in Mexico*.
[16] Karol Garcia, "Broadband," [in Spanish] Media Telecomm, May 2, 2012, http://www.mediatelecom.com.mx/index.php?option=com_content&view=article&id=21217&catid=9&Itemid=35.
[17] Henry Lancaster, "Mexico – Mobile Market Insights, Statistics and Forecasts," BuddeComm, last updated July 4, 2012, http://www.budde.com.au/Research/Mexico-Mobile-Market-Insights-Statistics-and-Forecasts.html.
[18] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[19] Ariadna Cruz, "Mobile lines still growing in Mexico" [in Spanish], El Universal, November 14, 2011, http://www.eluniversal.com.mx/finanzas/91029.html.

use has helped accelerate growth.[20] Perhaps the most notable change since 2011 has been the growth in the use of smartphones and with it, mobile internet access. By April 2012, industry insiders estimated that 17 million of the country's 97 million mobile phones were smartphones, or about 17.5 percent.[21]

Mexico's legal framework for telecommunications is complicated and outdated, as the main legislation on the topic was passed in the 1960s. In January 2012, the OECD published a report recommending quick legal and regulatory reforms in order to boost competition and investment in the sector.[22] The Federal Commission of Telecommunications (COFETEL) and the Federal Competition Commission (CFC), an antitrust body, are the primary agencies tasked with regulation.[23] Observers and press freedom advocates have criticized COFETEL for its lack of independence from the Department of Communications and Transportation and the executive branch. The president directly appoints COFETEL commissioners without the need for Senate approval, and the commission operates with limited transparency. These problems contribute to mistrust of its actions, especially regarding frequency allocations. The agency's credibility was further damaged with the 2010 appointment as director of Mony de Swaan Addati, perceived to be a political ally of the president and ruling party with little expertise in telecommunications.[24] After his appointment, de Swaan encountered conflicts with other commissioners and reports emerged of several contracts being awarded without a competitive bidding process.

The CFC has a better reputation, and its head commissioner has demonstrated the will to enforce antitrust legislation, but the institution remains weak and has limited power to enforce sanctions on large companies like Telmex. In June 2011, the commission imposed a 91 million peso (US$7.9 million) fine on Telmex for monopolistic practices after it denied a subsidiary of Telefonica (the second largest mobile phone service provider after Telmex) the ability to interconnect with its network in 2007-2008. In September, however, the commission revoked the fine after an appeal from Telmex and what some observers believed

[20] In May 2011, COFETEL ordered telecom firms to reduce interconnection fees between landlines and mobile phones to a more affordable level . The fees were dropped to 0.39 pesos (US$0.03) for mobile phones. The decision was later affirmed by the Supreme Court. "Cofetel reduces interconnection fees" [in Spanish], Revista Opcion, June 10, 2011, http://www.revistaopcion.com/tag/de-mayo/.

[21] Interview Guillermo Perezbolde, Vicepresident of Marketing, Public Relations and Social Media at Asociación Mexicana de Internet (AMIPCI).

[22] *OECD Review of Telecommunication Policy and Regulation in Mexico*, OECD, January 30, 2012, http://www.oecd.org/document/18/0,3746,en_2649_34223_49453202_1_1_1_1,00.html.

[23] COFETEL, "Scope of Action," [in Spanish] Federal Competition Commission, accessed August 31, 2010, http://www.cofetel.gob.mx/wb/Cofetel_2008/Cofe_ambito_de_accion.

[24] Organizacion Editorial Mexicana (Mexican Editorial Organization), "Por Correo Electronico El Valor de la Amistad" [By Email, The Value of Friendship], El Sol de Leon, February 10, 2012, http://www.oem.com.mx/elsoldeLEON/notas/n2422115.htm. ; "Biografia de Mony de Swaan" [Mony de Swaan Biography], Terra.com, June 30, 2010, http://economia.terra.com.mx/noticias/noticia.aspx?idNoticia=201006301612_TRM_79128653.

was political pressure.[25] There are no restrictions on opening cybercafes, though like other businesses they are required to obtain a license to operate.[26]

LIMITS ON CONTENT

The Mexican authorities do not employ any technical methods to filter or systematically curb access to online content, and no legislation restricts the internet as a medium for mass communication. This absence of regulation, even on content internationally recognized as harmful, is evident from Mexico's ranking as second worldwide in the production and distribution of child pornography.[27]

In previous years, isolated incidents were recorded of government agencies instigating the removal of online content in the public interest. However, in 2011 and early 2012, there were no reports of such deletion requests by the federal government. For example, according to Google's Transparency Report, the firm did not receive any requests for content removal from the Mexican authorities in 2011.[28]

More notable for its negative impact on the availability of online information to the public has been the rise in cyberattacks against independent online news sources. Beginning in mid-2011, a series of denial-of-service (DoS) attacks targeted political websites and online news outlets, shuttering them for days at a time or otherwise damaging their capacity to provide information to the public (see "Violations of User Rights").

In addition, as independent news websites covering state governments gained prominence, reports emerged of measures taken by some governors to neutralize their influence. In July 2011, Expediente Quintana Roo reported that four local government agencies had without explanation decided not to renew advertising contracts at a time when the recently elected government was showing growing hostility towards the year-old news website known for its investigative reporting and public opinion surveys.[29] In October 2011, E-consulta accused the governor of Puebla of using sympathetic news outlets to discredit the website after it

[25] The fine was suspended in August pending further examination, then revoked the following month. Notimex, "CFC backs up on fine imposed to Telmesx," [in Spanish], El Universal, August 4, 2011 http://www.eluniversal.com.mx/notas/783712.html.
[26] "Why an Internet Café Is Still Good Business in Mexico," InternetCafes.com.mx (blog), July 1, 2010, http://internetcafes.com.mx/2010/07/por-que-un-cafe-internet-aun-es-buen-negocio-en-mexico/ (subscription required).
[27] "Mexico, gran productor de pornografia infantile" [Mexico, a major producer of child pornography], Periodistasenlinear.org, http://www.periodistasenlinea.org/modules.php?op=modload&name=News&file=article&sid=4011; http://www.vanguardia.com.mx/unainfanciadesprotegidaporlaley-1277522.html, April, 2012.
[28] "Google Transparency Report July to December 2011," http://www.google.com/transparencyreport/removals/government/MX/?p=2011-12.
[29] "Ataque cibernetico en contra de tres medios digitales de Quintana Roo" [Cyber-attack against three Quintana Roo Digital Media], Instituto Prensa y Sociedad [Press and Society Institute], July 14, 2011, http://www.ipys.org/index.php?q=alerta/723.

leaked information indicating that the governor had distributed millions of dollars in advertising to such outlets,[30] while reports also emerged of efforts to discourage advertisements in E-consulta.[31]

Although self-censorship is extensive among traditional media journalists, particularly regarding police activity and drug trafficking, the phenomenon is less prevalent among online reporters, as the sphere is not well developed and physical attacks are less common. This dynamic began to change in 2011 with the brutal killing of several internet users who had used social media to expose information related to drug violence (see "Violations of User Rights"). The murders generated somewhat of a chilling effect on online speech, but primarily prompted reminders from the moderators of forums on drug violence that contributors protect their anonymity. The editor of a news website anticipated that online journalists may come under attack more often in the coming years as their influence grows.[32]

Due to scarce funding, including a lack of investor interest in internet advertising, it is difficult for individuals and nonprofit initiatives to establish sustainable online media projects. However, since early 2011, efforts to develop politically-oriented web portals have gained momentum and met with some success. For example, in Mexico City, the portals Animal Político, Sin Embargo, La Silla Rota, Gurú Político, and SDP Noticias have emerged as important venues for political discussions and analysis not typically available from the traditional press. As their influence has grown, so too has the traffic to their websites.[33] Visits to Animal Politico, for example, increased 300,000 to 700,000 within one year. Some news websites have focused on typically more marginal social issues, such as Subversiones, which receives about 6,000 visits per month.[34] Many civil society groups also have their own sites, and those that cannot afford a website use blogging platforms to publicize their activities. According to the World Association of Community Radio in Mexico, the internet has been a helpful tool for nongovernmental organizations operating in rural areas, and especially for female activists.[35] Some community radio stations, such as RadioAMLO have successfully migrated online after being shut down by the authorities

[30] "Acoso del gobernador de Puebla Rafael Moreno Valle contra e-consulta (Harassment by the Puebla governor Rafael Moreno Valle on e-consulta)," YouTube video, 4:48, posted by "videoeconsulta," October 24, 2011, http://www.youtube.com/watch?v=tbqGB24McG8.

[31] "La confrontación como política de comunicación en Puebla" [Confrontation over political communication in Puebla], Lado B, October 12, 2011, http://ladobe.com.mx/2011/10/la-confrontacion-como-politica-de-comunicacion/.

[32] "Acoso del gobernador de Puebla Rafael Moreno Valle contra e-consulta (Harassment by the Puebla governor Rafael Moreno Valle on e-consulta)," YouTube video; Interview with Daniel Moreno, editor of Animal Político, February 2012.

[33] Websites of these portals: www.animalpolitico.com, www.lasillarota.com, www.sinembargo.mx, www.sdpnoticias.com

[34] Subversiones website: www.agenciasubversiones.org.

[35] Interview with Laura Salas, advocacy coordinator for AMARC–México, October 2011.

because of Mexico's restrictive legal framework on such outlets.[36] Despite these changes, blogging remains relatively underdeveloped in Mexico. This is not due to deliberate government censorship, however, and the Mexican public generally has open access to the full range of national and international news sources.

Applications like Facebook, Twitter, the video-sharing site YouTube, and international blog-hosting services are freely available and growing in popularity. Facebook and Twitter have emerged as especially important tools for social and political mobilization, as well as for exchanging information about drug-related violence, thereby providing critical warnings to local communities about dangerous situations.[37] As of March 2012, Mexico was home to over 33 million Facebook users, the second largest contingent in Latin America after Brazil and fifth largest in the world.[38] Twitter also has a growing number of accounts, increasing from 146,000 in February 2010 to four million by February 2011.[39] Nevertheless, throughout 2011, online activism remained limited to a small community, as many of the most popular bloggers address personal topics rather than engaging in political or social commentary.[40] Some observers anticipated, however, that mobilization via online tools might gain momentum in the run-up to general elections in July 2012.

In addition to civil society uses of social media tools, most political parties have an online presence, with some candidates using Twitter or Facebook to communicate their platforms to voters.[41] In April 2011, President Felipe Calderon and several cabinet members announced they had opened Twitter accounts.[42] A review of the scale and nature of their activities indicates that most ministers are not particularly adept at using social media and that Twitter has typically served as a medium to communicate information and views to

[36] Julio Hernández López, "Cofetel Shuts Down Two Community Radio Stations" [in Spanish], La Jornada, October 4, 2007, http://www.jornada.unam.mx/2007/10/04/index.php?section=opinion&article=004o1pol.

[37] Damien Cave, "Mexico Turns to Twitter and Facebook for Information and Survival," New York Times, September 24, 2011, https://www.nytimes.com/2011/09/25/world/americas/mexico-turns-to-twitter-and-facebook-for-information-and-survival.html?_r=1; Miguel Castillo, "Mexico: Citizen Journalism in the Middle of Drug Trafficking Violence," Global Voices (blog), May 5, 2010, http://globalvoicesonline.org/2010/05/05/mexico-citizen-journalism-in-the-middle-of-drug-trafficking-violence/.

[38] "Mexico Facebook Statistics," SocialBakers, accessed March 9, 2012, http://www.socialbakers.com/facebook-statistics/mexico.

[39] "Twitter in Mexico, some numbers" [in Spanish], Webadictos.com, accessed February 14, 2011, http://www.webadictos.com.mx/2010/02/08/twitter-en-mexico-algunos-numeros/; Damien Cave, "Mexico Turns to Twitter and Facebook for Information and Survival," New York Times, September 24, 2011, https://www.nytimes.com/2011/09/25/world/americas/mexico-turns-to-twitter-and-facebook-for-information-and-survival.html?_r=1.

[40] Kaitlyn Wilkins, "Social Media in Mexico: 5 Things You Need to Know," Ogilvy Public Relations Worldwide, September 24, 2009, http://blog.ogilvypr.com/2009/09/social-media-in-mexico-5-things-you-need-to-know/.

[41] Octavio Islas, Amaia Arribas, and Erika Minera, "The Use of Web 2.0 Propaganda in Campaigns for Elected Office, State of Mexico, July 2009" [in Spanish], *Razon y Palabra* 14 no. 70, November 2009–January 2010, http://www.razonypalabra.org.mx/N/N70/Final_Argentina.pdf.

[42] Deborah Esch, "Mexico: Felipe Calderon's Cabinet on Twitter," Global Voices (blog), April 19, 2011, http://globalvoicesonline.org/2011/04/19/mexico-felipe-calderons-cabinet-on-twitter/.

citizens, rather than engage in interactive conversations.[43] One notable exception has been Labor Minister Javier Lozano, who had by far the largest number of tweets and used a more engaging, relaxed tone in his communications. In a more disturbing trend, drug cartels have also begun using social media applications to exchange information on military checkpoints, prompting calls by some Mexican politicians for increased government monitoring and regulation of these tools.[44]

VIOLATIONS OF USER RIGHTS

The constitution guarantees freedom of speech and freedom of the press, as well as the privacy of personal communications. The federal criminal defamation law was repealed in 2007, but civil insult laws remain on the books and criminal defamation statutes exist in 15 of Mexico's 32 states.[45] Although the upper echelons of the judiciary are independent, rule of law protections are relatively weaker at state levels.

With online tools becoming crucial sources of public information on drug-related violence, controversy has emerged when local authorities have sought to punish false reports that cause public alarm. For example, in Veracruz, amidst a surge in violence in August 2011, two users posted unconfirmed reports to Twitter of an attack on a school, sparking panic among parents.[46] Local authorities arrested the pair, a schoolteacher and journalist, on charges of terrorism and sabotage, which can yield punishments of up to 30 years in prison. A public outcry ensued over due process shortcomings and the disproportionate charges for citizens who may have been negligent in publishing unconfirmed reports but demonstrated no malicious intent.[47] The prosecutor's office subsequently dropped the charges in September and the two were released. That month, the state congress also amended the criminal code such that creating a "public order disturbance," would be punishable by one to

[43] Felipe Coredero, "Mexico: President Felipe Calderon's Twitter Use," Global Voices (blog), May 19, 2011, http://globalvoicesonline.org/2011/05/19/225272/; Claudia Benassini, "Calderon's cabinet on Twitter" [in Spanish], *Razón y palabra*, April 2012, http://www.razonypalabra.org.mx/caja_pandora/gabinete.html.

[44] Alexis Okeowo, "To Battle Cartels, Mexico Weighs Twitter Crackdown," Time, April 14, 2010, http://www.time.com/time/world/article/0,8599,1981607,00.html/r:t#ixzz0laM8OTIa.

[45] Freedom House, "Mexico," *Freedom in the World 2012*, http://www.freedomhouse.org/sites/default/files/Mexico%20draft.pdf.

[46] Daniel Hernandez, "Terrorism charges for 2 in Mexico who spread attack rumor on Twitter, Facebook," LA Times (blog), September 1, 2011, http://latimesblogs.latimes.com/laplaza/2011/09/twitter-tweets-veracruz-mexico-terrorism-drug-war-censorship-rumors.html.

[47] Local media reported that the pair was subject to psychological pressure to plead guilty and according to Amnesty International, denied access to a lawyer for 60 hours. Javier Duarte Ochoa, "Personas en riesgo de prision en Mexico tras publicaciones en Twitter y Facebook" [in Spanish], Amnesty International, August 31, 2011, http://amnistia.org.mx/nuevo/2011/09/01/personas-en-riesgo-de-prision-en-mexico-tras-publicaciones-en-twitter-y-facebook/.

four years in prison and a fine equivalent to 1,000 days of wages.[48] Similarly, in late August 2011, the state of Tabasco's congress approved a law punishing false alarms spread via mobile phones or social media that provoke panic or require mobilization of emergency personnel with between six months and two years in prison.[49] Local lawyers raised concerns that the new provision could be used to unnecessarily restrict freedom of expression.

The Mexican constitution has strong privacy protections, including requiring a judicial warrant for any interception of personal communications. In 2010, a new law on data protection was adopted that expanded the oversight powers of the data protection authority.[50] Nonetheless, amidst efforts to curb drug-related violence, Mexican security agencies have sought to improve their surveillance capabilities. In 2007, the Federal Investigations Agency reportedly began acquiring equipment with high technical sophistication from the Israeli firm Verint with the assistance of the United States government. The contract called for a system capable of intercepting mobile and landline phone calls, email communications, VoIP services, and internet chat programs.[51] In April 2012, a second procurement was announced, aimed at increasing the number of work stations from 30 to 107.[52] Human rights and privacy advocates have acknowledged the need for law enforcement agencies to improve their capacity to fight drug cartels and protect the public given rising violence levels. However, they have also raised concerns that corruption and weak rule of law among some state governments—including the infiltration of law enforcement agencies by organized crime—leave much room for abuse and that citizens could be endangered should their private communications fall into the wrong hands. Such concerns were heightened with the passage of a Geolocalization Law that came into effect in April 2012. The legislation enables law enforcement agencies, including potentially low-level public servants, to gain access without a warrant and in real time to the location data of mobile phone users.[53] Critics of the law warned that it set a worrisome precedent of warrantless surveillance and was unconstitutional.[54] They also claimed location data was easy

[48] "After wasted month in prison, two social network users freed, charges dropped," Reporters Without Borders, September 22, 2011, http://en.rsf.org/mexico-two-social-network-users-held-on-02-09-2011,40907.html.
[49] H. Congreso del Estado de Tabasco, *Constitution of the State of Tabasco* [in Spanish], http://www.congresotabasco.gob.mx/60legislatura/trabajo_legislativo/pdfs/decretos/Decreto%20125.pdf; Leobardo Perez Marin, "Apreuban Ley contra 'rumor'; coartara libertades" [in Spanish], Tabasco Hoy, August 31, 2011, http://www.tabascohoy.com/noticia.php?id_nota=220149.
[50] Jeremy Mittman, "Mexico Passes Sweeping New Law on Data Protection," Proskauer Rose LLP, May 11, 2010, http://privacylaw.proskauer.com/2010/05/articles/international/mexico-passes-sweeping-new-law-on-data-protection/.
[51] Bob Brewin, "State Department to Provide Mexican Security Agency with Surveillance Apparatus," NextGov, April 30, 2012, http://www.nextgov.com/technology-news/2012/04/state-department-provide-mexican-security-agency-surveillance-apparatus/55490/.
[52] Ibid.
[53] Katitza Rodriguez, "Mexico Adopts Alarming Surveillance Legislation," Global Voices (blog), March 2, 2012, http://advocacy.globalvoicesonline.org/2012/03/02/mexico-adopts-alarming-surveillance-legislation/.
[54] Cyrus Farivar, "Mexican 'Geolocalization Law' draws ire of privacy activists," ArsTechnica, April 24, 2012, http://arstechnica.com/tech-policy/2012/04/mexican-geolocalization-law-draws-ire-of-privacy-activists/.

for savvy criminal elements to hide, while the law could potentially endanger ordinary citizens.[55]

A 2008 law mandated that mobile phone companies keep a registry of users, communications, and text messages for use by law enforcement agencies in combating extortion and kidnappings.[56] Critics expressed doubt that the authorities would securely store the information to protect users' privacy, especially given past failures by the state to safeguard such data.[57] Nevertheless, 70 percent of users complied with the registration requirement, partly due to threats that their line would be cancelled if they did not. In 2012, the above mentioned Geolocalization Law revoked the registration requirement and the federal data protection agency subsequently ordered the registry destroyed.[58] According to some reports, however, copies had already been put up for sale on the black market, confirming earlier fears regarding weak data protection.[59]

Mexico continues to be one of the most dangerous countries in the world for journalists, who are mostly targeted by individuals linked to drug cartels for probing trafficking, corruption, and police issues. This phenomenon has been exacerbated by widespread impunity for those carrying out such attacks.[60] In 2011, for the first time, individuals who had circulated information online on the above issues were also the victims of brutal murders. Specifically, four people were killed between September and November 2011 in the city of Nuevo Laredo, all of their bodies accompanied by notes from their killers linking their murders to online reporting about local organized crime and gangs. The first victims were a man and woman whose bodies bearing signs of torture were hung from an overpass in the city alongside a message warning of retribution for those who contribute to websites that expose organized crime activities, as the two victims had on the popular online forum Frontera Al Rojo Vivo.[61] The next victim was Maria Elisabeth Macias, a journalist and blogger, whose beheaded body was found on October 27 accompanied by a similarly

[55] Lisa M. Brownlee, Esq., "Memo to Privacy Commissioners," April 24, 2012, http://static.arstechnica.net/2012/04/24/brownlee.mexico.geoloc.pdf.

[56] "In Mexico, All Telephone Conversations Will Be Recorded and Stored for One Year," [in Spanish] Babel Del Norte, December 16, 2008, http://www.babeldelnorte.com/index.php?view=article&catid=39%3Acultura&id=719%3Aen-mexico-todas-las-conversaciones-telefonicas-seran-grabadas-y-se-guardaran-por-un-ano.

[57] Miguel Castillo, "Mexico: Fear and Intimidation in Electronic Media," Global Voices (blog), May 12, 2010, http://globalvoicesonline.org/2010/05/12/mexico-fear-and-intimidation-in-electronic-media/.

[58] Nicole Toderas, "IFAI ordena destruir los datos recavados por el RENAUT" [IFAI ordered to destroy the data obtained by RENAUT], PoderPDA, March 3, 2012, www.poderpda.com/uso-smartphones/ifai-ordena-destriur-los-datos-recavados-por-el-renaut/.

[59] Lisa M. Brownlee, Esq., "Memo to Privacy Commissioners," April 24, 2012; "The Geolocalization law came into effect in Mexico and the RENAUT dies" [in Spanish], PoderPDA, April 24, 2012, http://www.poderpda.com/uso-smartphones/entra-en-vigor-en-mexico-la-ley-de-geolocalizacion-y-muere-el-renaut/.

[60] Committee to Protect Journalists, "27 Journalists Killed in Mexico since 1992/Motive Confirmed," accessed September 18, 2012, https://www.cpj.org/killed/americas/mexico/.

[61] Chris Taylor, "Mexican Blog Wars: Couple Hanged for Denouncing Cartel Online," Mashable, September 14, 2011, http://mashable.com/2011/09/14/mexican-blog-wars/.

threatening message linking her death to online writings on the popular website Nuevo Laredo en Vivo and signed "Z" for Zetas, a cartel active in the area. The body of the fourth victim was found on November 9 with a note reading, "This happened to me for not understanding that I shouldn't report things on social networks," and again naming Nuevo Laredo en Vivo, though it remained unclear whether he had actually contributed to the website.[62] Although the precise perpetrators remain unknown, the circumstances of the killings pointed to drug cartels being involved. Website moderators responded by reminding contributors to adhere to rules regarding anonymity when denouncing cartel activities, while urging them not to be intimidated into silence.[63]

Since mid-2011, cyberattacks have emerged as a new threat to online news websites in Mexico. In July 2011, the free expression group Article 19 reported that three online news outlets—Expediente Quintana Roo, Noticaribe and Cuarto Poder—had been temporarily forced offline by cyberattacks, and that some also had personal information and reporters' notes stolen from their servers.[64] The sites are known for the critical coverage of the state government of Quintana Roo. In November 2011, the weekly Riodoce was informed by its hosting provider that the website had been the target of a large distributed denial-of-service (DDoS) attack and that the provider was therefore unable to continue to offer server capacity. As a result, the publication's website was unavailable for several days. Although the source of the attack was unclear, it was widely suspected to be a reprisal for the publication's reporting, as it is one of the few media outlets in Mexico to report aggressively on crime and drug trafficking, and has been the target of offline attacks.[65] Sporadic cyberattacks continued to be reported in early 2012. Some targeted the above mentioned outlets for a second time, while others paralyzed previously unaffected websites.[66]

[62] Robert Beckhusen, "Mexican Man Decapitated in Cartel Warning to Social Media," Wired, November 9, 2011, http://www.wired.com/dangerroom/2011/11/mexican-blogger-decapitated/.
[63] Sarah Kessler, "Mexican Blog Wars: Fourth Blogger Murdered for Reporting on Cartel," Mashable, November 10, 2011, http://mashable.com/2011/11/10/mexico-blogger/.
[64] Monica Medel, "Three news websites hacked in Mexico," Knight Center for Journalism in the Americas, July 15, 2011, https://knightcenter.utexas.edu/blog/three-news-websites-hacked-mexico.
[65] International Freedom of Expression eXchange (IFEX), "Weekly goes offline after cyber attack," news release, November 28, 2011, http://ifex.org/mexico/2011/11/30/riodoce_cyberattack/.
[66] Tania Lara, "Mexican digital newspaper disabled by frequent cyberattacks," Knight Center for Journalism in the Americas, April 20, 2012, http://knightcenter.utexas.edu/blog/00-9806-mexican-digital-newspaper-disabled-frequent-cyberattacks.

NIGERIA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	13	12
Limits on Content (0-35)	10	9
Violations of User Rights (0-40)	12	12
Total (0-100)	**35**	**33**

* 0=most free, 100=least free

POPULATION: 170 million
INTERNET PENETRATION 2011: 28 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Nigeria saw marked progress in its information and communications technology (ICT) sector in 2011 with the pronounced use of ICTs during the April 2011 elections and the mid-year announcement of a new communication technology ministry (also known as the ICT ministry). Since 1999, when Nigeria returned to civilian governance after almost 30 years of military rule,[1] press freedom and the space for free expression have increased significantly. Nevertheless, the legal and political environment for traditional media remains harsh, and a major story in 2011 was the death of a journalist for which a radical Islamic sect, Boko Haram, claimed responsibility.

Online media has been comparatively free from such restrictions, though a blogger was detained for questioning in January 2011. The Nigerian authorities do not carry out any filtering of content, and while access to information technology is still limited for many Nigerians, the number of internet users nearly quadrupled between 2008 and 2011. Legislative initiatives introduced in the National Assembly in 2007, which threatened to impinge upon the relative freedom and privacy enjoyed by online journalists, expired when the newly-elected National Assembly convened in June 2011.

The internet was first introduced in the early 1990s, and usage grew more popular following an internet workshop organized by the Yaba College of Technology in 1995.[2] Internet access

[1] Abegunrin Olayiwola, *Nigerian Foreign Policy Under Military Rule, 1966–1999* (Westport, CT: Praeger, 2003).
[2] The workshop was hosted by the Yaba College of Technology in Lagos in collaboration with the Nigerian Communications Commission, the National Data Bank, the Literacy Training and Development Program for Africa (University of Ibadan), the

expanded when cybercafes sprang up in major cities across Nigeria in 1999, though it was expensive and connections were very slow. The introduction of internet access via mobile phone service in 2004 has spurred further increases in internet use.

OBSTACLES TO ACCESS

Internet access in Nigeria has grown exponentially in recent years, particularly after the introduction of mobile phone data services and Fixed Wireless Access (FWA) services. There were about 100,000 internet users in 1999,[3] but the figure grew exponentially to 11 million in 2008[4] and reached 46 million in 2011.[5] This large jump in access is due to an increase in mobile phone usage and data services, private sector and government investment in technology, and increased competition between FWA providers over this period. Nevertheless, internet penetration stood at 28.4 percent in 2011 according to the International Telecommunications Union (ITU),[6] and access is greater in urban areas than in rural regions.

Increased competition has decreased the cost of access for many Nigerians, and while the price for internet use remains about US$1 per hour in cybercafes, which have seen sharp decline in patronage in recent years due to increasing mobile internet usage enabled by decreasing costs of data plans. The average cost is now US$1 per megabyte of data on Global System for Mobile (GSM) networks, compared to US$7 in 2010. FWA services now cost an average of US$65 per month, down from US$80 in 2010. In comparison, the minimum wage in Nigeria is about US$116 per month, and the country's poverty rate actually increased in 2011.[7] Literacy remains an obstacle to access, with 28 percent of the population illiterate, particularly in English, the main language used by Nigerian online news outlets and blogs.[8]

Administrative Staff College of Nigeria (ASCON), the United States Information Service (USIS), the Regional Information Network for Africa (RINAF), and the British Council. United Nations Economic Commission for Africa, "Nigeria: Internet Connectivity," http://www.uneca.org/aisi/nici/country_profiles/Nigeria/nigeriainter.htm, accessed August 27, 2010.

[3] Ibid.

[4] "Nigeria Internet Users Tops 11 Million, Penetration Now 7.8%," Web Trends Nigeria (blog), October 8, 2009, http://webtrendsng.com/blog/nigeria-internet-users-tops-11-million-penetration-now-7-8/.

[5] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[6] Ibid.

[7] Paul Okolo, "Nigeria's Poverty Ratio Rises to 70% of Population, Trust Says," Bloomberg, January 18, 2011, http://www.bloomberg.com/news/2011-01-18/nigeria-s-poverty-ratio-rises-to-70-of-population-trust-says.html.

[8] "At a Glance: Nigeria—Statistics," United Nations Children's Fund (UNICEF), last modified March 2, 2010, accessed June 29, 2012, http://www.unicef.org/infobycountry/nigeria_statistics.html.

Frequent power cuts remain an impediment to internet access, with many users reportedly relying more than ever on private generators to stay online during outages. In January 2011, a report quoted Nigeria as the largest importer of private power generators in Africa, despite the country's status as an oil-rich country.[9] Cybercafes continue to close due to difficulties paying for such expensive backup power generation in addition to the growing popularity of access via mobile devices and data plans offered by FWA and GSM companies. Although many providers use the word "broadband" in their promotional materials, in practice there is limited broadband service available in Nigeria, with latest statistics from the ITU placing the number of broadband subscribers at only 215,000 in 2011, amounting to a penetration rate of just 0.13 percent.[10]

The number of mobile phone subscribers has increased dramatically over the past decade from almost no users in 2000 to over 100 million as of May 2012, according to official data from the Nigerian Communications Commission (NCC).[11] The latest ITU data notes over 95 million mobile phone subscriptions in 2011, amounting to a mobile phone penetration rate of 58.6 percent.[12] Mobile internet subscriptions reached 7.3 million users by 2008[13] and grew by over 25 percent between October 2010 and October 2011.[14] While smart phone users can access the internet on their mobile devices, specific handsets such as Nokia's range of phones and Research in Motion's BlackBerry provide bundled data services to mobile subscribers. The number of BlackBerry users appears to be growing, particularly among young Nigerians, though the service costs US$20 per month. Nevertheless, the quality of service remains poor, with users frequently complaining about their inability to enjoy data services. Competition has forced service providers to offer alternative plans based on time (daily, weekly, or monthly payments) or use (social or messaging). According to credible sources in the industry, there were approximately 500,000 BlackBerry subscribers with all service providers as of October 2011.[15]

In March 2007, the government established the Nigerian Internet Exchange Point as a means of connecting internet service providers (ISPs) to one another; as of mid-2011, it had 32

[9] Clara Nwachukwu, "Nigeria maintains lead in generator imports in Africa…," Vanguard Newspaper, January 10, 2011, http://www.vanguardngr.com/2011/01/nigeria-maintains-lead-in-generator-imports-in-africa-%E2%80%A6/.
[10] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[11] "Subscriber Data – Monthly Subscriber Data," Nigerian Communications Commission, accessed June 29, 2012, http://www.ncc.gov.ng/industry-statistics/subscriber-data.html.
[12] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[13] Charlie Fripp, "Mobile Internet Usage Soars in Nigeria," IT News Africa, December 4, 2008, http://www.itnewsafrica.com/?p=1906.
[14] Jayne Augoye, "Why More Internet Users Prefer Mobile Browsers to Desktop," Nigerian Best Forum, November 10, 2011, http://www.nigerianbestforum.com/generaltopics/?p=108283.
[15] Interview with a service provider who requested anonymity, August 2010.

members.[16] Several telecommunications companies have also migrated to private fiber-optic cable projects, such as Glo-1 and MainOne. The latter cable went live on July 1, 2010 and now provides connectivity for 18 ISPs and telecommunication companies in Nigeria and Ghana,[17] though the reduced cost of a cable rather than a satellite connection has yet to be passed on to consumers. The Glo-1 cable, a project of Globacom, launched in Ghana in April 2011.[18]

The video-sharing website YouTube, social-networking site Facebook, microblogging application Twitter, and various international blog-hosting services are freely available and among the most popular websites in the country. As of May 2012, there were over five million Facebook users.[19] According to Alexa, a website rating company, the ten most popular websites in Nigeria as of 2011 were Facebook, Google, Yahoo, Google.com.ng, YouTube, Blogspot.com, Twitter, Vanguard Newspaper, Wikipedia, and Nairaland (a Nigerian online discussion forum).[20] Four other Nigerian websites—VConnect (a local search engine with a huge database of relevant locations) at number 13, GTBank at number 14, Punch newspaper at number 16, and Jobberman (a job search portal) at number 20—were cited in the top 20.

The ICT market in Nigeria has expanded significantly over the past decade. The number of licensed ISPs has risen from 18 in 2000 to 136 (with 35 holding licenses that need renewal) as of mid-2011,[21] in addition to 11 active FWA providers[22] and four GSM mobile phone operators that also provide internet access to their subscribers.[23] Nigeria had more licensed ISPs and active FWA providers in 2010, but unlike the growth recorded by GSM operators, ISPs and FWA providers have not had as much success, as more people now access the internet through mobile (GSM) phones. As of June 2011, the four GSM companies had a total of 84 million subscribers between them: MTN had 40.5 million, compared to Globacom's 19.5 million, Airtel's 16 million, and Etisalat's 7.8 million.[24] All of the above companies are privately-owned.

[16] "Our Members," Internet Exchange Point of Nigeria, accessed December 13, 2011, http://www.nixp.net/index.php?option=com_content&view=article&id=13&Itemid=13.
[17] "Our Clients," Main One Cable Company, accessed December 23, 2011, http://www.mainonecable.com/our-clients.
[18] "Glo 1 Cable Launches in Ghana," AfricanBrains, April 15, 2011, http://www.africanbrains.net/2011/04/15/glo-1-cable-launches-in-ghana/.
[19] "Nigeria Facebook Statistics," Socialbakers, accessed June 29, 2012, http://www.socialbakers.com/facebook-statistics/nigeria.
[20] "Top Sites in Nigeria," Alexa Web Information, accessed December 4, 2011, http://www.alexa.com/topsites/countries/NG.
[21] "Internet Services," Nigerian Communications Commission, accessed December 31, 2011, http://ncc.gov.ng/component/docman/doc_download/11-internet-services.html.
[22] "Fixed Wireless Access," Nigerian Communications Commission, accessed December 31, 2011, http://ncc.gov.ng/component/docman/doc_download/4-fixed-wireless-access-fwa.html.
[23] "Digital Mobile License," Nigerian Communications Commission, accessed December 31, 2011, http://ncc.gov.ng/component/docman/doc_download/2-digital-mobile-licence-gsm-.html.
[24] "Fixed Wireless Access," Nigerian Communications Commission, accessed December 18, 2011.

The only government-owned firm in the market, NITEL, is now inactive, with only 58,750 land lines and 258,520 mobile lines. It has remained on the government's privatization list for several years following multiple attempts to sell it. In February 2009, Transcorp, a local conglomerate with strong ties to the government, relinquished its 51 percent stake, which it had acquired in 2006.[25] In February 2010, New Generation Telecoms, a consortium that includes China Unicom, won a controversial bid to purchase the company.[26] Responding to allegations of corruption surrounding the purchase, the president initiated an investigation,[27] but the findings have not yet been published. As at the end of 2011, NITEL remained on the government's list of to-be-sold companies.

Internet services are governed by the Nigerian Telecommunications Act, which vests regulatory responsibilities in the Nigerian Communications Commission (NCC). All ISPs must obtain a license from the NCC to operate, but there have been no reports of any ISP being denied a license or registration renewal. However, new ISPs seeking to enter the market have faced challenges in their operations due to competition from larger ISPs and investor focus on the mobile sector. Although the NCC's nine-member board is nominated by the government, the regulator's decisions are viewed as relatively independent.

LIMITS ON CONTENT

There have been no reports of the Nigerian government engaging in any form of internet filtering.[28] According to the most recent study by the OpenNet Initiative (ONI), several websites were inaccessible surrounding the elections in 2007; however, the ONI researchers concluded that the disruptions were due to technical problems, not government intervention.[29] On May 29, 2011, there were reports by residents of the capital city, Abuja, that telecommunication services were inaccessible in certain areas. While the incident was not confirmed or reported by the mainstream media, various blogs covered the story, with one blogger reporting quotes from NCC representatives and the Visaphone service provider that confirmed the security reasons behind the isolated telecom shutdown.[30] Nevertheless,

[25] "NITEL Board Ratifies Appointment of Chairman: About NITEL," Transcorp, September 24, 2008, http://www.transcorpnigeria.com/corporatecom/archives.php?page=fullstory&nid=60; Betrand Nwankwo and Juliet Alohan, "Nigeria: Transcorp Relinquishes 51 Percent Equity Share in Nitel/Mtel," *Leadership*, February 26, 2009, http://allafrica.com/stories/200902260498.html.

[26] Camillus Eboh, "New Generation Telecoms Acquires NITEL," Reuters, February 16, 2010, http://234next.com/csp/cms/sites/Next/Home/5527697-146/new_generation_telecoms_acquires_nitel_.csp.

[27] Camillus Eboh, "Nigeria Cabinet Sacking Delays Nitel sale," Reuters, March 19, 2010, http://www.reuters.com/article/idUSLDE62I0WS20100319.

[28] OpenNet Initiative, "Internet Filtering in Nigeria," October 1, 2009, http://opennet.net/research/profiles/nigeria.

[29] OpenNet Initiative, "Internet Watch Report: The 2007 Presidential Elections in Nigeria," November 2007, http://opennet.net/research/bulletins/014.

[30] Charlie Fripp, "Nigerians angry over Abuja telecom shutdown," IT News Africa, May 31, 2011, http://www.itnewsafrica.com/2011/05/nigeria-angry-over-abuja-mobile-shutdown.

the complex nature of Nigeria's internet framework as described above makes it difficult to carry out systematic filtering or censorship. Some ISPs have been known to block access when users infringe on laws by downloading copyrighted content, but this has often been done to manage network traffic rather than protect intellectual property.

In June 2009, reports emerged that the Nigerian government planned to invest in sponsoring pro-government websites and blogs.[31] In practice, it has not been possible to confirm whether the plan has been implemented. Websites, blogs, and commentators are generally divided among anti-government, pro-government, and neutral leanings, and this continued as online political discussions increased in advance of the parliamentary and presidential elections in April 2011. Web commentary appeared to tilt in favor of anti-government leanings in January 2012 during the protests that became known as the Occupy Nigeria protests, but there has been a more balanced set of discussions since then, with many online commentators moving the conversation away from pro- and anti- leanings towards socioeconomic debates.

The April 2011 elections also saw heavy use of social media in discussions concerning the elections, campaigns, and citizen participation. A youth-led group, Enough is Enough Nigeria,[32] launched the Register-Select-Vote-Protect (RSVP) project that relied heavily on the use of social media to mobilize citizens for voter registration and disseminate information on competing candidates, actual voting drives, and election monitoring. The group also launched the mobile application, ReVoDa, which enabled citizens to monitor elections from their respective polling locations on their mobile phones.

Nigeria is home to a diverse blogosphere, with entertainment blogs drawing the most readers and a growing number of Nigerians blogging about their personal lives or social activism issues. Blogs have gradually emerged as an important platform for discussion and a source of reliable news for many users. Readers often leave comments on popular news-oriented blogs to express their frustration with societal ills. The Facebook page of the president has also become a major avenue through which citizens comment on public issues. At the height of the increasing security tensions in the country in January 2012, various comments on the president's Facebook page went as far as accusing the president of incompetence.

[31] Sokari Ekine, "Nigeria government launches attack against bloggers," Global Voices, June 25, 2009, http://advocacy.globalvoicesonline.org/2009/06/25/nigeria-government-launches-attack-against-bloggers/; "Umaru Yar'adua Regime Launches $5 Million Online War," Sahara Reporters, June 16, 2009, http://www.saharareporters.com/news-page/umaru-yar%E2%80%99adua-regime-launches-5-million-online-war.

[32] The report author is a founding member of the EnoughisEnough Nigeria group (http://www.eienigeria.org).

The Nigerian blogosphere includes both Nigerians living abroad and locally-based writers. While many of the former are longtime bloggers, only in the past six years have Nigerian residents actively joined the blogosphere,[33] with local blogging gaining momentum following a Nigerian bloggers' conference in 2008.[34] Although two attempts to create Nigerian blog aggregators have failed,[35] GlobalVoicesOnline.org, Blogger.com, Afrigator.com, and WordPress.com are popular platforms on which Nigerian bloggers interact and learn from one another. ICTs have also played an important role in mobilizing people for real life protests and providing updates on unfolding events. In November 2008, a widely circulated YouTube video showed an admiral and several other military officers severely beating a woman whom they deemed too slow in making way for their convoy.[36] Following public outcry, the woman received legal aid from the state government and sued the officers for assault and battery. In January 2010, a court awarded her 100 million naira (approximately US$613,000) in compensation.[37]

Online citizen activism in Nigeria was particularly evident during the 2011 elections, with social media enhancing the flow of information for mobilization and reporting. According to one report,[38] social media changed how information was disseminated, and "citizens accessed information directly and more accurately, resulting in unsurpassed participation in politics during the 2011 elections."[39] In January 2012, following an announcement of fuel pump price increases, protests were staged across Nigeria with the help of information disseminated on social media networks. The protests came to be known as Occupy Nigeria and were also covered by citizens using social media applications.[40]

[33] Remmy Nweke, "Nigeria: Blogging as a Trend in Nigeria," *Daily Champion*, January 12, 2006, http://allafrica.com/stories/200601120144.html.
[34] Gbenga Sesan, "The Nigerian Bloggers' Forum," *Oro* (blog), September 22, 2005, http://www.gbengasesan.com/blog/?p=10.
[35] The Nigerian Blog Aggregator is available at http://www.nigerianbloggers.com and the Nigerian Weblog Ring at http://nwr.cowblock.net.
[36] "Brutalization of Uzoma Okere," YouTube, November 10, 2008, 1 min., 40 sec., http://www.youtube.com/watch?v=VHdkyvn41us.
[37] "Uzoma Okere Won N 100 Million," *Nigerian Curiosity* (blog), January 29, 2010, http://www.nigeriancuriosity.com/2010/01/uzoma-okere-won-n100-mn-video.html.
[38] Judith Asuni and Jacqueline Farris, "Tracking Social Media: The Social Media Tracking Center and the 2011 Nigerian Elections," Shehu Musa Yar'Adua Foundation, 2011, accessed March 31, 2012, http://www.cfr.org/content/publications/attachments/Tracking-Social-Media-COMPLETE-final.pdf.
[39] Ibid., pg. 18.
[40] Peter Vlam, "Social media inspires Nigerian protests," Radio Netherlands, January 12, 2012, http://www.rnw.nl/africa/article/social-media-inspires-nigerian-protests.

VIOLATIONS OF USER RIGHTS

Nigeria's legal framework has not been revised to reflect the use of new media technologies.[41] This lack of internet-specific legislation has generally fostered an open environment for online activities. Much of the public accepts the need for some regulation of internet use in light of the unchecked cybercrime in the country and the costs it has imposed on Nigeria's economy and global reputation.

At the commencement of the newly-elected National Assembly in June 2011, several proposed bills that could be used to restrict users' rights expired, and many of them have yet to be reintroduced on the assembly floor. In November 2011, the office of the National Security Adviser and other government departments drafted the Cybersecurity Bill, a revised version of the earlier Cyber Security and Information Protection Agency Bill, which had provisions that could restrict users' rights to free expression and privacy because it suggested that security officials could apprehend and prosecute users based on suspicion and without a court order. Taking into account feedback from citizens and stakeholders in the Nigerian ICT sector, the revised version reduced the powers granted to security officers by requiring a court order for the seizure of any equipment and for arrests based on suspicion.

While the 1999 constitution guarantees freedom of expression and of the press, the state often uses arbitrary and extralegal measures to suppress political criticism in the traditional media, and there is a culture of impunity for crimes against media workers. Libel remains a criminal offense, with the burden of proof resting on the defendant. Journalists covering sensitive issues such as official corruption, the president's health, and communal violence are regularly subjected to criminal prosecution. However, no such cases have yet been brought for online expression.[42] The implementation of Sharia (Islamic law) penal codes in 12 northern states has generally not affected internet freedom. However, in March 2010, a Sharia judge in Kaduna state banned efforts by the Civil Rights Congress of Nigeria to initiate online discussion of an amputation sentence on Facebook and Twitter.[43]

[41] For example, the Evidence Act does not provide for the acceptance of digital evidence in court, although an appellate court in Lagos ruled in May 2010 that computer-generated bank statements could be admitted in the graft trial of a former minister. See, Patience Akpuru, "Nigeria: Fani-Kayode Appeal Court Admits Computer Print-Out," *Daily Champion*, May 28, 2010, http://allafrica.com/stories/201005310338.html.

[42] Karin Karlekar, ed., "Nigeria," in *Freedom of the Press 2009* (New York: Freedom House, 2009), http://www.freedomhouse.org/inc/content/pubs/pfs/inc_country_detail.cfm?country=7675&year=2009&pf.

[43] The case centered on Buba Bello Jangebe, whose hand was amputated in 2000 as punishment for stealing a cow. See, Imam Imam, "Nigeria: Sharia Judge Bans Amputation Discussion on Facebook, Twitter," *This Day*, March 24, 2010, http://allafrica.com/stories/201003240460.html; "Civil Right Congress—Nigeria," Facebook page, accessed March 31, 2012, http://www.facebook.com/group.php?gid=372845616580; Shehu Sani, "CRC Condemns the Amputation of Buba on March 22, 2000," Twitter post, March 30, 2010, http://www.twitter.com/shehusani.

Cybercafes do not require customers to register or present any form of identification to go online, and any monitoring software installed on their computers is used only for billing purposes. In June 2009, drawing on the 2003 Nigerian Communications Act, the NCC announced that mobile phone companies would be expected to register all SIM cards by March 1, 2010 (later postponed to September 28, 2011).[44] After the cut-off date, the telecom regulator denied news reports that it had extended the registration deadline,[45] but it allowed the exercise to continue until the completion of the reconciliation exercise for data submitted by telecom service providers. Though the telecom regulator has complained that the exercise has suffered delays because of how telecom companies have managed decentralized registration, users could still register their SIM cards as of March 31, 2012.

Nigerian security services do not appear to proactively monitor internet and mobile phone communications, but many online journalists suspect that they are being monitored by the state. Due to the increase in activities considered acts of terrorism, the Nigerian government announced in November 2011 its intention to acquire "state of the art" security equipment to combat terrorism.[46] As of December 2011, not much has been heard of the project, but suspicions of state monitoring have increased since then, mostly because of the increased use of social media channels by government representatives. At least three government ministers have hosted Twitter chats between January 2011 and March 31, 2012.[47]

The Nigerian authorities have a history of arresting and intimidating traditional media workers, and at least eight journalists have been killed in connection with their work since 1998.[48] Although no individuals have been sentenced to prison or physically attacked for online activities as of April 2012, security agencies in late-2008 detained and interrogated two overseas bloggers upon their arrival in Nigeria. Jonathan Elendu, author of the website Elendu Reports, was arrested in October 2008 by the State Security Service, which is known to take orders directly from the president. He was reportedly questioned in relation to national security issues and for "sponsoring a guerrilla news agency."[49] Many observers believed he was detained for an alleged connection with another online platform, Sahara Reporters, that had published photographs of President Yar'Adua's 13-year-old son "waving

[44] Nigerian Communications Commission (NCC) and National Identity Management Commission (NIMC), *Design, Development and Delivery of SIM Card Registration Solution* (Abuja: NCC and NIMC, June 15, 2009), http://www.ncc.gov.ng/Headlines/SIM_Registration_RFP.pdf.

[45] "Nigerian regulator will not extend SIM registration deadline," Telecom Paper, September 22, 2011, http://www.telecompaper.com/news/nigerian-regulator-will-not-extend-sim-registration-deadline.

[46] "Federal government to acquire ₦10b gadgets to combat terrorism," Next Newspapers, November 11, 2011, http://234next.com/csp/cms/sites/Next/Home/5747537-146/story.csp.

[47] "[Town Hall Chat] Nigerian Youth Minister On Twitter @ 3-5pm Today," Tekedia, September 8, 2011, http://tekedia.com/21375/town-hall-chat-nigerian-youth-minister-twitter-35pm-today/.

[48] "8 Journalists Killed in Nigeria Since 1992/Motive Confirmed," Committee to Protect Journalists, accessed August 27, 2010http://www.cpj.org/killed/africa/nigeria/.

[49] Ndesanjo Macha, "Nigerian Blogger Arrested for Sponsoring a 'Guerilla News Agency,'" Global Voices, October 24, 2008, http://globalvoicesonline.org/2008/10/24/nigerian-blogger-arrested-for-sponsoring-a-guerilla-news-agency.

wads of money around and holding a policeman's gun,"[50] or for falsely reporting that Yar'Adua had died during the 2007 presidential election campaign. Elendu was released after two weeks without facing charges.[51] The following month, another U.S.-based online journalist Emmanuel Emeka Asiwe, editor of the Huhuonline website, was detained. The State Security Service similarly stated that Asiwe was being questioned about "matters of national security" and released him after a week of interrogation.[52]

Most recently in January 2011, Okey Ndibe, a non-resident columnist with a local newspaper and online blogger was briefly detained on arrival in Nigeria. His passports were seized,[53] and he was directed to report to the State Security Service offices. Mr. Ndibe told the *Associated Press* that "he believed his brief detention and the passport seizures came from the government's displeasure over his articles." According to the news blog TransparencyNG, "Ndibe's columns criticized the 2007 election that brought late President Umaru Yar'Adua to power… From then on, Ndibe never referred to Yar'Adua as the president." The government did not make any comments about the reason for his arrest, but his passports were given back two days later.[54]

Cyberattacks have increased in Nigeria, though most of the targets remain government websites. The website of the National Assembly was hacked on October 1, 2010 by activists who posted remarks criticizing the ruling elite for poor governance and wastefulness in spending significant resources on celebrations of Nigeria's 50 years of independence.[55] In October 2011, following a statement by the head of the telecom regulatory agency calling for internet control, the website of the NCC and another government agency, the Economic and Financial Crimes Commission, were hacked by a group known as Naija Cyber Hacktivists,[56] the same activists who have claimed almost all such incidents to date. Cybercrime remains a major problem in Nigeria, and conversations around the need for cybercrime legislation have since moved on to broader discussions on cyber security, mostly

[50] "News Blogger Detained in Nigeria," British Broadcasting Corporation (BBC), October 23, 2008, http://news.bbc.co.uk/1/hi/world/africa/7686119.stm. Sahara Reporters stated that Elendu was not on their staff and had nothing to do with the photos.
[51] Reporters Without Borders, "Nigeria: Online Journalist Emmanuel Emeka Asiwe Freed After One Week," news release, November 18, 2008, http://allafrica.com/stories/200811181177.html.
[52] Ibid.
[53] "Jonathan Government Arrests US -based Newspaper Columnist, Okey Ndibe, At Murtala Mohammed Airport In Lagos," Sahara Reporters, January 8, 2011, http://saharareporters.com/news-page/jonathan-government-arrests-us-based-newspaper-columnist-okey-ndibe-murtala-mohammed-airpo.
[54] "Okey Ndibe's Passport Released," Transparency for Nigeria, January 9, 2011, http://www.transparencyng.com/index.php?option=com_content&view=article&id=3139:okey-ndibes-passports-released&catid=88:society&Itemid=131.
[55] "Protest Against Wastage At 'Nigeria At 50' Anniversary: Hackers Hijack National Assembly Website," Sahara Reporters, October 2, 2010, http://www.saharareporters.com/news-page/protest-against-wastage-nigeria-50-anniversary-hackers-hijack-national-assembly-website.
[56] Richard Essien, "EFCC & NCC websites hacked," Daily Times, October 29, 2011, http://dailytimes.com.ng/article/efcc-ncc-websites-hacked.

because of incidents of terrorism led by an Islamic sect popularly referred to as Boko Haram. A new draft cybercrime bill, coordinated by the offices of the National Security Adviser and the Attorney General, is expected to be presented to the National Assembly as a cyber security bill.

PAKISTAN

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Not Free**
Obstacles to Access (0-25)	16	19
Limits on Content (0-35)	17	18
Violations of User Rights (0-40)	22	26
Total (0-100)	**55**	**63**

* 0=most free, 100=least free

POPULATION: 180 million
INTERNET PENETRATION 2011: 9 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Pakistan has experienced rapid growth in information and communication technologies (ICTs) in recent years. The proliferation of ICTs has also triggered an increase in citizen journalism and online activism, despite numerous social and political obstacles. In response, over the past decade, under both military rule and a civilian government, the authorities have adopted various measures to exert control over the Pakistani cyberspace and frequently frame such restrictions as necessary for "national security," the "war on terror," and the preservation of the "glory of Islam." However, the underlying pretext for censorship is often steeped with political motives.

While internet accessibility and penetration statistics have improved in 2011, the state of Pakistan's internet freedom has become precarious as a result of growing instances of political censorship and the moral policing of ICTs. Alarming events over the past year include a block on all mobile phone networks in Balochistan during the Pakistan Day celebrations in March 2012; a number of arrests and the death sentence issued for the transmission of blasphemous text messages on mobile phones; the bombing of internet cafes by Islamic militant groups; and a ban on encryption and virtual private networks (VPNs).

Furthermore, 2011 saw increased efforts by the Pakistani authorities to exert greater control over ICTs, including through the proposed Punjab Cyber & Gaming Cafe Regulation Act 2012 that aims to increase regulations on cybercafes and restrict user anonymity; an order by the Pakistan Telecommunications Authority to filter a list of "offensive" and "indecent" English and Urdu words sent via mobile phone text messages; and the request for proposals

by the National ICT Research and Development Fund for the development of a national firewall to filter and block "undesirable" content. The latter two initiatives were shelved shortly after widespread uproar from netizens and activists, demonstrating successful examples of pushback from civil society against infringements on internet freedom in Pakistan. Nevertheless, the increasing aggressiveness of the authorities to control the internet is a worrisome trend that could have significant consequences on the country's socioeconomic development in the long run.

OBSTACLES TO ACCESS

According to the International Telecommunications Union (ITU), internet penetration in Pakistan stood at close to 9 percent in 2011, up from 6.5 percent in 2006,[1] while mobile phone penetration reached nearly 62 percent.[2] Factors such as poor infrastructure, high costs, low literacy, difficult economic conditions, age, and culture are some of the constraints that have particularly limited the development and proliferation of the ICTs in Pakistan.[3] Poor copper wire infrastructure and inadequate monitoring of service quality by the Pakistan Telecommunication Authority (PTA) have further stymied the expansion of broadband internet penetration.[4] While the cost of internet use has fallen considerably in the last few years,[5] access remains out of reach for the majority of people in Pakistan. Most users go online either at their workplace or as students at universities and colleges. Cybercafes are largely limited to major cities.

Better quality broadband services remain concentrated in urban areas like Karachi, Lahore, Peshawar, Faisalabad, and Islamabad. Wireless service providers using WiMAX and EVDO along with mobile operators Mobilink, Ufone, Telenor, Warid, and Zong have also been struggling to attract consumers due to high prices and poor access quality and coverage. Pakistan does not yet have a 3G or 4G network, which is another hindrance to the spread of

[1] ITU internet penetration statistics for Pakistan were re-estimated in 2011 due to a discrepancy in past data in which the percentage of internet users in Pakistan was found to be an overestimation compared to countries with similar characteristics, according to an email communication with an ITU representative. In 2010, the ITU indicated an internet penetration rate of 17 percent based on estimates by the PTA; this figure has now been revised to 8 percent for 2010. By contrast, data from Internet World Stats, which sources its statistics from the PTA, indicated an internet penetration rate of 15.5 percent for 2011 (http://www.internetworldstats.com/stats3.htm#asia). Source: ITU, "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[2] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[3] A. Khan, *Gender Dimensions of the Information Communication Technologies for Development* (Karlstad: University of Karlstad Press, 2009).

[4] Muhammad Jamil Bhatti, "Broadband Faces Obstacles in Pakistan," Ohmy News, December 20, 2006, http://english.ohmynews.com/articleview/article_view.asp?at_code=381272.

[5] "Incentive package," Knowledge Management, accessed August 24, 2012, http://www.kmincorp.com/km/index2.php?option=com_content&do_pdf=1&id=24.

broadband internet and other wireless services;[6] however, a new 3G policy for Pakistan was approved by the prime minister in November 2011.[7] Unfortunately, most remote areas of the country have no access to broadband and are left with only slow, intermittent, poor quality connections, rendering any meaningful online activities very difficult.[8] This situation is particularly challenging for students in rural areas, who seek to study via distance learning but are deprived of multimedia lectures and tutorials. In addition, most of the areas in the conflict-stricken Khyber Pakhtunkhwa (formerly North West Frontier Province) and the Federally Administered Tribal Areas (FATA) are largely without internet access.

In 2006, the government of Pakistan initiated the Universal Service Fund (USF) to promote access to ICT services and broadband across the country.[9] As one of its special projects, the USF is piloting "Universal Telecenters" (UTCs) to be deployed in rural areas with populations above 5,000.[10] The core purpose of such telecenters is to provide the local population with equal access to health, education, and employment opportunities.[11] These centers are still in the procurement stage at the time of writing.

Power shortages in Pakistan have become an alarming issue in recent years, and throughout 2011, Pakistan faced frequent electricity shortfalls, resulting in hours-long electricity load-shedding across the country. The situation was particularly grim in rural areas where the rolling blackouts extended to as many as 20 hours a day. Urban centers also suffered from hectic load-shedding, and access to the internet was directly affected.

According to the latest data from 2012, there are 50 operational internet service providers (ISPs) throughout Pakistan,[12] along with ten broadband service providers and five hybrid fiber-coaxial (HFC) operators providing broadband internet. All ISPs are under complete control of the government through the PTA. For its backbone, the country is connected via the government-controlled Pakistan Internet Exchange (PIE) with the SEA-ME-WE 3 and 4 cables,[13] along with backup bandwidth provided by TransWorld Associates (TWA).[14] The current internet bandwidth in Pakistan is approximately 130,000 Mbits.[15]

---

[6] "3G Mobile Phones but no 3G Networks in Pakistan," Mobile Phones Blog, June 16, 2010, http://www.best-mobiles.com/3g-mobile-phones-but-no-3g-networks-in-pakistan/.

[7] "Gilani gives Pakistan's 3G policy green light," The Express Tribune (blog), International Herald Tribune, November 23, 2011, http://tribune.com.pk/story/296573/gilani-gives-3g-policy-green-light/.

[8] Pakistan Ministry of Information Technology, "Broadband Penetration in Pakistan: Current Scenario and Future Prospects," accessed February 3, 2012, http://www.ispak.pk/Downloads/MoITStudyonBroadbandPenetration.pdf.

[9] "Universal Service Fund," Ministry of Information Technology, http://www.usf.org.pk/.

[10] "Universal Telecentres (UTCs) – Pilot Project," Universal Service Fund, http://www.usf.org.pk/project.aspx?pid=16.

[11] "USF Connects Pakistani Villages to the World of Infinite Possibilities," Pakistan Insider, June 6, 2011, http://insider.pk/technology/usf-connects-pakistan/.

[12] "Internet Facts," Internet Service Providers Association of Pakistan (ISPAK), last updated April 26, 2012, www.ispak.pk.

[13] SEA-ME-WE is short for "South-East Asia – Middle East – Western Europe" and is a fiber-optic submarine telecommunications cable that provides the internet backbone between those regions. SEA-WE-ME 4 was completed in 2005 to complement SEA-WE-ME 3 which was constructed in 2000.

The PTA is responsible for issuing licenses to telecom service, internet service, and mobile phone providers through a process that is routinely bureaucratic and involves the payment of hefty licensing fees.[16] By contrast, internet cafes do not require a license to operate, and opening an internet cafe is relatively easy.[17] However, in 2011 the Government of Punjab began preparing legislation for regulating internet cafes across the province,[18] and on January 14, 2012, the Provincial Cabinet in Punjab gave formal approval to the proposal of Net Cafe Regulations Act (Punjab Cyber & Gaming Cafe Regulation Act 2012).[19] While the document has not yet been made public as of mid-2012, it is said that proposed bill focuses heavily on the work procedures of internet cafes and will oblige cafe owners to register their businesses, among other requirements that will aim to restrict user anonymity (see "Violations of User Rights").[20] As per usual practice by the government, this policy was developed in isolation and without multi-stakeholder consultations.

In recent years, the Pakistani authorities, through either government orders or court decisions, have on several occasions blocked access to various Web 2.0 applications such as YouTube, Flickr, Facebook, and different blogs and websites containing pornography.[21] Such blocks are often carried out under the rubric of restricting access to "blasphemous" content, pornography, or religious morality; however, further research into individual incidents found that the restrictions consistently corresponded to potentially politically motivated censorship (see "Limits on Content").[22] The blanket shut downs have affected a large number of users. According to the latest statistics from early 2012, there are over six million Facebook users, amounting to approximately 33 percent of all online users in the country.[23] While social-networking and blog-hosting platforms were mostly available throughout 2011 and early 2012 with several temporary disruptions of Facebook and

[14] "Cable and Wireless Worldwide Wins New Contract from Transworld Associates for International Data Services," Cable and Wireless Worldwide, July 21, 2010, http://new.cw.com/news-and-views/press-releases/2010/cable-and-wireless-worldwide-wins-new-contract-from-transworld-associates/.
[15] "Internet Facts," Internet Service Providers Association of Pakistan (ISPAK), last updated April 26, 2012, www.ispak.pk.
[16] Pakistan Telecommunications Authority, "Functions and Responsibilities," December 24, 2004, http://www.pta.gov.pk/index.php?option=com_content&task=view&id=359&Itemid=325.
[17] Sehrish Wasif, "Dens of Sleaze," The Express Tribune (blog), International Herald Tribune, July 22, 2010, http://tribune.com.pk/story/29455/dens-of-sleaze/.
[18] "Punjab makes laws to regulate internet cafes," Samaa.tv, December 19, 2011, http://samaa.tv/newsdetail.aspx?ID=40390&CID=1.
[19] "Provincial Cabinet Sanctions Net Café Regulations Act," Chief Minister Punjab, January 14, 2012, http://chiefminister.punjab.gov.pk/index.php?q=node/1228.
[20] Mehwish Shan, "Punjab to Regulate Internet Cafes," Pro Pakistani, December 21, 2011, http://propakistani.pk/2011/12/21/punjab-to-regulate-internet-cafes/.
[21] "Pakistan Blocks Access to YouTube in Internet Crackdown," BBC, May 20, 2010, http://www.bbc.co.uk/news/10130195.
[22] "How come content against Salman Taseer can be termed as 'blasphemous'?" Bytes for All Pakistan - ICT Policy Monitor Network, March 1, 2009, http://pakistanictpolicy.bytesforall.net/?q=node/160. See also, Jillian C. York, "Pakistan escalates its internet censorship," Al Jazeera, July 26, 2011, http://www.aljazeera.com/indepth/opinion/2011/07/201172511131058991 2.html.
[23] "Pakistan Facebook Statistics," Socialbakers, http://www.socialbakers.com/facebook-statistics/pakistan.

Twitter services, different religious groups persistently exerted pressure on the Pakistani courts to ban Facebook completely.[24]

The southern province of Balochistan, where a conflict between Baloch nationals and the Government of Pakistan has persisted since 1948, has been subject to increasing efforts by the Pakistani authorities to obstruct the ability of Balochi residents to access ICTs. In a worrisome incident during the national celebration of Pakistan Day on March 25, 2012, the entire province was cut off from cellular services for a day based on "an order to implement national security policy," according to the chairman of the PTA.[25] The stated aim of the mobile phone block was to thwart militant activity during the national holiday, though some saw the incident as part of the government's continual campaign of oppression against the Baloch people and nationalist movement.[26]

The PTA is the primary regulatory body overseeing internet and mobile phone services. The prime minister appoints the body's chairman and members of the PTA, and the body reports to the Ministry of Information Technology and Telecommunication.[27] Given the PTA's connections to the government, international human rights organizations, free expression groups, and independent experts have serious reservations about the PTA's governance structures, openness, and independence as a regulatory body.[28]

LIMITS ON CONTENT

Since January 2003, the government of Pakistan has taken steps to censor some online content, and the system for doing so has become increasingly sophisticated.[29] The authorities rely primarily on a blacklist of URLs that are blocked at both the internet exchange point (IXP) through the PIE and by individual ISPs. These efforts are pursued under the pretext of national security, the "war on terror," or the desire to preserve the "glory of Islam."

[24] "Permanently banning Facebook: Court seeks record of previous petitions," The Express Tribune (blog), International Herald Tribune, May 6, 2011, http://tribune.com.pk/story/162801/permanently-banning-facebook-court-seeks-record-of-previous-petitions/.
[25] Zahid Gishkori, "Security: Cell phone services in Balochistan suspended on Pakistan Day," The Express Tribune (blog), International Herald Tribune, March 23, 2012, http://tribune.com.pk/story/354095/security-cellphone-services-in-balochistan-suspended-on-pakistan-day/.
[26] "Communication siege in Balochistan to mark Pakistan Day 2012," Bytes for All, Pakistan (blog), March 25, 2012, http://content.bytesforall.pk/node/45.
[27] "Pakistan Telecommunications Authority," Pakistan Telecommunication (Re-organization) Act, 1996, October 17, 1996, Chapter II, pp 6, accessed January 26, 2012, http://www.pta.gov.pk/media/telecom_act_170510.pdf.
[28] "Legal Analysis – Pakistan: Telecommunications (Re-organization) Act," Article 19, February 2, 2012, http://www.article19.org/resources.php/resource/2949/en/pakistan:-telecommunications-%28re-organization%29-act.
[29] "Country Profile—Pakistan," OpenNet Initiative, December 26, 2010, http://opennet.net/research/profiles/pakistan.

The first incident of internet blocking occurred at the end of February 2006 when the PTA issued instructions to all ISPs in the country to block any website displaying the controversial cartoon images of the prophet Mohammed that had been published in a Danish newspaper. The block focused particularly on Google and its blog-hosting platform Blogger[30] and lasted for approximately two months.[31] In May 2010, the PTA ordered ISPs to block Facebook, YouTube, and a few Flickr and Wikipedia pages after the Lahore High Court ruled in favor of a legal appeal made by the Islamic Lawyers Movement over the Facebook page, "Everybody Draw Mohammed Day."[32] Over 10,500 websites were blocked in total,[33] while mobile phone providers also halted Blackberry services, at first completely, but later only web-browsing functions.[34] The blocking was widely criticized by civil society circles, particularly given the collateral damage inflicted on the thousands of users of these particular applications. The blanket blocks were generally temporary as a result of heavy public protests. Most of these services were available as of mid-2012, though the authorities seem to have shifted their efforts to blocking individual YouTube videos or Facebook pages instead. The exception was access to applications such as Facebook and Twitter on BlackBerry devices, which remained restricted throughout 2011; nevertheless, a range of tips for circumventing the blockage circulated online.[35]

According to the latest tests conducted by the OpenNet Initiative, censorship efforts focused symbolically on pornography and websites related to religious conversion, with some restrictions being inconsistent across different ISPs.[36] More comprehensively blocked is content perceived as anti-military, blasphemous, or anti-state, while information disseminated by Balochi and Sindhi political dissidents is the most systematically censored.[37] These blocking trends have persisted through early 2012. For example, the website of the Washington-based World Sindhi Institute[38] and the website of Lal-Masjid[39] have been

[30] Jefferson Morley, "Pakistan's Blog Blockade," Washington Post (blog), March 8, 2006, http://blog.washingtonpost.com/worldopinionroundup/2006/03/pakistans_blog_blockade.html.
[31] "PTA Unblocks Blogspot," Teeth Maestro, May 3, 2006, http://teeth.com.pk/blog/2006/05/03/pta-unblocks-blogspot.
[32] "Pakistan court orders Facebook ban," Al Jazeera, May 20, 2010, http://www.aljazeera.com/news/2010/05/201051994155758717.html.
[33] "The Shameful Saga of the Internet Ban in Pakistan," Association for Progressive Communication (APC), July 22, 2010, http://www.apc.org/en/node/10786/.
[34] Aamir Attaa, "Blackberry Services Go Offline in Pakistan," Pro Pakistani, May 20, 2010, http://propakistani.pk/2010/05/20/blackberry-services-go-offline-in-pakistan/; Aamir Attaa, "Blackberry Services Yet to be Fully Restored," Pro Pakistani, June 4, 2010, http://propakistani.pk/2010/06/04/blackberry-services-yet-to-be-fully-restored/.
[35] Omair Zeeshan, "Getting Around the Blackberry Browsing Quagmire," The Express Tribune (blog), International Herald Tribune, January 7, 2011, http://tribune.com.pk/story/97391/getting-around-the-blackberry-browsing-quagmire/; "Blackberry users in Pakistan can Migrate to Enterprise Service for Unrestricted Use," Teeth Maestro (blog), January 23, 2011, http://teeth.com.pk/blog/2011/01/23/blackberry-users-in-pakistan-need-to-migrate-to-enterprise-service-for-unrestricted-use.
[36] "Pakistan," OpenNet Initiative, August 6, 2012, http://opennet.net/research/profiles/pakistan.
[37] Pakistan Telecommunication Authority, "Blocking of Websites Access," Letter to All ISP/DSL Operators, April 25, 2006, http://pakistan451.files.wordpress.com/2006/04/PTA%20-%20Blocking%20of%20website%2025-4-06.pdf.
[38] World Sindhi Institute: http://www.worldsindhi.org/, blocked in Pakistan.

blocked since 2007. In November 2010, the authorities blocked *The Baloch Hal,* the first English language news website focused on Baluchistan, approximately one year after its launch.[40] In July 2011, the website of the popular American music magazine *Rolling Stone* was blocked by at least 13 ISPs after the site published a blog post discussing Pakistan's "insane military spending."[41] Rollingstone.com remains blocked as of May 2012.

To justify the website blockings, the authorities typically cite Section 99 of the penal code, which allows the government to restrict information that might be prejudicial to the national interest.[42] Furthermore, ISPs are required to carry out the blocking directives issued by the PTA, facing license suspensions for failure to respond.

In June 2011, a petition was brought to the Lahore High Court that sought to enable the Ministry of Telecommunications to ban obscene content such as pornography on the internet on the basis of religious morality. The petitioner was of the view that under the constitution, the state needs to prevent prostitution, gambling, and the use of illegal drugs by restricting the print, publication, circulation, and display of obscene literature and advertisements.[43] The petition is still pending as of mid-2012; however, the government has already started proactively blocking pornography websites in Pakistan on moral grounds.[44] For example, in October 2011 the PTA announced that a list of 150,000 pornographic websites had been sent to ISPs, mobile phone service providers, and international bandwidth providers to be filtered and blocked.[45] By November 2011, over 1,000 pornography websites were in the process of being blocked by ISPs.[46] Civil society organizations and the media have been actively campaigning against the block but to no avail as of yet.[47]

[39] "Lal Masjid issue and its Blocked Website," Teeth Maestro, April 12, 2007, http://teeth.com.pk/blog/2007/04/12/lal-masjid-issue-and-its-blocked-website.
[40] "The Baloch Hal Banned," Baloch Hal, November 9, 2010, http://www.thebalochhal.com/2010/11/the-baloch-hal-banned/.
[41] Jillian York, "Pakistan escalates its internet censorship," AlJazeera, July 26, 2011, http://www.aljazeera.com/indepth/opinion/2011/07/201172511131058991 2.html; "Pakistan blocks sex, drugs AND rock and roll," Association for Progressive Communications (APC) (blog), http://www.apc.org/en/blog/pakistan-blocks-sex-drugs-and-rock-and-roll.
[42] Section 99, Pakistan: Code of Criminal Procedure, 1898, http://www.intermedia.org.pk/mrc/medialawdocs/CriminalProcedureCode.pdf, accessed January 14, 2011.
[43] "Internet censorship: Court asked to ban inappropriate content," The Express Tribune (blog), International Herald Tribune, June 14, 2011, http://tribune.com.pk/story/188404/internet-censorship-court-asked-to-ban-inappropriate-content/.
[44] "Government blocks 13,000 obscene websites: Official," The Express Tribune (blog), International Herald Tribune, February 9, 2012, http://tribune.com.pk/story/334055/government-blocks-13000-obscene-websites-official/.
[45] "Pakistan Bans Porn as 150,000 explicit content website addresses are officially blocked on social and moral ground," Internet's Governance (blog), October 29, 2011, http://internetsgovernance.blogspot.com/2011/10/pakistan-bans-porn-as-150000-explicit.html; Aamir Attaa, "Breaking: PTA Decides to Ban Explicit Websites," Pro Pakistani (blog), October 20, 2011, http://propakistani.pk/2011/10/20/breaking-pta-decides-to-ban-explicit-websites/.
[46] Jahanzaib Haque, "PTA approved: Over 1,000 porn sites blocked in Pakistan," The Express Tribune (blog), International Herald Tribune, November 17, 2011, http://tribune.com.pk/story/293434/pta-approved-over-1000-porn-sites-blocked-in-pakistan/.
[47] "Pakistan: Moral Policing – a vicious cycle," Bytes for All, Pakistan (blog), October 29, 2011, http://content.bytesforall.pk/node/28; Jahanzaib Haque, "Why a ban on porn sites is futile," The Express Tribune (blog), International Herald Tribune, February 12, 2012, http://tribune.com.pk/story/335423/why-a-ban-on-porn-sites-is-futile/.

Although the professed goal of government control over the internet is to limit access to pornographic materials, extremist groups, and anti-state activists, targeted content also includes information perceived as damaging to the image of the military or top politicians. For example, the government has blocked access to specific URLs such as a video of an armed forces member's involvement in a land grab[48] and the video of the president telling members of the audience to "shut up" in the middle of a public speech.[49] Error messages seen by users trying to access blocked websites usually refer to the censored content as "blasphemous" or state that the "site is restricted." By contrast, Facebook and Twitter postings by militant Islamic groups such as Hizbut al-Tahrir or banned outfits that post comments inciting violence against sexual and religious minorities have been allowed to circulate with few restrictions.[50]

A wide variety of government agencies are involved in the censorship of online content, but the PTA is the main body overseeing such restrictions. A broad range of provisions exist in the 1996 Pakistan Telecommunications Act that support online censorship and restrict freedom of expression for the protection of national security and the glory of Islam.[51] There are no published or known guidelines as to how or why some content is blocked, or what mechanisms may be available for challenging censorship decisions.

The proposal to filter SMS text messages was another strategy attempted by the Pakistani authorities to govern moral issues in the country.[52] In November 2011, the PTA sent two extensive lists of certain English[53] and Urdu[54] words to telecommunication companies with an order to filter the listed words from any SMS message exchanged in Pakistan. There were over 1,000 English words listed while the Urdu list contained over 550 words. Many of the listed words were not generally offensive or indecent, including words such as foot, taxi, idiot, killing, damn, and Jesus Christ.[55] The SMS filtering initiative was justified by the

[48] Shahzad Ahmad, "Internet Censorship in Pakistan: Naval Chief Misusing His Powers," Association for Progressive Communications (APC), August 18, 2008, http://www.apc.org/en/blog/freedom/asiapacific/internet-censorship-pakistan-naval-chief-misusing.

[49] "When Zardari 'Shut Up' an Inattentive Audience," Indian Express, February 10, 2010, http://www.indianexpress.com/news/when-zardari-shut-up-an-inattentive-audien/578139/.

[50] Issam Ahmed, "Newest Friends on Facebook? Pakistan Militants," Christian Science Monitor, July 8, 2010, http://www.csmonitor.com/World/Asia-South-Central/2010/0708/Newest-friends-on-Facebook-Pakistan-militants.

[51] ARTICLE 19, "Pakistan: Telecommunications (Re-organization) Act," legal analysis, January 2012, http://www.article19.org/data/files/medialibrary/2949/12-02-02-pakistan.pdf.

[52] "Moral Policing gets an Upgrade in Pakistan!" Bytes for All, Pakistan (blog), November 18, 2011, http://content.bytesforall.pk/moral_policing.

[53] List of English words to be blocked on SMS in Pakistan, http://content.bytesforall.pk/sites/default/files/content%20filtering%20ENGLISH_0.PDF.

[54] List of Urdu words to be blocked on SMS in Pakistan, http://content.bytesforall.pk/sites/default/files/content%20filtering%20URDU_0.PDF.

[55] Shaheryar Popalzai and Jahanzaib Haque, Filtering SMS: PTA may ban over 1,500 English, Urdu words," The Express Tribune (blog), International Herald Tribune, November 16, 2011, http://tribune.com.pk/story/292774/filtering-sms-pta-may-ban-over-1500-english-urdu-words/.

"Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009" under the 1996 Pakistan Telecommunications Act.[56] After strong reaction from civil society and rights groups against the attempts at moral policing,[57] the decision was temporarily shelved and not in effect as of mid-2012.

Another controversy involving freedom of expression on the internet occurred on February 23, 2012 when the National ICT Research and Development Fund placed an advertisement in the press calling relevant ICT providers and companies to submit proposals "for the development, deployment and operation of a national level URL Filtering and Blocking System" in Pakistan.[58] The request for proposals expressed the desire for a sophisticated filtering system that "should be able to handle a block list of up to 50 million URLs with a processing delay of not more than 1 millisecond"[59] in order to block websites with "blasphemous, un-Islamic, offensive, objectionable, unethical, and immoral material."[60] After widespread protest from civil society and NGOs, the request for proposals was shelved less than a month after it was advertised.[61]

Despite numerous limitations on content, Pakistanis have relatively open access to international news organizations and other independent media, as well as a range of websites representing Pakistani political parties, local civil society groups, and international human rights organizations.[62] Nevertheless, most online commentators exercise a degree of self-censorship when writing on topics such as religion, blasphemy, separatist movements, or human rights protection for women and homosexuals, given the sensitivity of both the government and non-state actors to these subjects. In 2011, there were a few reports of authorities contacting bloggers to remove specific content or requiring moderators on discussion forums to delete certain messages.

The relationship between citizen journalism and traditional media in Pakistan is mutually reinforcing, particularly with respect to a number of daring, investigative bloggers and the circulation of online videos. For example, when Pakistani security forces killed five people

[56] "Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009," Pakistan Telecommunications Authority, published July 2010, http://www.ictregulationtoolkit.org/en/Publication.3919.html.
[57] "Moral Policing gets an Upgrade in Pakistan!" Bytes for All, Pakistan (blog).
[58] National ICT R&D Fund, "Request for Proposal: National URL Filtering and Blocking System," accessed August 30, 2012, http://ictrdf.org.pk/RFP-%20URL%20Filtering%20%26%20Blocking.pdf.
[59] Ibid.
[60] "PTA determined to block websites with 'objectionable' content," The Express Tribune (blog), International Herald Tribune, March 9, 2012, http://tribune.com.pk/story/347708/pta-determined-to-block-websites-with-objectionable-content/.
[61] Shahbaz Rana, "IT ministry shelves plan to install massive URL blocking system," The Express Tribune (blog), International Herald Tribune, March 19, 2012, http://tribune.com.pk/story/352172/it-ministry-shelves-plan-to-install-massive-url-blocking-system/.
[62] "Country Profile: Pakistan," Open Net Initiative, December 26, 2010, http://opennet.net/research/profiles/pakistan.

in Kharotabad near Quetta in May 2011,[63] law enforcement agencies initially justified the killing by calling the victims "terrorists" and claiming they had acted in self-defense. Upon examination of post-mortem reports and video footage of the incident uploaded on YouTube by activists, an inquiry by a judicial panel determined that the victims were actually unarmed, poor travelers.[64] In the absence of an active campaign by online activists, this crime by the security forces would have likely gone unnoticed.

Similarly, in June 2011 personnel from the Pakistan Rangers—a law enforcement agency in Karachi—killed Sarfaraz Shah upon accusations that the young man was a "dacoit" (bandit) or terrorist. The incident was caught on camera and uploaded on YouTube,[65] and the Supreme Court of Pakistan took notice of the killing,[66] ultimately leading to the conviction of the Ranger personnel for the murder.[67]

Although many civil society groups have been able to use the internet to advance their cause, mobile phones still remain the predominant medium for mobilization around political and social issues. The 2008-2010 movement by lawyers and others calling for the reinstatement of Supreme Court Chief Justice Iftikhar Chaudhry and for greater protection of judicial independence is perhaps the most prominent example of how citizens have used text-messaging, social-networking websites, and other new media tools to successfully challenge state repression.[68] The 2010 floods in Pakistan also inspired many Pakistani citizens and members of the diaspora to mobilize and raise funds online on websites such as Facebook and Twitter.[69]

VIOLATIONS OF USER RIGHTS

Article 19 of the Constitution of Islamic Republic of Pakistan grants the fundamental right of freedom of speech, although it is subject to several restrictions.[70] Pakistan also became a

[63] "5 innocent Chechens killed in Kharotabad Quetta," video, Chowk.com, May 28, 2011, http://www.chowk.com/SafroKarsevak/videos/Views/5-innocent-chechens-killed-in-kharotabad-Quetta.
[64] "Judicial panel to probe Kharotabad incident," The Nation, May 21, 2011, http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/politics/21-May-2011/Judicial-panel-to-probe-Kharotabad-incident.
[65] Faraz Khan, "Rangers shooting: Extrajudicial killing caught on tape," The Express Tribune (blog), International Herald Tribune, June 9, 2011, http://tribune.com.pk/story/185274/unarmed-youth-shot-dead-by-rangers-at-point-blank/.
[66] Nasir Mahmood, "SC takes suo motu notice of Rangers killing," Pakistan Observer, http://pakobserver.net/detailnews.asp?id=96701.
[67] "One Rangers personnel sentenced to death for Sarfaraz killing," Dawn.com, August 12, 2011, http://www.dawn.com/2011/08/12/one-rangers-personnel-sentenced-to-death-for-sarfraz-killing.html.
[68] "In Pictures: Lawyers Protest," BBC, March 12, 2007, http://news.bbc.co.uk/2/hi/in_pictures/6442747.stm.
[69] Issam Ahmed, "Pakistan Floods: How New Networks of Pakistanis are Mobilizing to Help," Christian Science Monitor, August 19, 2010, http://www.csmonitor.com/World/Asia-South-Central/2010/0819/Pakistan-floods-How-new-networks-of-Pakistanis-are-mobilizing-to-help.
[70] "Article 19," Chapter 1. Fundamental Rights, The Constitution of Pakistan, accessed September 18, 2012, http://www.pakistani.org/pakistan/constitution/part2.ch1.html.

signatory to the International Covenant on Civil and Political Rights (ICCPR)[71] in June 2010. In October 2011, Pakistan People's Party lawmaker, Sherry Rehman, introduced the Right to Information Bill in the National Assembly, a law that would prevent all public bodies from blocking a requester's access to public records.[72] As of May 2012, the bill has been submitted to a Standing Committee of the National Assembly for further discussion and is progressing towards becoming a law.

Section 124 of the Pakistan Penal Code (PPC) on sedition is extremely broadly worded, and the 2004 Defamation Act allows for imprisonment of up to five years, though they have been used infrequently to punish journalists and have yet to be used to punish online speech.[73] Rather, Section 295(c) of the penal code addressing blasphemy is more often invoked to limit freedom of expression, and most the cases concerning internet censorship in recent years have been registered under articles dealing with blasphemy. This was the case in May 2010 when the police initiated legal proceedings against Facebook founder Mark Zuckerberg following the "Everyone Draw Mohammad Day" incident.[74] The maximum punishment for blasphemy under the law is life imprisonment or the death penalty.

Amid the country's harsh legal environment limiting free expression, there were a number of arrests in 2011 and early 2012 for the transmission of blasphemous text messages on mobile phones. In one case, a Pakistani Christian man named Sajjad Masih was arrested in December 2011on charges of sending blasphemous SMS messages to Muslim clerics using a SIM card registered in his fiancé's name. Masih admitted to sending the text messages to punish his fiancé for breaking their engagement and has been in detention since his arrest. His case is still ongoing as of mid-2012.[75] In a particularly alarming case on June 21, 2011, a

[71] "President Signs Convention on Civil, Political Rights," Daily Times, June 4, 2010, http://www.dailytimes.com.pk/default.asp?page=2010\06\04\story_4-6-2010_pg7_18.

[72] According to the Right to Information bill: "This Act shall be interpreted so as to (i) promote the right to information as a constitutional right; (ii) facilitate and encourage, promptly and at the lowest reasonable cost, the disclosure of information; and (iii) All public bodies falling within the ambit of this Act shall publish, in simple terms, a yearly report on documents and activities of relevance to the public including information on organizational structure, norm and functioning, budget and finance, content of decisions and activities affecting the public and efforts to include public consultation in decision making." See, Maha Mussadaq, "Sherry Rehman's bill: Public may eventually access organisations' official records," The Express Tribune, October 17, 2011, http://tribune.com.pk/story/275663/sherry-rehmans-bill-public-may-eventually-access-organisations-official-records/.

[73] "PPC Section 124-Sedition**:** Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Federal or Provincial Government established by law shall be punished with imprisonment for life to which fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine." http://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html; Karin Deutsch Karlekar, ed., "Pakistan," in *Freedom of the Press 2011* (New York: Freedom House, 2011), http://www.freedomhouse.org/report/freedom-press/2011/pakistan.

[74] Maija Palmer, "Facebook Founder Faces Pakistan Probe," Financial Times, June 17, 2010, http://www.ft.com/cms/s/0/3aaf867e-7a42-11df-aa69-00144feabdc0.html.

[75] Shams Islam, "Blasphemy prosecution: Cleric made complainant on court directive," The Express Tribune (blog), International Herald Tribune, March 3, 2012, http://tribune.com.pk/story/344660/blasphemy-prosecution-cleric-made-complainant-on-court-directive/.

judge in the Talagang district of Pakistan issued the death sentence to 29-year old Abdul Sattar for committing blasphemy through a text message.[76]

In August 2011, the PTA sent a legal notice to all ISPs in the country ordering a ban on encryption and the usage of virtual private networks (VPNs),[77] the technology that allows internet users to go online undetected, access blocked websites, and conceal communications from government monitoring. The notice urged ISPs to report customers who used encrypted VPNs, reasoning that the ban was intended to curb communication between terrorists.[78] International and civil society organizations in Pakistan raised effective voice against this repressive development;[79] however, the orders still stand as of early 2012.

Fear of government surveillance is not a significant concern among most bloggers and online activists in Pakistan, with the exception of activists, bloggers, and media representatives in Balochistan. Nevertheless, the Pakistani authorities, particularly intelligence agencies, have been expanding their monitoring activities in recent years. For example, ISPs, telecom companies, and SIM card vendors are required to authenticate the National Identity Card details of prospective customers with the National Database Registration Authority before providing service.[80] Furthermore, under the Prevention of Electronic Crimes Ordinance—a 2007 bill that required ISPs to retain traffic data for a minimum of 90 days, among many other ICT regulations[81]—ISPs and telecom companies were obliged to keep logs of customer communications and convey them to security agencies as needed when directed by the PTA. While the bill officially expired in 2009, the practice is reportedly still active as of mid-2012.

If passed, the proposed Punjab Cyber & Gaming Cafe Regulation Act 2012 (discussed above) will place severe restrictions on anonymous communication in internet cafes in Punjab, the most populous province in Pakistan. Among the proposed regulations, users will have to register with a national identification card to log on at a cafe, while cafe owners will be

[76] Nabeel Anwar Dhakku, "Man sentenced to death for blasphemy," Dawn.com, June 22, 2011, http://dawn.com/2011/06/22/man-sentenced-to-death-for-blasphemy/.
[77] Josh Halliday and Saeed Shah, "Pakistan to ban encryption software," The Guardian, August 30, 2011, http://www.guardian.co.uk/world/2011/aug/30/pakistan-bans-encryption-software.
[78] "Pakistan needs comms security not restrictions," Privacy International, September 12, 2011, https://www.privacyinternational.org/blog/pakistan-needs-comms-security-not-restrictions.
[79] Barbora Bukovska, "Pakistan: Ban on internet encryption a violation of freedom of expression," Article 19, September 2, 2011, http://www.article19.org/resources.php/resource/2719/en/index.php?lang=en.
[80] National Database Registration Authority (NADRA), www.nadra.gov.pk; "Verification of CNICs: Nadra Signs Contract with Three Cell Phone Companies," NADRA, July 29, 2009, http://www.nadra.gov.pk/index.php?option=com_content&view=article&id=111:verification-of-cnics-nadra-signs-contract-with-three-cell-phone-companies&catid=10:news-a-updates&Itemid=20; Bilal Sarwari, "SIM Activation New Procedure," Pak Telecom, September 3, 2010, http://www.paktelecom.net/pakistan-telecom-news/pta-pakistan-telecom-news/sim-activation-new-procedure/.
[81] Kelly O'Connell, "INTERNET LAW – Pakistan's Prevention of Electronic Crimes Ordinance, 2007," Internet Business Law Services (IBLS), April 14, 2008, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2030.

required to maintain records of user information and activity for at least one year and submit monthly reports of computer usage to a national registrar. Owners will also be obliged to report any suspicious activity immediately to the police, or be held liable for user violations. Furthermore, cubicles that partition computer stations will be banned to make user activity clearly visible.[82] As of April 2012, the Act was still being deliberated in the Punjab Assembly.[83]

Provincial authorities have been exerting pressure on the central government to grant local police forces with greater surveillance powers and location tracking abilities, ostensibly to curb terrorism and violent crimes.[84] According to unofficial reports, the PIE positioned at the international internet gateway has the technical capability to monitor all incoming and outgoing traffic, as well as store all emails. In addition, Pakistan is reported to be a long-time customer of Narus, a U.S.-based firm known for designing technology that allows for monitoring of traffic flows and deep-packet inspection of internet communications.[85]

Although Pakistan is one of the most dangerous environments for traditional journalists, with 16 journalists killed and 47 injured in 2011,[86] no bloggers or online activists have been harmed to date. However, several free expression activists and bloggers have received anonymous death threats. Most of such threats were sent via text message from untraceable, unregistered mobile phone connections, usually originating from the tribal areas of the country, and several had very specific details related to the individuals' profiles or recent activities. Similarly, some militant Islamic groups consider cybercafes to be sites of moral degradation and have initiated attacks and bombings of such access points, most of which have occurred in the Khyber Pakhtunkhwa Province and FATA region. Recently in January 2012, an explosion outside of an internet cafe in Peshawar killed two people and injured 24 others.[87]

---

[82] Abdul Sattar Khan, "Punjab moves to control, regulate cyber cafes," The International News, July 9, 2012, http://www.thenews.com.pk/Todays-News-2-119345-Punjab-moves-to-control-regulate-cyber-cafes

[83] Fahim K., "Act for Monitoring Internet Cafes in Punjab to be Imposed Soon," Pro Pakistani, April 13, 2012, http://propakistani.pk/2012/04/13/act-for-monitoring-internet-cafes-in-punjab-to-be-imposed-soon/

[84] Masroor Afzal Pasha, "Sindh Police To Get Mobile Tracking Technology," Daily Times, October 29, 2010, http://www.dailytimes.com.pk/default.asp?page=2010\10\29\story_29-10-2010_pg7_18; "Punjab Police Lack Facility of 'Phone Locator', PA Told," The News, January 12, 2011, http://www.thenews.com.pk/TodaysPrintDetail.aspx?ID=25244&Cat=2&dt=1/14/2011.

[85] Timothy Carr, "One U.S. Correspondent's Role in Egypt's Brutal Crackdown," Huffington Post, January 28, 2011, http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html; "Narus: Security Through Surveillance," Berkman Center for Internet and Society at Harvard University, November 11, 2008, http://blogs.law.harvard.edu/surveillance/2008/11/11/narus-security-through-surveillance/.

[86] "PAKISTAN: 16 journalists killed and 47 were injured in different incidents during the eleven months of 2011," Asian Human Rights Commission, November 30, 2011, http://www.humanrights.asia/news/ahrc-news/AHRC-STM-184-2011.

[87] "Bomb blasts in Pakistan kill six, wound 29," UPI, January 3, 2012, http://www.upi.com/Top_News/World-News/2012/01/03/Bomb-blasts-in-Pakistan-kill-six-wound-29/UPI-89341325603299/.

Technical attacks against the websites of NGO's, opposition groups, and activists are rampant in Pakistan but typically go unreported due to self-censorship. A recent cyberattack involved the popular Pak Tea House blog, which was taken down by unknown hackers. Similarly, minority organizations such as the NCJP have also been subject to technical attacks, while online political discourse coming from Balochistan is frequently taken down without notice. The websites of government agencies are also commonly attacked, often by ideological hackers attempting to make a political statement. For example, in September 2011, the website of the Supreme Court of Pakistan was defaced by a hacker who left a message demanding the court to ban pornographic content on the internet.[88] The PTA website was attacked in October 2011 by the same hacker with the same demands.[89]

[88] Shaheryar Popalzai, "Compromised: Official website of the SC hacked," The Express Tribune (blog), International Herald Tribune, September 27, 2011, http://tribune.com.pk/story/261497/hacker-defaces-supreme-court-website/.
[89] Jahanzaib Haque, "Ban porn or else: Hacker penetrates PTA site," The Express Tribune (blog), International Herald Tribune, October 10, 2011, http://tribune.com.pk/story/271116/ban-porn-or-else-hacker-penetrates-pta-site/.

PHILIPPINES

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Free**
Obstacles to Access (0-25)	n/a	10
Limits on Content (0-35)	n/a	5
Violations of User Rights (0-40)	n/a	8
Total (0-100)	**n/a**	**23**

* 0=most free, 100=least free

POPULATION: 96 million
INTERNET PENETRATION 2011: 29 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

The Philippines connected to the internet in 1994 via the Philippine Internet Foundation (PHNet), the first internet service provider in the country. Penetration increased slowly until 2005, when Executive Order 109 was enacted calling for the expansion of telecommunication services to underserved areas, which in turn promoted competition in the information and communications technology (ICT) sector. Internet use further accelerated after 2008 with the entry of a number of industry players, although the use of mobile phones has remained more widespread. Penetration of such technologies is higher in urban areas where middle- to upper-income classes are concentrated.

People in the Philippines enjoy nearly unrestricted access to the internet and other ICTs. To date, the government has steered clear of blocking access to any type of online content. Currently weak regulations, however, have been at the center of heated debates among citizens and lawmakers, some of whom argue that new threats to the safety of online users call for stricter laws pertaining to child pornography, gambling, and cybercrime. Such proposals have, in turn, raised concerns that the government is seeking to institute filtering without blatantly violating the freedom of expression and speech, and when the filtering infrastructure is in place, it could be potentially used for political and social censorship as well.

OBSTACLES TO ACCESS

According to the International Telecommunications Union (ITU), internet penetration in the Philippines stood at 29 percent as of 2011, up from under 6 percent in 2006.[1] Nevertheless, usage is mainly limited to the national capital region and other urban areas, and it remains largely absent among the lower-income population, most of whom live in rural areas.[2] An increasing number of users are now accessing the internet from home and workplace,[3] although cybercafés remain popular among those without a personal computer. In contrast, there were over 87 million mobile phone subscribers in 2011, a penetration rate of 92 percent.[4] Subscriptions to fixed telephone lines lag far behind with approximately 3.5 million.[5] Mobile phone subscriptions increased significantly in recent years, and the SMS application has dominated the market for 2G cell phones since the mid-2000s.

Steep broadband internet subscription fees have stood in the way of a higher penetration rate in a country where 45 percent of the population lives on US$2 a day.[6] The average monthly broadband subscription is between US$7 to US$19,[7] and the penetration of fixed broadband subscriptions stood at only 1.9 percent in 2011.[8] Internet cafes charge from US$0.30 to $0.50 per hour.[9] The national government acknowledged many weaknesses in the development of ICT infrastructure in the Philippine Digital Strategy for 2011 to 2016, a roadmap for ICTs in the country. Among the weaknesses are limited market competition, poorly dispersed broadband services, lack of ICT training and skills among government leaders, and lack of transparency in the government.

The government does not place any restrictions on internet connectivity, and a wide range of Web 2.0 applications are available in the country. YouTube, Facebook, Twitter, and

[1] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[2] Iremae D. Labucay, "Internet Use in the Philippines," paper presented at the 2011 Annual Conference of the World Association for Public Opinion, September 21-23, 2011, Amsterdam, The Netherlands.

[3] "Digital Philippines 2011: Yahoo!-Nielsen Net Index Highlights," Yahoo! Southeast Asia Ptd. Ltd.and The Nielson Company (Philippines), Inc., 2011, accessed February 2, 2012, http://www.scribd.com/doc/70871638/PH-Net-Index-2011-PR-Final.

[4] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[5] National Statistics Office, "Philippines in Figures 2011," Republic of the Philippines, 2011, accessed February 2, 2012, http://www.census.gov.ph/data/publications/2011PIF_final.pdf.

[6] "Country briefing: Philippines. Multidimensional Poverty Index (MPI) At a Glance," Oxford Poverty and Human Development Initiative (OPHI), December 2011, http://www.ophi.org.uk/wp-content/uploads/Philippines1.pdf?cda6c1.

[7] Based on current rates published in March 2012 on the websites of the three biggest providers: Sun Broadband (owned by Digitel and acquired by PLDT in October 2011), PLDT, and Globe Telecom.

[8] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[9] "Digital Media in the Philippines," Singapore Management University, last modified March 31, 2012, https://wiki.smu.edu.sg/digitalmediaasia/Digital_Media_in_Philippines#cite_note-7.

international blog-hosting services are freely available, and penetration rates of these platforms are among the highest in the region.[10] However, a significant number of users still rely on dial-up connections[11] as broadband adoption in the country remains slow due to constraints such as access to frequencies, quality of service, and universal access.[12] The opposition of the Philippine Long Distance Telephone Company (PLDT)/Smart to the National Telecommunications Commission's (NTC) move to reduce interconnection prices has also slowed down broadband services.[13]

Latest government statistics reported 241 registered internet service providers (ISPs) as of 2009.[14] The slow growth of the broadband industry is mainly due to the dominance of the privately-owned PLDT that has maintained a stronghold since the late 1920s, owning a vast majority of fixed-lines and, consequently, the most stable backbone. Many local ISPs go through the PLDT because it owns the 10,000-kilometer Domestic Fiber Optic Network (DFON) connected to several international cable routes and has the highest capacity in the country at 250 Gbps.[15] PLDT also owns or manages several international cable landings in the country.[16] Further, the country's telecommunications industry in the last decade has been characterized by mergers and acquisitions amid the country's market liberalization initiatives during the 1980s and the absence of anti-trust laws. By the end of 2010, three privately-owned telecom companies were dominant: PLDT/Smart, Globe Telecommunications, Inc., and Digitel.[17] With PLDT's recent acquisition of majority shares in Digitel, the company now controls 70 percent of the country's ICT sector.[18]

To enter the ICT industry in the Philippines, companies must go through a two-stage process. First, they must obtain a congressional license that involves parliamentary hearings

[10] "Philippines Facebook Statistics," Socialbakers, accessed July 13, 2012, http://www.socialbakers.com/facebook-statistics/philippines.

[11] The Philippines saw an increase of 7.8 percent in narrowband adoption in the 3rd quarter of 2011. Source: Akamai Technologies, Inc., "The State of the Internet, 3rd Quarter, 2011 Report," 2012, http://www.akamai.com/dl/whitepapers/akamai_soti_q311.pdf?curl=/dl/whitepapers/akamai_soti_q311.pdf&solcheck=1& (registration required).

[12] Fiber infrastructure remains unavailable to "more than a fifth" of the country's provinces and 33 percent does not have access to 3G/HSPA mobile services. Source: Erwin A. Alampay, "ICT Sector Performance Review for Philippines," in LIRNE*asia's Sector Performance Review (SPR)/Telecom Regulatory Environment (TRE)* research project, September 2011.

[13] Lenie Lectura, "Smart opposes NTC interconnection fees," Business Mirror, February 12, 2012, http://businessmirror.com.ph/home/top-news/23188-smart-opposes-ntc-interconnection-fees. The Philippines has the highest interconnection rates in Asia at an average of US$0.10 compared to others' average of $0.03-05. Source: Erwin A. Alampay, "ICT Sector Performance Review for Philippines," in LIRNE*asia's Sector Performance Review (SPR)/Telecom Regulatory Environment (TRE)* research project, September 2011.

[14] National Statistics Office, "Philippines in Figures 2011," Republic of the Philippines, 2011.

[15] Mary Ann LL. Reyes, "PLDT boosts domestic fiber optic network," The Philippine Star, September 14, 2011, http://www.philstar.com/Article.aspx?articleId=726803&publicationSubCategoryId.

[16] Erwin A. Alampay, "ICT Sector Performance Review for Philippines."

[17] Ibid.

[18] Winston Castelo, "Controversy on PLDT-Digitel Merger," The Official Website of Congressman Winston "WINNIE" Castelo, November 22, 2011, http://www.winniecastelo.net/controversy-on-pldt-digitel-merger/.

and the approval of both the upper and lower houses. Second, they need to apply for a Certificate of Public Convenience and Necessity (CPCN) from the NTC. The constitution limits foreign entities to only 40 percent ownership of a business to be established in the country. Internet service is currently classified as a value-added service and is therefore subject to fewer regulatory requirements compared to mobile and fixed phone services.

Institutional arrangements regarding the ICT sector are highly bureaucratic, with much ambiguity and overlapping responsibilities among government bodies overseeing ICT development in the country. Successive government administrations have in one way or another modified the structure of the administrative body for ICTs. The latest changes came through Executive Order 47, [19] issued by President Benigno Aquino, Jr. on June 23, 2011, that created the Information and Communications Technology Office (ICTO) under the Department of Science and Technology (DOST), abolishing the Commission on Information and Communications Technology (CICT).[20] The ICTO is tasked with conducting research, development, and capacity-building in the ICT industry. The National Telecommunications Commission (NTC), created in 1979, regulates the industry with quasi-judicial powers and develops tariff and technical regulations, licensing conditions, and competition and interconnection requirements. All heads of the aforementioned organizations are appointed by the president.

The ICT sector is expecting a few more changes after the president signs Senate Bill No. 50, which will create the Department of Information and Communications Technology (DICT) and subsequently abolish the National Computer Center (NCC), Telecommunications Office (TELOF) and units in the Department of Transportation and Communications (DOTC) dealing with communications.[21] The new department will be the primary administrative entity of the executive branch tasked to oversee policy, planning, coordination, implementation, and regulation of all ICT matters. It will be composed of a secretary, undersecretaries, and assistant secretaries—all to be appointed by the president. There are sentiments that these government bodies will not able to operate independently because of their susceptibility to the influence of the incumbent administration and Congress, which determines their budget.[22]

[19] Executive Order No. 47, signed June 23, 2011, http://www.gov.ph/2011/06/23/executive-order-no-47/.
[20] The CICT was created in 2004 as the primary administrative entity of the executive branch mandated to "promote, develop, and regulate integrated and strategic ICT systems" and to serve as a transition to a proposed Department of Information and Communications Technology (DICT).
[21] Senate Bill No. 50, "An Act Creating the Department of Information and Communications Technology, defining its powers and functions, appropriating funds therefore, and for other purposes." The Bill has been awaiting a bicameral conference committee as of February 7, 2012 after being approved by both Houses and is expected to be signed by the President. See, Ricardo Saludo, "Will ICT finally get its own department?" The Manila Times, April 30, 2012, http://www.manilatimes.net/index.php/opinion/columnist1/21967-will-ict-finally-get-its-own-department.
[22] Erwin A. Alampay, "ICT Sector Performance Review for Philippines."

LIMITS ON CONTENT

There is no systematic government censorship of online content, and internet users in the Philippines enjoy unrestricted access to both domestic and international sources of information. Incidents of politically-motivated website blocking or the proactive stifling of internet expression have also not been reported.[23] The latest study by the OpenNet Initiative (ONI) found no evidence of national filtering in the country,[24] though several organizations reported monitoring and filtering activities in the workplace,[25]emerging privacy problems with regard to unrestricted access by the state and private individuals to mobile content, and local governments issuing ordinances requiring internet cafes to use monitoring technologies.[26]

Only one law, the Anti-Child Pornography Act of 2009, places restrictions on online content, and it aims to penalize access and distribution of child pornography. The law requires ISPs to install software to monitor a user's access to prohibited content and inform the authorities of user violations, though it does not require ISPs to proactively monitor the content of user communications.[27] Section 12 of the law also authorizes local government units to monitor and regulate commercial establishments that provide internet services. As of May 2012, there are eight proposed bills in the Senate calling for regulation of online content pertaining to child pornography, gambling, and phishing, some of which would require ISPs, web-hosts, and educational institutions to monitor its users and disable access to banned content. Some of these bills have prompted concerns among internet freedom advocates about the government's intent to impose certain morality norms in cyberspace.

There have been no reports of officials putting pressure on online journalists or bloggers to delete content when it is critical of the authorities. However, given that many news websites are online versions of traditional media—many of whom self-censor due to the high levels of violence against journalists in the country—it is fair to surmise that self-censorship is reflected in the content of online outlets as well. As such, the precise degree of self-censorship among online journalists and users is difficult to establish, particularly since there have been few attacks against people for their online writings.

[23] Jacques DM Gimeno, "Democracy as the Missing Link: Global Rankings of e-Governance in Southeast Asia," in A. Manoharan & M. Holzer (eds.), *E-Governance and Civic Engagement: Factors and Determinants of E-Democracy* (Hershey, PA: IGI Global, 2012), 561-583.
[24] OpenNet Initiative, "Internet Filtering in Asia," 2009, accessed July 13, 2012, http://opennet.net/research/regions/asia.
[25] Erwin A. Alampay and Regina Hechanova, "Monitoring employee use of Internet: Employers' perspective," Inquirer.net, January 24, 2010, http://business.inquirer.net/money/topstories/view/20100124-249272/Monitoring-employee-use-of-Internet-Employers-perspective.
[26] "Philippines," OpenNet.Asia, accessed February 2, 2012, http://www.oni-asia.net/country-projects/philippines/.
[27] http://www.lawphil.net/statutes/repacts/ra2009/ra_9775_2009.html

More generally, the Filipino blogosphere is rich and thriving. In 2010, the Philippines together with Indonesia led blog growth in Southeast Asia with an 18 percent increase from the previous year.[28] Both state and non-state actors actively use the internet as a platform to discuss politics, especially during elections. Some studies suggest that the popular mass uprising against then-President Joseph Estrada in 2001, later known as People Power II or EDSA Dos, could have been the result of the first active online protests facilitated by blogs and online discussion forums.[29] These forums sought to mobilize and gather people in the historic Epifanio de los Santos Avenue (EDSA) in Metro Manila, the site of the first People Power movement in 1986 that ousted the dictator Ferdinand Marcos.

A more recent example of citizen mobilization through social media occurred in September 2011 when approximately ten thousand people gathered at the Mendiola Bridge in front of the presidential palace in Manila to protest the president's proposal to cut the education budget. The event became possibly the world's largest "planking" protest during which protestors lied face down and motionless on the streets to disrupt traffic.[30] Parallel protests were staged around the country and were believed to have been organized and sustained by online protests on Facebook, Twitter, and blogs.

VIOLATIONS OF USER RIGHTS

No laws currently exist that directly encroach on citizens' freedom of expression due to the presence of a strong Bill of Rights within the 1987 Constitution, which protects freedom of expression (Section 4) and privacy of communication (Section 1).[31] However, violence against traditional journalists is a significant problem, and many fear that as internet penetration grows and more people start turning to web-based news sources, the phenomenon may spill into web-based media as well.

Statistics gathered by the Committee to Protect Journalists (CPJ) found that 70 journalists have been murdered in the country since 1992, mostly while covering political beats.[32] Violence against individuals exercising free speech, combined with a culture of impunity, the absence of a right to information law, and the use of criminal defamation laws against

[28] "Philippines and Indonesia Drive Blog Growth in SE Asia," Online Marketing Trends, March 28, 2011, http://www.onlinemarketing-trends.com/2011/03/philippines-and-indonesia-drive-blog.html.
[29] Mirandilla (2007) cited in Karan, Gimeno, and Tandoc, "The Internet and Mobile Technologies in Election Campaigns: The GABRIELA Women's Party During the 2007 Philippine Elections," *Journal of Information Technology & Politics* 6, no.3 (2009): 326-339.
[30] Karlo Mikhail Mongaya, "Philippines: Creative Protests During Campus Strikes," Global Voices Online, September 28, 2011, http://globalvoicesonline.org/2011/09/28/philippines-creative-protests-during-campus-strikes/.
[31] 1987 Philippine Constitution, Article III, Bill of Rights, http://philippines.ahrchk.net/news/mainfile.php/leg_sel/15/.
[32] "70 Journalists Murdered in Philippines since 1992," Committee to Protect Journalists, accessed February 5, 2012, http://cpj.org/killed/asia/philippines/murder.php.

critics have had a profoundly negative effect on freedom of expression.[33] Three cases of media-related murders and several instances of threats and intimidation against journalists and other media workers in 2011 were also reported. Nevertheless, there have been no reports of online journalists being harmed, threatened, or intimidated thus far.

Libel is another contentious issue in the country and is punishable by fines and imprisonment. The current law against defamatory statements is being challenged amid the unrestricted nature of the internet. In 2009, a Department of Justice resolution established that Articles 353 and 360 of the Revised Penal Code covering libel do not apply to statements posted on websites and thus cannot be treated in the same light as statements made via media covered by the law.[34] Nevertheless, three controversial cases of alleged libel committed online were filed in recent years. They involved a government official suing a citizen blogger in early 2010 after she reported that relief goods were left to rot,[35] an accusation of medical malpractice over Facebook against a popular "cosmetic surgeon to local stars in 2009,"[36] and gossip between local celebrities that went viral.[37] The case filed by the cosmetic surgeon, considered the first internet libel case in the country, was dismissed in 2011 on the grounds that prosecuting internet libel in the Philippines has jurisdictional constraints.[38]

There are no restrictions on anonymous communication in the Philippines. The government does not require the registration of user information prior to logging online or subscribing to internet and mobile phone services, especially since prepaid services are widely available even in small neighborhood stores. Nevertheless, lawmakers have repeatedly warned the public that the lack of internet regulation is resulting in the proliferation of cybercrimes, which range from harmful content for children, sexual exploitation of minors, and identity theft; as a result, several proposals have been pending to address these issues.

[33] "Philippines: ARTICLE 19's Submission to the UN Universal Periodic Review," Article 19, November 29, 2011, http://www.article19.org/resources.php/resource/2879/en/philippines:-article-19%27s-submission-to-the-un-universal-periodic-review.

[34] Department of Justice, Resolution No. 05-1-11895 on Malayan Insurance vs. Philip Piccio, et al., June 20, 2009. Article 353 states that, "libel is committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means." The Department also stated that the accused are not culpable because they cannot be considered as authors, editors, or publishers as provided for in Article 360.

[35] Leila Salaverria, "Solons defend blogger sued by DSWD for libel," Philippine Daily Inquirer, January 25, 2010, http://newsinfo.inquirer.net/breakingnews/nation/view/20100125-249403/Solons-defend-blogger-sued-by-DSWD-for-libel.

[36] Melvin G. Calimag, "Philippine Court Hears 'Facebook Libel' Case," Bloomberg Businessweek, September 25, 2009, http://www.businessweek.com/globalbiz/content/sep2009/gb20090925_532132.htm.

[37] Kristine Servando, "How to avoid libel suits on Facebook," ABS-CBNnews.com, January 5, 2010, http://www.abs-cbnnews.com/lifestyle/01/05/10/how-avoid-libel-suits-facebook.

[38] Karen Flores, "Court junks PH's first Facebook libel case," ABS-CBNnews.com, July 26, 2011, http://www.abs-cbnnews.com/lifestyle/07/26/11/court-junks-phs-first-facebook-libel-case.

Extralegal government surveillance of online communication does not appear to be a serious problem. Under the Human Security Act of 2007, law enforcement officials must obtain a court order to intercept communications or conduct surveillance activities against individuals or organizations suspected of terrorist association.[39] To date, no reports of abuse of this law have been recorded. Moreover, there have been no reports of politically-motivated incidents of technical violence or cyberattacks.

[39] "Republic Act 9372 – Human Security Act of 2011 (full text)," Philippine e-Legal Forum, July 10, 2007, http://jlp-law.com/blog/ra-9327-human-security-act-of-2007-full-text/.

RUSSIA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	12	11
Limits on Content (0-35)	17	18
Violations of User Rights (0-40)	23	23
Total (0-100)	**52**	**52**

* 0=most free, 100=least free

POPULATION: 143 million
INTERNET PENETRATION 2011: 49 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

After independent television channels were eliminated and press regulations tightened from 2000-2001, the internet became Russia's last relatively uncensored platform for public debate and the expression of political opinions. In response, the government has tried various tactics to suppress citizens' right to free speech online over the years. In 2009-2010, many bloggers were harassed and opposition blogs were hacked. While these incidents still occurred in 2011, the tactics to restrict freedom of expression online have slightly changed, with the deployment of distributed denial-of-service (DDoS) attacks[1] and various smear campaigns[2] to discredit online activists becoming more common. Extralegal intimidation of social network activists and independent forum moderators[3] has become another line of pressure over the online world through strategies such as informal meetings with the security services, calls from the Federal Security Service (FSB) to the parents of activists,[4] or the sudden refusal of forum ad sponsors to buy advertisements.

The post-election events of December 2011 through March 2012 became an important period of awakening for the Russian digital civil society. Numerous demonstrations

[1] Hal Roberts, Bruce Etling, "Coordinated DDoS Attack During Russian Duma Elections," Internet and Democracy Blog, December 8, 2011, http://blogs.law.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/.
[2] Alexey Sidorenko, "Russia: The Data Leak War and Other Pre-Election Surprises," Global Voices, October 29, 2011, http://globalvoicesonline.org/2011/10/31/russia-the-data-leak-war-and-other-pre-election-surprises/.
[3] Alexey Sidorenko, "Russia: Digital Oppression Hits Web Forums as Election Approaches," Global Voices, November 22, 2011, http://globalvoicesonline.org/2011/11/22/russia-digital-oppression-hits-web-forums-as-election-approaches/.
[4] "FSB officers and 'Extremism' center policemen threaten parents of a journalist," Grani.ru, January 20, 2011, http://www.grani.ru/Politics/Russia/activism/m.194998.html [in Russian].

organized through social-networking websites took place across the country, with the largest taking place in Moscow. Citizen and netizen activism ultimately led the government to concede a few demi-measures to pacify the protest movement, including the installation of electoral webcams (which despite poor quality, helped to identify more election fraud) and the liberalization of political party regulations.

OBSTACLES TO ACCESS

Internet and mobile phone penetration in Russia has continued to grow in 2011 and 2012,[5] and the government largely supports the dissemination of these technologies, both directly and through state-controlled internet service providers (ISPs) that offer relatively low broadband prices. In 2011, internet penetration in Russia stood at 49 percent, up from 18 percent in 2006 according to the International Telecommunication Union (ITU).[6] Approximately 71 percent of those living in urban areas have access to broadband internet,[7] and prices for unlimited broadband plans vary from US$6 in Central Russia to US$29.5 in the Far East.[8]

The level of infrastructure differs significantly across the country, and gaps are evident between urban and rural areas as well as between different types of cities. The rapid spread of mobile internet in recent years, however, has significantly improved connectivity in remote areas. Still, the worst access conditions can be found in the North Caucasus mountainous regions and the industrial towns of Siberia and the Far East. Access on Sakhalin Island at the Northern Pacific with nearly 500,000 inhabitants is particularly endangered: in May 2011, the fiber-optic cable connecting the island with the mainland was damaged, leaving inhabitants with an unreliable satellite connection as the only means to connect.[9]

By the end of 2008, the majority of schools were connected to the internet, but connection speeds are sometimes low. Libraries have been connected less extensively. Most Russians access the internet from their homes (94 percent of users) and workplaces (48 percent), while the use of cybercafes has significantly declined due to the growing penetration of WiFi

[5] Public Opinion Foundation, "Интернет-аудитория растет быстрее, чем ожидалось" [Internet audience grows faster than expected], July 15, 2011, http://bd.fom.ru/report/cat/smi/smi_int/pressr_150611.
[6] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[7] "TNS Gallup Zip Web Index," TNS Gallup, April 2012, http://www.tns-global.ru/media/content/B7525726-B5E1-4C12-BE25-4C543F42F3EE/!Web%20Index%20Report%20201204.zip [in Russian].
[8] "Internet development in Russia's regions," Yandex Company, 2011, http://company.yandex.ru/researches/reports/internet_regions_2011.xml [in Russian].
[9] "Internet access in difficult because of the wind on Sakhalin fiber-optic cable," RIA Novosti, May 19, 2011, http://dv.ria.ru/society/20110519/82009204.html [in Russian].

and mobile internet.[10] The internet is especially popular among youth, with 96 percent of individuals between 12 and 34 years old connected.[11] Applications such as the social-networking site Facebook, the Russian social-networking site VKontakte, the Twitter micro-blogging platform, and various international blog-hosting services are freely available.

Mobile phone penetration has also grown rapidly in recent years, standing at over 179 percent at the end of 2011.[12] Third-generation (3G) mobile phone infrastructure began developing relatively late due to resistance from military officials, who claimed that the technology might weaken national security.[13] Now approximately 27 percent of mobile subscribers, mostly in the largest cities, own 3G and 4G/LTE phones, and the 3G and 4G/LTE networks are expanding rapidly. Internet access via mobile telephones and similar devices has gained popularity since 2006, and 27 million people report using this method.[14]

Five access providers—MTS (former Comstar), Vimpelcom, ER-Telecom, AKADO, and the state-owned Rossvyaz (previously branded as SvyazInvest)—controlled more than 71 percent of the broadband market as of November 2011.[15] Regional branches of Rossvyaz/SvyazInvest, the fastest growing provider in the country, now account for 41 percent of subscribers, up from 36 percent in 2010. Similar to the federal level, regional dominance usually depends on political connections and tacit approval from regional authorities. Although this situation is not the direct result of legal obstacles, it nonetheless reflects an element of regional favoritism that is widespread in many parts of the Russian economy.

Three leading operators—MTS, Vimpelcom, and MegaFon—hold 83 percent of the mobile phone market.[16] While formally independent, each of these firms has indirect ties to the government. According to independent analyst Vadim Gorshkov, MegaFon is connected to former minister of telecommunications Leonid Reyman, and MTS is linked to the former Moscow regional leadership. In March 2012, Dmitry Medvedev signed a presidential decree that authorized a merger between two government-controlled ISPs, RosTelecom and

[10] Public Opinion Foundation, "Новый выпуск бюллетеня 'Интернет в России, Зима 2009/2010'" [New Issue of the Bulletin 'Internet in Russia, Winter 2009/2010'], news release, March 24, 2010, http://bd.fom.ru/report/cat/smi/smi_int/int240310_pressr [in Russian].
[11] "TNS Gallup Zip Web Index," TNS Gallup, April 2012.
[12] "Cellular Data 2011," Advanced Communications and Media Report, December 2011, http://www.acm-consulting.com/data-downloads/cat_view/7-cellular/18-cellular-2011.html.
[13] The frequency used by 3G had been restricted by the military as "strategic."
[14] J'Son and Partners, "Мобильный Интернет в России" [Mobile Internet in Russia], October 31, 2011, http://www.json.ru/files/mobile_internet_in_russia.pdf [in Russian].
[15] Advanced Communications and Media, "Russian Residential Broadband Data 2Q2011," data report, October, 21 2011, http://www.acm-consulting.com/data-downloads/doc_download/94-russian-residential-broadband-data-2q2011.html.
[16] "Cellular Data 2011," Advanced Communications and Media Report, November 2011, http://www.acm-consulting.com/data-downloads/cat_view/7-cellular/18-cellular-2011.html.

SvyazInvest.[17] While the decision does not automatically increase government control over the industry, it does significantly change the concentration of internet service provision.

The information and communications technology (ICT) sector is regulated by the Federal Service for the Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), whose director is appointed by the prime minister. Given Russia's closed political system and dominant executive branch, the appointment process is not transparent. There are no special legal restrictions on opening cybercafes or starting ISP businesses, but unfair competition, widespread corruption, and other such obstacles are not unusual in Russia.

LIMITS ON CONTENT

Although attempts to establish a comprehensive, centralized filtering system in Russia have been abandoned, content is most frequently removed and blocked on the ISP level if it violates Russia's laws against "extremism." The procedure for identifying extremist materials is nontransparent, leaving room for politically-motivated content removal.[18] Providers are punished for hosting or not blocking materials that are proscribed in a list on the the Ministry of Justice's website.[19] The list is updated on a monthly basis and included 1,066 items as of January 2012 (compared to 748 items in January 2011).[20]

Officially banned sites include Kavkazcenter.com (a radical terrorist and separatist website), Tawba.info (a site dedicated to Tatar), and radical leftist Limonka.nbp-info.ru, among others.[21] In 2011, a Moscow prosecutor tried to add LiveJournal.com to the extremist list in response to a blog post created by user "nb_licantrop,"[22] but the claim was never realized. Nonpolitical reasons for content removal have also been reported, with most involving child pornography and file-sharing services that violate copyright law.

[17] "Medvedev ordered to reorganize Rostelekom by adding Svyazinvest within one year," Gazeta.ru, March 26, 2012, http://www.gazeta.ru/business/news/2012/03/26/n_2259933.shtml [in Russian].

[18] As Dmitri Solovyev's case showed, the results may vary depending on the institution where the extremism check was performed. See, Alexey Sidorenko, "Russia: Prosecution Against Opposition Blogger Stopped," Global Voices, January 28, 2010, http://globalvoicesonline.org/2010/01/28/russia-prosecution-against-opposition-blogger-stopped/.

[19] Two such cases occurred in the Kirov and Khanty-Mansiisk regions. See, Alexey Sidorenko, "Russia: Hosting Providers Sued for Refusal to Block Web Sites," Global Voices, May 13, 2010, http://globalvoicesonline.org/2010/05/13/russia-hosting-providers-sued-for-refusal-to-block-web-sites/; "Провайдера обязали ограничить доступ к экстремистским сайтам" [Provider Obliged to Filter Extremist Sites], Regnum, February 24, 2010, http://www.regnum.ru/news/1256707.html.

[20] Ministry of Justice, "Федеральный список экстремистских материалов" [Federal List of Extremist Materials], accessed April 1, 2012, http://www.minjust.ru/ru/activity/nko/fedspisok/.

[21] These websites were included in the latest update of the Federal list of extremist materials.

[22] The official letter from the Prosecutor's office proposing to block LiveJournal was published by LiveJournal blogger "nb-licantrop" on February 22, 2011 at: http://nb-licantrop.livejournal.com/262567.html#cutid1.

In addition, there were several reports in 2011 of "regional blocking," the practice in which a website is blocked in selective areas of the country. Initiated by prosecutors in lawsuits and direct appeals to regional service providers, many of the regional blocks in 2011 were based on charges of extremism or vague claims that the sites or materials on them were otherwise harmful to society. Often, the web contents in question were not on the official list of extremist materials maintained by the Ministry of Justice. For example, some regional blocks were ordered for religious websites such as those of the Jehovah's Witnesses in the republic of Mari El in September 2011 and in the region of Chuvashia in November 2011.[23]

The practice of putting pressure on service providers and content producers by telephone has become increasingly common. Police and representatives of the prosecutor's office often call the owners and shareholders of websites to remove unwanted material. Most providers do not wait for court orders to remove targeted materials, and such pressure encourages self-censorship. As a result, there has been a massive exodus of opposition websites to foreign site-hosting providers, as well as a trend toward greater use of social-networking sites. For example, in May 2011, science fiction writer and blogger Leonid Kaganov had to change both the host and domain of his website due to allegations from the FSB of anti-Semitism and extremism and the subsequent extralegal pressure placed on the hosting providers to remove "extremist" content.[24] Kaganov, being a satirical blogger and poet, had mocked an anti-Semitic poem considered by Angarsk (a city in Siberia) as "extremist."[25]

On November 11, 2011, regulations governing the domains ".rf" and ".ru"[26] were updated to allow any law enforcement agency (such as the police, FSB, Federal Drug Control Services (FDCS), or prosecutor's office) to seize a domain without a court order. Under these new regulations, the FDCS successfully seized the domain of Rylkov-fond.ru, a website of the Rylkov Foundation that had severely criticized the country's drug trafficking situation, on February 3, 2012.[27] Later in February, the FSB seized the domain FSB21.ru on the same grounds.[28] On February 24, 2012, the largest domain registrar in Russia, Nic.ru,

[23] "В городах Чувашии заблокирован доступ к сайтам Свидетелей Иеговы" [Access to websites of Jehovah's Witnesses blocked in town of Chuvashia], Sova Center, November 22, 2011, http://www.sova-center.ru/religion/news/harassment/non_state_discrimination/2011/11/d23076/.

[24] Alexey Sidorenko, "Russia: Famous Sci-Fi Writer's Blog Removed for 'Anti-Semitism,'" Global Voices, May 29, 2011, http://globalvoicesonline.org/2011/05/29/russia-famous-sci-fi-writers-blog-removed-for-anti-semitism/.

[25] Later, Kaganov received an official explanation from the FSB that it had ordered the provider, Zenon NSP, to remove only a particular page of "material that presents a threat to the security of Russian Federation" without telling the provider to remove the whole website. "A Letter from the FSB," Leonid Kaganov's blog, July 13, 2011, http://lleo.me/dnevnik/2011/07/13.html [in Russian].

[26] Particularly Article 5, point 5.5, "Rules of the domain registration in .rf and .ru," CCTLD.ru, http://www.cctld.ru/ru/docs/rules.php [in Russian].

[27] "ARF Open letter to Mr. Ivanov – head of Russian Federal Drug Control Services," Andrei Rylkov Foundation, April 2, 2012. http://en.rylkov-fond.org/blog/ost/rost/arf-open-letter-to-mr-ivanov-head-of-russian-federal-drug-control-services/.

[28] "FSB21 Blocked By FSB Order," Openinform.ru, February 22, 2012, http://openinform.ru/news/unfreedom/22.02.2012/26450/ [in Russian].

introduced stricter rules of third level domain cancellation, which now allow for the cancelation of a domain delegation if the site includes "calls to violence, extremist activity, calls to take over power, activity that contradicts with social interests, principles of humanity and morality, offends human dignity or religious feelings."[29]

Following the elections in December 2011, numerous groups on the popular Russian social-networking website Vkontakte were created to coordinate protests against the disputed election results. In response, the FSB contacted Pavel Durov, creator of Vkontakte, to demand the removal of seven groups. Durov refused and was later summoned to the prosecutor's office, which he also ignored.[30] Despite Durov's refusal to cooperate, a user in Brynask reported that the FSB had forced the closure of the Bryansk group's Vkontakte page by contacting one of the page administrators directly. The group in Nizhny Novgorod had its webpage hacked and event cancelled. In Tver, the police temporarily detained the group's creators, Sergey Shilov and Sergey Osipov.[31] In addition, in October 2011, a Twitter user named "@Vasiliy," an anonymous military conscript and the author of the "Barracks Blog," had his identity revealed by the military authorities and the contents of his micro-blog deleted.[32]

Aside from the prosecutor's office, which serves as the government body that monitors extremist materials, the Russian police have also acquired the power to remove online content. Beginning on March 1, 2011, the vaguely-worded new law "On Police" (Article 13, point 12) granted the police the right to order hosting companies to terminate the activity of webpages that infringe on Russian or international law or endanger individual or public security.[33] Previously, the police needed a court order to close a website. Claiming that the powers are intended to provide compliance with international copyright standards,[34] the new legal framework provides more freedom for the authorities to remove content on Russia-based hosting platforms. In February 2012, Interior Minister Nurgaliev announced that the police had closed 8,500 child pornography websites in 2011.[35] Nonetheless, critics

[29] Such as ".spb.ru" and particularly ".msk.ru," where the independent ratio station Echo Moskvy has its domain. "Changes in the Terms of Service," Nic.ru, February 24, 2012, http://nic.ru/news/2012/24.02.regl-ch.html [in Russian].
[30] The full story see here: Gregory Asmolov, "Russia: Social Network In-Between Security Services and Free Market," Global Voices, December 28, 2011, http://globalvoicesonline.org/2011/12/28/russia-social-network-in-between-security-services-and-free-market/.
[31] "В Твери задержали организаторов группы "В контакте" "Против нечестных выборов," TverNews, December 9, 2011, http://www.tvernews.ru/news/27095.html [in Russian].
[32] "The author of "Barrack-blog" in danger," RealArmy.org, October 26, 2011, http://realarmy.livejournal.com/2281.html [in Russian].
[33] "Article 13. Police Powers," Codes and Laws of the Russian Federation, accessed September 11, 2012, http://www.zakonrf.info/zakon-o-policii/13/ [in Russian].
[34] "Taras Podrez, Valery Weisburg, "Russia promised the United States to close pirate sites with the help of the law 'On Police,'" Marker.ru, February 25, 2011, http://marker.ru/news/3761 [in Russian].
[35] "Nurgaliev: Policemen had closed more than 8,5 thousand websites with child pornography within a year," Fontanka.ru, Feburary 10, 2012, http://www.fontanka.ru/2012/02/10/086/ [in Russian].

have remained concerned that the law would not only be used for criminal activity but also to selectively shut down websites of political nature.

The Kremlin allegedly influences the blogosphere through media organizations as well as the pro-government youth movements, Nashi ("Ours") and Molodaya Gvardiya ("Young Guard").[36] The emergence of competing propagandist websites has led to the creation of a vast amount of content that collectively dominates search results, among other effects.[37] Leaked emails allegedly belonging to the Nashi leaders revealed that the pro-Kremlin movement had been widely engaging in all kinds of digital activities, including paying commentators to post content, disseminating DDoS attacks, and hijacking blog ratings.[38] Propagandist commentators simultaneously react to discussions of "taboo" topics, including the historical role of Soviet leader Joseph Stalin, political opposition, dissidents like Mikhail Khodorkovsky, murdered journalists, and cases of international conflict or rivalry (with countries such as Estonia, Georgia, and Ukraine, but also with the foreign policies of the United States and the European Union). Furthermore, minority languages are underrepresented in Russia's blogosphere.

Paid online campaigns against opposition activists were widely used in 2011. In October, the newspaper *Novaya Gazeta* reported that the United Russia party was planning to invest nearly US$320,000 in an effort to discredit Alexey Navalny, the prominent anti-corruption blogger and activist. The news report also wrote that the campaign might disseminate compromising footage of a Navalny look-alike involved in some illegal and/or immoral activities.[39] Several weeks later, the contents of different private mailboxes belonging to Navalny and his wife were published online at Navalnymail.kz.[40] Similarly, the private communications of Lilia Shibanova,[41] an election monitoring activist, and Boris Nemtsov, an opposition politician,[42] were published online.

[36] The Kremlin-affiliated media organizations include the Foundation on Effective Politics, led by Gleb Pavlovsky; New Media Stars, led by Konstantin Rykov; and the Political Climate Center, led by Aleksey Chesnakov.

[37] Ksenia Veretennikova, "'Медведиахолдинг': Единая Россия решила формировать собственное медиапространство" ['Medvediaholding': United Russia Decided to Form Its Own Media Space], *Vremya*, August 21, 2008, http://www.vremya.ru/2008/152/4/210951.html.

[38] Leaked mailboxes are published at this website: http://slivmail.com/ [in Russian]. Email that contains the plan to paralyze Kommersant newspaper website published at: http://rumol-leaks.livejournal.com/12040.html.

[39] "Заказ на Навального. Политический детектив," Novaya Gazeta, October 17, 2011, http://www.novayagazeta.ru/politics/48964.html [in Russian].

[40] Alexey Sidorenko, "Russia: The Data Leak War and Other Pre-Election Surprises," Global Voices, October 31, 2011, http://globalvoicesonline.org/2011/10/31/russia-the-data-leak-war-and-other-pre-election-surprises/.

[41] Alexey Sidorenko, "Russia: Creators of Election Violation Map Come Under Attack," Global Voices, November 30, 2011, http://globalvoicesonline.org/2011/11/30/russia-creators-of-election-violation-map-come-under-attack/.

[42] Anton Stepanov, "Life News publishes secret talks with the opposition Nemcova," Life News, December 19, 2011, http://lifenews.ru/news/77459 [in Russian].

Smaller smear campaigns were also implemented against less prominent bloggers such as Suren Gazaryan, a Krasnodar-based environmental activist, who discovered evidence that a campaign to discredit him had a budget amounting US$15,000.[43] In November 2011, Yevgeniy Roizman, a Yekaterinburg-based anti-drug activist, stumbled upon a job posting for campaign against him at a headhunter agency. The employers were offering US$8 for posting 100 short comments that bad-mouthed the activist.[44]

Many social-networking sites and blogging platforms belong to Kremlin-friendly business magnates, or oligarchs. Metals magnate Alisher Usmanov owns 50 percent of SUP, the company that owns LiveJournal, as well as a 35 percent stake in Digital Sky Technologies, which owns the two most popular social-networking sites in Russia and a number of other sites elsewhere in the former Soviet Union. Mikhail Prokhorov, another billionaire oligarch, owns RosBusinessConsulting (RBC), whose hosting service is home to 19 percent of all Russian websites.[45] Vladimir Potanin owns Prof-Media, which in turn owns the search engine Rambler.ru, its news portal Lenta.ru, and other popular resources. Yuri Kovalchuk, a close friend of Prime Minister Vladimir Putin's who controls the media arm of state-owned energy giant Gazprom, recently bought RuTube, the Russian analogue of YouTube.[46]

This oligarchic control over an important bloc of online media, social-networking applications, and blogging platforms has raised concerns about the Russian internet's vulnerability to political manipulation. One such politicized decision was reported in 2011: in November, the editorial board of Gazeta.ru, an outlet controlled by the metals magnate Alisher Usmanov, was allegedly forced by one of its owners to remove a banner featuring a map of voting irregularities from the portal Kartanarusheniy.ru, even though Gazeta.ru was one of the co-creators of the map together with election observation association Golos. Roman Badanin, Gazeta.ru deputy chief editor responsible for the project, had to resign due to "disagreement with the owners."[47]

The blog-hosting platforms LiveJournal, LiveInternet, Blogs.mail.ru, and Ya.ru together host the majority of all Russian-language blogs. LiveJournal has retained its leading position, though consistent DDoS attacks (in April, July, and December 2011; see "Violations of User

[43] Suren Ghazaryan, "As a journalist, Soloviev defended me from port terminals, and how much it cost budget," LiveJournal (blog), July 18, 2011, http://gazaryan-suren.livejournal.com/12446.html [in Russian].
[44] Yevgeny Roizman, "Администрации президента срочно требуются клеветники и мелкие пакостники. Оплата сдельная," LiveJournal (blog), November 2, 2011, http://roizman.livejournal.com/1268886.html#cutid1.
[45] RBC Information Systems, *Годовой отчет РБК за 2008 год* [RBC Annual Report 2008] (Moscow: RBC, 2009), http://www.rbcinfosystems.ru/ir/2008.pdf.
[46] Open Source Center, "Kremlin Allies' Expanding Control of Runet Provokes Only Limited Opposition," Office of the U.S. Director of National Intelligence, February 28, 2010, http://www.fas.org/irp/dni/osc/runet.pdf.
[47] "Замглавреда "Газеты.ру" уволился из-за проекта с "Голосом," Lenta.ru, November 30, 2011, http://lenta.ru/news/2011/11/30/gazetaru/ [in Russian].

Rights") together with rivalry from social networks such as Twitter, Facebook, and Google Plus have resulted in its decline in popularity.

Russia's vibrant blogosphere includes over 52 million blogs and micro-blogs, up from 3.8 million in 2008.[48] Blog campaigns serve as the main platform for social mobilization and play an ever-increasing role in influencing government decisions. Directed against corrupt or unacceptably arrogant government officials, bloggers' wrath has led to dismissals, boycott campaigns, and demonstrations. For example, following the parliamentary elections in December 2011, disagreement over the official results and evidence of vote-rigging collected by the crowd-sourced online portal Kartanarusheniy.ru, among others, led to a public protest that later transformed into an all-Russian movement for free elections and political reform. These post-election protests were coordinated through numerous Vkontakte event groups. A YouTube channel dedicated to documenting instances of electoral fraud also served as a major impetus for the post-election protests, garnering millions of hits.[49]

The portal Kartanarusheniy.ru is one example of the growing number and popularity of online crowdsourcing tools in Russia, which have increased from two websites in 2009 to at least 14 crowdsourcing communities in 2011. The anti-corruption portal Rospil.info created by blogger and activist Alexey Navalny, is another good example of online crowd-funding, and the tool was able to fundraise nearly six million Roubles, the largest amount ever raised in Russian history. In December 2011, another online crowd-funding strategy (facilitated by e-money platform Yandex.money) was used to collect money to sponsor a pro-democracy demonstration at Sakharov prospect (a street in Moscow) that was attended by nearly 60,000 participants.

VIOLATIONS OF USER RIGHTS

Although the constitution grants the right of free speech, this guarantee is routinely violated, and there are no special laws protecting online modes of expression. Online journalists do not possess the same rights as traditional journalists unless they register their websites as mass media. Recent police practice has been to target online expression using Article 282 of the criminal code, which restricts "extremism." The term is vaguely defined and includes "xenophobia" and "incitement of hatred toward a social group."

[48] Number of total indexed blogs and microblogs by Yandex blog search engine found at: http://blogs.yandex.ru/.
[49] Arch Puddington, "A Victory for the Net in Russia," Freedom at Issue (blog), December 8, 2011, http://www.freedomhouse.org/blog/victory-net-russia.

In 2011, Russian officials went further and proposed—in partnership with China, Tajikistan, and Uzbekistan—an "International code of conduct for information security"[50] and later a United Nations convention "On ensuring international information security."[51] The latter document would make member countries pledge to combat sources that disseminate information "that incites terrorism, secessionism or extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment." The document was not adopted internationally, although countries like Belarus have used its concepts to enact more restrictive reforms.[52] In a positive development, the criminal code was amended at the end of 2011 to decriminalize libel, reducing it to an administrative infraction punishable by fines, effective on December 8, 2011.[53]

There was less physical violence and legal harassment of bloggers in 2011 compared to 2010. In a positive development, Irek Murtazin, a prominent blogger and journalist who was imprisoned for libel against Tatarstan President Mintimir Shaimiev, was released on parole in January 2011, seven months before his official release.[54] Nevertheless, at least ten and as many as 38 cases of prosecutions against bloggers and internet activists were reported in 2011.[55] At the beginning of 2011, the police tried to prosecute several bloggers who had published a poster online that was reportedly disagreeable to Prime Minister Vladimir Putin.[56] The prosecution began in the Komi Republic against the user, "onchoys," who was charged with "defamation against a representative of the government." Similarly in April 2011, the FSB in Orel City filed a complaint to start a criminal case against Georgiy Sarkisyan for posting the same image online.[57] The proceedings in both cases, however, were eventually dropped.

[50] "China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations," Ministry of Foreign Affairs of the People's Republic of China, September 9, 2011, http://www.fmprc.gov.cn/eng/zxxx/t858978.htm.

[51] "Convention on International Information Security," Concept paper prepared for the International Meeting of High-Ranking Officials Responsible for Security Matters (Ekaterinburg, Russia: September 21022, 2011), http://isocbg.files.wordpress.com/2011/09/russian-draft-un-cyber-convention-english.doc.

[52] Glyn Moody, "No, Belarus is not cut off from the internet, but new restrictions are still pretty bad," Tech Dirt, January 3. 2012, http://www.techdirt.com/articles/20120103/07193917260/no-belarus-is-not-cut-off-internet-new-restrictions-are-still-pretty-bad.shtml.

[53] Anastasia Baraulya, "For the Criminal Code – Libel Is Not A Crime Anymore," FederalInform.ru, February 15, 2012, http://federalinform.ru/index.php/russia/rpeople/4426-2012-02-15-08-43-22 [in Russian].

[54] "Irek Murtazin: First Interview After Imprisonment," Udikov.ru, February 1, 2011, http://www.udikov.ru/2011/02/01/irek-murtazin-pervoe-intervyu-na-svobode/ [in Russian].

[55] "Threats to Internet Freedom in Russia (2011)," Agora Association, accessed April 1, 2012, http://openinform.ru/fs/j_photos/openinform_354.pdf; "Journal of Internet Unfreedom," Agora Association, accessed April 1, 2012, http://openinform.ru/fs/j_photos/openinform_356.pdf [in Russian].

[56] The poster said, "Putin – pidoras." "Pidoras" is a name for a male homosexual.

[57] "In defense of honor," Kasparov.ru, April 6, 2011, http://www.kasparov.ru/material.php?id=4D9C1F162C3DF [in Russian].

In November 2011, the server of the Kostroma-based discussion board "Kostroma Jedis" (Jedi.net.ru) was physically confiscated by the police to be used as evidence in a defamation case against Kostroma governor, Igor Slyunyaev. Forum users who tried to gather to sign a petition were dispersed by the police.[58] They later created analogues of the discussion forum on a website hosted outside of Russia. In December 2011, the Moscow Election Committee called the authorities to start an investigation against popular Russian blogger Oleg Kozyrev for defamation, an effort which was viewed as an attempt by the authorities to punish bloggers for their reporting on electoral irregularities and fraud.[59]

In June 2011, blogger Aleksey (Alaudin) Dudko—who was arrested in 2010—was sentenced to six years in a penal colony for the possession of drugs and weapons. Dudko denied the accusations and claimed his sentence was due to his blogging activity.[60] The same month, Yuri Yegorov, a blogger from Tatarstan and a former employee of the regional government, was sentenced to six months imprisonment and six months of probation for libel against the local ombudsman, Rashit Vagizov.[61] His case was overturned by a local judge in March 2012 in response to the December 2011 decriminalization of libel.[62] In November 2011, Vladimir Pronin, a blogger from the Moscow region who had been publishing online materials about corruption in the Odintsovo city police, was arrested for 13 days.[63] Only after wide coverage by the national media did the court recognize Pronin's arrest as illegal and authorized his release.

It is unclear to what extent internet users in Russia are subject to extralegal surveillance of their online activities. Since 2000, all ISPs have been required to install the "system for operational investigative measures,"[64] or SORM-2, which gives the FSB and police access to internet traffic. The system is analogous to the Carnivore/DCS1000 software used by the U.S. Federal Bureau of Investigation (FBI), and operates as a packet-sniffer that can analyze

[58] Alexey Sidorenko, "Russia: Digital Oppression Hits Web Forums as Election Approaches," Global Voices, November 22, 2011, http://globalvoicesonline.org/2011/11/22/russia-digital-oppression-hits-web-forums-as-election-approaches/.

[59] "Избирком ответил мне уголовным делом. Против меня," Oleg-kozyrev.livejournal.com (blog), December 28, 2011, http://oleg-kozyrev.livejournal.com/3926225.html [in Russian].

[60] "The court in Moscow sentenced a blogger Alexei Deuko to six years in prison," Karachaevo, June 10, 2011, http://karachaevo-cherkesia.kavkaz-uzel.ru/articles/187049/ [in Russian].

[61] "In Tatarstan, a globber was sentenced to six months for libel against the Ombudsman," Openinform.ru, June 9, 2011, http://openinform.ru/news/pursuit/09.06.2011/25035/ [in Russian].

[62] "In Kazan, the blogger accused of libel against ombudsman, released from accusation," OpenInform.ru, March 3, 2012, http://openinform.ru/news/unfreedom/30.03.2012/26621/ [in Russian].

[63] "In suburban Odintsov unfolding saga involving bloggers to trial," Novaya Gazeta (blog), November 1, 2011, http://novayagazeta.livejournal.com/390785.html [in Russian].

[64] Konstantin Nikashov, "СОРМ для IP-коммуникаций: требуется новая концепция" [SORM for IP-Communications: New Concept Needed], Iksmedia.ru, December 10, 2007, http://www.iksmedia.ru/topics/analytical/effort/261924.html?__pv=1 [in Russian]. For more information on SORM, see V.S. Yelagin, "СОРМ-2 история, становление, перспективы" [SORM-2 History, Formation, Prospects], Protei, http://www.sorm-li.ru/sorm2.html [in Russian].

and log data passing through a digital network.[65] However, no known cases of SORM-2 use have been reported, and the efficiency of the system has been seriously questioned. Meanwhile, legislation approved in April 2007 allows government services to intercept data traffic without a warrant. Online surveillance represents much less of a threat in the major cities of Moscow and St. Petersburg than in the regions, where almost every significant blog or forum is monitored by the local police and prosecutor's office. Most of the harassment suffered by critical bloggers and other online activists in Russia occurs in the regions.

Roskomnadzor, the regulatory body overseeing information technology and mass communications, announced in late 2011 that it had installed online software to detect "extremist" material. Under the new system, websites flagged by the software are given three days to take down allegedly offending content. If a site does not comply, two additional warnings are sent followed by a complete shutdown. The test mode version of the software was to begin operating in December 2011, though its full deployment was indefinitely postponed as of mid-2012. The justice ministry, on the other hand, has invited bids to create its own internet monitoring system, apparently for the purposes of examining content relatied to the Russian government and justice systems and to any European Union statement concerning Russia.[66]

In 2011, the FSB became keenly interested in services that use encryption, particularly Skype, Hotmail, and Gmail. In January 2011, the regional government in Sverdlovsk prohibited its employees from using Skype and Gmail.[67] In April 2011, a representative of the FSB said that any service using protocols that could not be hacked by the FSB should be banned from use,[68] but these calls were dismissed by the Ministry of Telecommunications and Political Leadership.[69]

ICT providers are routinely asked to hand over user data to the authorities. In March 2011, the police requested from forum administrators the IP address of a graphic designer known as "Isabelle" after she had drawn a series of political posters, most of them mocking the ruling party United Russia, online at NevinkaOnline.ru.[70] In April 2011, donors to the

[65] B. S. Goldstein, Y. A. Kryukov, and V. I. Polyantsev, "Проблемы и Решения СОРМ-2" [Problems and Solutions of SORM-2], *Vestnik Svyazi* no. 12 (2006), http://www.protei.ru/company/pdf/publications/2007/2007-003.pdf [in Russian].
[66] "2012 Surveillance: Russia," Reporters Without Borders, March 12, 2012, http://en.rsf.org/russia-russia-12-03-2012,42075.html.
[67] Ashley Cleek, "Russia: Why Skype Worries the FSB?" Global Voices, January 22, 2011, http://globalvoicesonline.org/2011/01/22/russia-why-skype-worries-the-fsb/.
[68] "FSB wants to ban Skype and Gmail, as no control over communication and correspondence on these resources," Gazeta.ru, April 8, 2011, http://www.gazeta.ru/news/lastnews/2011/04/08/n_1784533.shtml [in Russian].
[69] Marina Litvinovich, Sian Sinnot, "Russia: Bloggers Stop FSB Initiative to Ban Skype," Global Voices, April 18, 2011, http://globalvoicesonline.org/2011/04/18/russia-bloggers-prevent-fsb-from-banning-skype/.
[70] "In the Stavropol region, the struggle between Russia and United Internet users," LiveJournal (blog), March 12, 2011, http://mredisonic.livejournal.com/7525.html [in Russian].

Russian anti-corruption website Rospil.info received calls and emails from unknown people (allegedly members of the pro-Kremlin youth movements) asking about their donations. Previously all donors had sponsored money via the aforementioned crowd-funding site Yandex.Money. In May 2011, Yandex.Money confirmed it had released Rospil.info donors' financial and personal information to the FSB.[71] In November 2011, the Russian Drug Control Service approached Habrahabr.ru, a popular IT-portal, and demanded[72] personal data of the Belarus-based staff writer Anatoly Alizar on the grounds of alleged drug propaganda.[73] In this instance, the portal refused to provide the data.

Extralegal intimidation of social network activists and independent forum moderators has become another line of pressure over the online world through strategies such as informal meetings with the security services, calls from the FSB to the parents of activists, or the sudden refusal of forum ad sponsors to buy advertisements. For example, in an attempt to intimidate activists during the post-election period in December 2011, the FSB called the parents of Ilya Klishin for questioning after Klishin had organized a rally to be held on December 10th in Moscow through the Facebook page, "For Fair Elections."[74]

In addition to official monitoring and prosecution, critical websites face censorship in the form of unexpected "technical difficulties." Over the past year, DDoS attacks have become an increasing problem for the Russian media sphere. Still, the police generally refuse to investigate the attacks.[75] LiveJournal, the most popular blogging platform in Russia, was attacked three times during the year. During the parliamentary election in December 2011, 22 websites became dysfunctional due to a powerful attack dubbed as the election "DDoS-alypse."[76]

More generally, cybercrime is a serious problem, as a significant number of cyberattacks were carried out from Russia and against Russian cyber actors. A number of factors contribute to this threat. First, many personal computers in Russia are not protected by antivirus software, leaving them vulnerable to infection and integration into "botnets"—networks of computers that are controlled remotely for malicious purposes. Second,

[71] Ashley Cleek, "Russia: Anti-Corruption Donor Details Leaked," Global Voices, May 4, 2011, http://globalvoicesonline.org/2011/05/04/russia-anti-corruption-donor-details-leaked/.
[72] Dura Lex, "Federal Drug Control Service aims Alizar," Habrababr.ru, October 14, 2011, http://habrahabr.ru/blogs/Dura_Lex/132109/ [in Russian].
[73] In his post, Alizar speculated on Steve Jobs' ingenuity, marijuana and LSD, and the governments' policies towards light drugs, citing such widely recognized media outlets as *Time Magazine*, the *New York Times*, etc.
[74] "FSB officers and 'Extremism' center policemen threaten parents of a journalist," Grani.ru, January 20, 2011, http://www.grani.ru/Politics/Russia/activism/m.194998.html [in Russian].
[75] "«Живой журнал» остался без дела," Gazeta.ru, August 22, 2011, http://www.gazeta.ru/business/2011/08/19/3739473.shtml [in Russian].
[76] Alexey Sidorenko, "Russia: Election Day DDoS-alypse," Global Voices, December 5, 2011, http://globalvoicesonline.org/2011/12/05/russia-election-day-ddos-alypse/.

information and instruction on how to build and develop botnets is widely accessible. Finally, punishment of cybercriminals is rare, contributing to a culture of impunity. According to some sources, many hackers for hire are willing to carry out DDoS attacks for as little as €200 (US$260) per day.[77]

[77] "В России DDoS-атака стоит от 200 евро в сутки" [In Russia DDoS Attack Costs 200 Euros Per Day]," iToday.ru, April 5, 2010, http://itoday.ru/news/35916.html [in Russian].

RWANDA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	14	13
Limits on Content (0-35)	19	19
Violations of User Rights (0-40)	17	19
Total (0-100)	**50**	**51**

* 0=most free, 100=least free

POPULATION: 11 million
INTERNET PENETRATION 2011: 7 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Since Rwanda's 1994 genocide that ravaged the country's skilled workforce and destroyed its already underdeveloped telecommunications infrastructure,[1] the ruling Rwandan Patriotic Front (RPF) has set forth an ambitious plan to establish Rwanda as a globally competitive, knowledge-based society and economy.[2] Although the internet penetration remains low, over the past decade the country has experienced an increase in the number of fixed telephone lines, mobile phones, and technicians. The proliferation of information and communication technologies (ICTs), in return, has contributed to progress in education, good governance, human capacity development, and rural community activities.

While internet and mobile phone usage has expanded over the past two decades, the country's tenuous political environment has led the government to exert some controls over online content and expression. In addition, despite recent improvements to internet access, poverty and lack of appropriate infrastructure, especially in rural areas, continue to impede access to and the expansion of ICTs in Rwanda.

There remain concerns that the government's firm restrictions on print and broadcast media—particularly on contentious content regarding the ruling party or the 1994 genocide—will cross over into the internet sphere, as occurred when the authorities

[1] Albert Nsengiyumva and Emmanuel Habumuremyi, *A Review of Telecommunications Policy Development and Challenges in Rwanda* (Johannesburg: Association for Progressive Communications, September 2009), http://www.apc.org/en/pubs/research/review-telecommunications-policy-and-challenges-rw.
[2] Glen Farell, "Survey of ICT and Education in Africa: Rwanda Country Report," *info*Dev, April 2007, http://www.infodev.org/en/Document.423.pdf.

blocked the online version of an independent newspaper in the lead-up to the 2010 presidential election. Furthermore, violence against online journalists, although sporadic, appears to be on the rise, with one alarming murder of an online journalist reported in December 2011.

OBSTACLES TO ACCESS

Widespread poverty is the primary impediment barring Rwandans from accessing new ICT developments, especially the internet. Over 90 percent of the population lives in rural areas, with the majority practicing subsistence agriculture and approximately 64 percent living below the poverty line. In addition, though over 70 percent of the population is literate,[3] between 70 and 90 percent speak only Kinyarwanda.[4] Further, while the cost of internet services and private VSAT[5] satellite links has dropped in recent years, access is still limited mostly to Kigali, the capital city, and remains beyond the economic capacity of most citizens, particularly those in rural areas who are limited by low disposable incomes. Consequently, the internet penetration rate is still quite low at 7 percent in 2011, according to official government statistics and the International Telecommunication Union (ITU).[6]

In the face of such challenges, the Rwandan government has made ICT development a high priority, spending in this domain more than most other countries on the continent, and instituting incentives such as tax exemptions on ICT equipment. Although the full impact of these investments has yet to be felt, broadband internet service is progressively replacing dial-up connections, and a 2012 analysis of worldwide broadband download performance ranks Rwanda in 105th place worldwide with an internet speed of 3.60 Mbps as of March 2012,[7] and third place in Africa for downloading speeds, outperforming both Kenya and South Africa.[8] Broadband connectivity is expected to increase further with the completion of

[3] Central Intelligence Agency (CIA), "Rwanda," The World Factbook, accessed June 26, 2012, https://www.cia.gov/library/publications/the-world-factbook/geos/rw.html.
[4] Ann Garrison, "Rwanda Shuts Down Independent Press," *Digital Journal*, April 14, 2010, http://www.digitaljournal.com/article/290545; Beth Lewis Samuelson and Sarah Warshauer Freedman, "Language Policy, Multilingual Education, and Power in Rwanda," *Language Policy* 9, no. 3 (June 2010), http://gse.berkeley.edu/faculty/swfreedman/10samuelson_freedman.pdf.
[5] VSAT stands for "very small aperture terminal," an earthbound station used in satellite communications of data, voice and video signals, excluding broadcast television.
[6] Rwanda Utilities Regulatory Agency (RURA), "Statistics and Tariff Information in Telecom Sector as of September 2011," Republic of Rwanda, September 2011, http://www.rura.gov.rw/docs/STATISTICS_TARIFF_INFORMATION_IN_TELECOM_SEPTEMBER_2011.pdf; International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[7] Net Index, "Rwanda," Download Index, accessed June 26, 2012, http://www.netindex.com/download/2,174/Rwanda/.
[8] Afrographique, "African Broadband Download Performance," April 2011, http://afrographique.tumblr.com/post/4533385659/infographic-showing-african-broadband-download.

a 2,300 kilometer (1,380 miles) fiber-optic telecommunications network across the country that will link Rwanda to the undersea cables running along the East African coast. The fiber-optic project is meant to boost access to various broadband services, increase electronic commerce, and attract foreign direct investment through business process outsourcing.[9] The project is also expected to expand internet service to the countryside.[10] In 2010, e-government and videoconferencing platforms were developed to help make governance more efficient by shortening travel times, cutting expenses, and improving communication among district authorities. Advanced social-networking web applications such as YouTube, Facebook, Twitter, and international blog-hosting services are freely available.

The mobile phone penetration rate is significantly higher than that for internet access, reaching 41.3 percent and 4.4 million subscribers as of November 2011, according to official statistics and the ITU.[11] While there is great disparity in internet penetration rates between urban and rural areas, rural populations have a comparatively high mobile phone usage rate, as illustrated by an August 2011 report from MTN Rwanda, one of the largest telecom operators in the country, which stated that the majority (60 percent) of its mobile voice users resides outside of Kigali.[12] Access is made easier by a well-developed mobile phone network that covers nearly 96 percent of the population;[13] however, in remote border areas, coverage remains faulty or nonexistent. To facilitate greater access, the Rwanda Utilities Regulatory Agency (RURA) is attempting to reduce the price of handsets from 8,000 Rwandan francs (US$13) to 2,000 RWF (US$3.25). RURA's move is to cover half of the total cost, whereas operators would contribute 30 percent and consumers would pay the remaining 20 percent. Talks are also being held with the Rwanda Development Bank to provide micro-loans for handsets.[14]

However, the rates for calls from mobile phones to fixed lines remain prohibitively expensive for much of the population, limiting the number of these calls. The current estimate is that 90 percent of interconnection calls are from the fixed-line company, Rwandatel network, to mobile phone companies rather than the other way around. TIGO is

[9] "Rwanda completes $95 mln fibre optic network," Reuters Africa, March 16, 2011, http://af.reuters.com/article/investingNews/idAFJOE72F07D20110316.

[10] Emmanuel Habumuremyi and Alan Finlay, "Rwanda's Policy Vacuum Could Mean Trouble for Broadband," Association for Progressive Communications, October 29, 2009, http://www.apc.org/en/news/rwanda-s-policy-vacuum-could-mean-trouble-broadban.

[11] "ICT Statistics, Mobile Subscribers as of November 2011," Rwanda Utilities Regulatory Agency (RURA), accessed January 24, 2011, http://www.rura.gov.rw/index.php?option=com_content&view=article&id=296; International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[12] Saul Butera, "Rwanda: High costs affecting rural internet penetration," The New Times, August 15, 2011, http://in2eastafrica.net/rwanda-high-costs-affecting-rural-internet-penetration/.

[13] RURA, "Statistics and Tariff Information in Telecom Sector as of September 2011."

[14] "Is Rwanda the Singapore of Africa," Association Rwandaise des Femmes des Medias, May 24, 2011, http://arfem.rw/wp/?p=511.

the cheapest in terms of both regional and international calls, which cost 120 RWF (US$0.20) and 200 RWF (US$0.32), respectively. MTN charges 139.8 RWF (US$0.23) for regional calls and 250.2 RWF (US$0.41) international calls. TIGO is also the cheapest in terms of both normal tariffs and also promotional tariffs on SMS (10 RWF for MTN and 3 RWF for TIGO).[15] Though Rwanda was said to have higher internet prices in the East African region, ISPs pledged to scale them down by the first quarter of 2012.[16]

Internet access via mobile phones has been available since 2007, but the high cost of data-enabled handsets and limited bandwidth restrained its popularity in the first few years. With the government-sponsored fiber-optic cable expansion project completed in early 2011, internet service throughout the country has improved, facilitating increased mobile phone internet access.[17] In addition, MTN Rwanda has introduced low-cost data-enabled mobile phones ranging from 18,500 to 20,000 RWF (US$20 to $32) to expand internet access, especially in rural areas.[18] Innovative initiatives targeting rural populations have further encouraged increased mobile phone and internet usage, such as the e-Soko (e-market) program created by the Rwanda Development Board to help farmers get real-time information about market prices for their agricultural produce through their mobile phones.[19]

Following the country's market liberalization policies implemented in 2001,[20] the number of companies providing telephone and internet services increased from one—the state-run Rwandatel—to about a dozen in 2011. These include fixed-line providers (Rwandatel, MTN Rwandacell, and Artel International), mobile phone providers (Rwandatel, MTN Rwandacell, and TIGO), and internet service providers (ISPA, Rwandatel, MTN Rwandacell, New Artel, Altech Stream Rwanda, Value Data Rwanda, Star Africa Media, Greenmax, Augere Rwanda, and Comium).[21] BhartiAirtel, an Indian telecommunications company, is the newest player on the market that was awarded a license to operate 2G and

[15] RURA, "Statistics and Tariff Information in Telecom Sector as of September 2011."
[16] "Rwanda: Internet Charges to Be Slashed," The New Times, November 28, 2011, http://allafrica.com/stories/201111280003.html.
[17] MasimbaTafirenyika, "Information technology super-charging Rwanda's economy," Africa Renewal, April 2011, http://www.un.org/ecosocdev/geninfo/afrec/vol25no1/rwanda-information-technology.html.
[18] Saul Butera, "Rwanda: High costs affecting rural internet penetration," The New Times, August 15, 2011, http://in2eastafrica.net/rwanda-high-costs-affecting-rural-internet-penetration/.
[19] Ruth Kang'ong'oi, "Rwanda Telecenter Network introduces Web 2.0 to farmers," CIO East Africa, November 15, 2011, http://www.cio.co.ke/view-all-top-stories/4482-rwanda-telecenter-network-introduces-web-20-to-farmers.html.
[20] Albert Nsengiyumva and Emmanuel Habumuremyi, *A Review of Telecommunications Policy Development and Challenges in Rwanda*, Association for Progressive Communications (APC), September 2009, http://www.apc.org/en/system/files/CICEWARwanda_20090908.pdf.
[21] National Institute of Statistics of Rwanda, *ScanICT Baseline Survey Report* (Kigali: National Institute of Statistics of Rwanda, November 2008), http://www.uneca.org/aisi/docs/RWANDA_SCAN_ICT_REPORT.pdf.

3G GSM mobile services in Rwanda in September 2011.[22] These providers are all privately owned, with the exception of the state-operated Rwandatel, which was partially privatized in 2010 when it sold 80 percent of the company to the Libyan firm, LAP Green. Due to the political turmoil in Libya in 2011 and the subsequent freeze on Libya's investments and assets, however, LAP Green was forced to terminate its business in Rwanda.[23]

Two government-appointed regulatory bodies—the Rwanda Information Technology Authority (RITA) and RURA—supervise the regulatory frameworks and implementation of the county's policies and strategies in the telecommunications sector. Although these bodies were created by the government, they seem to be working freely and no known complaint has been leveled against them by investors in telecommunications. In 2009, RURA set up the Rwanda Internet Exchange (RINEX) to connect ISPs and enable local internet communications to be routed through RINEX without having to pass through international networks.[24] ISPs may also opt to connect via RINEX to the international internet. The aim is ostensibly to make intra-Rwandan internet communications cheaper and faster, though such control over internet traffic has the potential to facilitate any future efforts to systematically censor or monitor domestic online communications. As of the end of 2009, only several ISPs were properly connected to RINEX, and the price for national access remained the same as for international access.[25] By 2011, it appeared that most ISPs were reluctant to exchange their data through RINEX as only five of them were connected.[26]

LIMITS ON CONTENT

Access to online content in Rwanda is generally unfettered; however, there have been increasing instances of government control over internet expression in recent years. The websites of international human rights organizations such as Freedom House, Amnesty International, and Human Rights Watch, as well as the online versions of media outlets like the British Broadcasting Corporation (BBC), *Le Monde*, Radio France Internationale, the *New York Times*, and many others are freely accessible. Websites of national news outlets are also

[22] "Indian firm BhartiAirtel new player on mobile market," The Rwanda Focus, September 9, 2011, http://focus.rw/wp/2011/09/indian-firm-bharti-airtel-new-player-on-mobile-market/.
[23] Samson Baranga, "UTL to get capital injection to clear debts," The Observer, December 14, 2011, http://www.observer.ug/index.php?option=com_content&view=article&id=16307%3Autl-to-get-capital-injection-to-clear-debts&catid=38%3Abusiness&Itemid=68.
[24] Rwanda Utilities Regulatory Agency (RURA), *Guidelines for Rwanda Internet Exchange Point (RINEX) Management* (Kigali: RURA, 2009), http://www.rura.gov.rw/docs/RINEX_GUIDELINES.pdf.
[25] Antoine Bigirimana, "Rwanda: The Story of the Internet—One Step Forward, Two Steps Backward," *The New Times*, December 12, 2009, http://allafrica.com/stories/200912150559.html.
[26] Justin Rugondihene, "Rwanda Internet Exchange Point (RINEX): Positive steps, key challenges, sustainability and management," EAIXP Taskforce Meeting, 1st to 3rd November 2011, accessed February 8, 2012, http://www.rura.gov.rw/docs/Rwand_IXP_Positives_Steps.pdf.

easily accessible, and one of the founders of the online news portal Igihe.com reported no constraints or pressures from the government in establishing and managing the website.[27] Nevertheless, the web versions of state-run media outlets—such as *Imvaho Nshya*, *La Nouvelle Relève*, the Rwanda News Agency, and the *New Times*—dominate the online information landscape. In addition, the economic environment for online news websites remains a challenge for independent outlets, particularly in comparison to their state-run counterparts that derive their income from government advertisements and direct subsidies.

Despite the generally open online atmosphere, an incident in the months leading up to the last presidential election in August 2010 raised concerns that the authorities may be willing and able to restrict online content. In April 2010, Rwanda's two main independent newspapers, *Umuseso* and *Umuvugizi*, both published in Kinyarwanda, were given six-month suspensions as a consequence for defaming the president and other offenses.[28] The suspension was widely perceived as an effort to suppress critical coverage in the run-up to the election. *Umuvugizi*'s editor, who fled Rwanda into exile, launched an online version of the paper in late April 2010, but in early June the Media High Council ordered the website to be blocked, arguing that the ban on the newspaper applied to the online version as well.[29] Appealing such a ban was possible based on provisions of the Media Law, although in this instance, the publications chose not to appeal. *Umuvugizi* was unblocked after the six-month suspension period had expired, though it reportedly experienced periodic filtering throughout the 2011 and was blocked again for three days in June 2011 prior to a court case that sentenced the website's exiled editor-in-chief to two and a half years in prison (see "Violations of User Rights").[30]

The government-operated High Media Council has established an online monitoring department to screen web content, and the Council has been known to contact websites to request the removal of certain information.[31] In addition to the blocking of *Umuvugizi*, two other online news websites, Umusingi and Umurabyo, have experienced government requests to delete content related to local political affairs and ethnic relations. There have

[27] Interview with Founder of Igihe.com in February 2010.
[28] Michael Fairbanks, "Nothing Good Comes Out of Africa," Huffington Post,May 3, 2010, http://www.huffingtonpost.com/michael-fairbanks/nothing-good-comes-out-of_b_560639.html; International Freedom of Expression eXchange (IFEX), "Rwanda Shuts Critical Papers in Run-Up to Presidential Vote," news release, April 13, 2010, http://www.ifex.org/rwanda/2010/04/14/papers_suspended/.
[29] Reporters Without Borders, "Persecution of Independent Newspapers Extended to Online Versions," news release, June 11, 2010, http://en.rsf.org/rwanda-persecution-of-independent-11-06-2010,37718.html. The newspaper *Umuseso,* which also was placed on a six month suspension, does not have an online version.
[30] "Rwanda: Exiled editor sentenced for 'insulting' president," Committee to Protect Journalists, June 6, 2011, http://www.cpj.org/2011/06/rwanda-exiled-editor-sentenced-for-insulting-presi.php.
[31] "Rwandan gov't officials to counter 'harmful' propaganda through social media," Great Lakes Voice, March 13, 2011, http://greatlakesvoice.com/?p=681.

also been instances reported of opposition sites being blocked.[32] As a result of these controls, online journalists based in Rwanda are joining their print and broadcast colleagues and exercising self-censorship, particularly on topics that can be construed as disruptive to national unity and reconciliation. Many fear the further increase of government control over online media with the proposed amendments to the 2009 Media Law currently in review as of early 2012, which if passed, may provide a legal basis for the blocking of unfavorable websites.[33]

There are no clear regulations outlining the treatment of obscene content, but Article 57 of the current Media Law indicates that cybercafe operators, business owners, and parents are expected to take responsibility for preventing minors from viewing websites that display pornography or information that might incite them to crimes such as drug use or theft.[34] Despite the government's efforts to regulate online content, the expansion of internet access has enabled the Rwandan blogosphere to evolve into a vibrant platform for expression, largely consisting of youth who write on a variety of topics, including their political views. The websites and blogs of opposition activists both within and outside Rwanda are more or less freely available;[35] however, opposition supporters living outside Rwanda, mainly in Europe and the United States, are responsible for most of the criticism against the government that appears on forums, websites, and blogs.

Facebook is also emerging as a popular site for online interaction with nearly 115,000 users of whom over 70 percent are between 18 and 34 years of age as of December 2011.[36] A government initiative in early 2011 urged all top government officials in Rwanda to sign up for and participate in social media networks such as Facebook and Twitter, which some believe is an effort to counter the growth of opposition voices online.[37] Nevertheless, the social media revolution has empowered Rwandans to discuss issues that were formerly taboo and not open to public discussion due to fears of persecution.[38] Rwandan President Paul Kagame is an active supporter of these social networks as he occasionally engages in discussions with users and responds openly to issues relating to the current state of

[32] Examples of these opposition sites include: http://inyenyerinews.org/, www.umuvugizi.com, www.umusingi.com, www.banyarwandapoliticalparty.org, http://leprophete.fr/.
[33] "Proposed media law fails to safeguard free press," IFEX, January 5, 2012, http://www.ifex.org/rwanda/2012/01/05/media_law/.
[34] "Law on Media," *Official Gazette of the Republic of Rwanda*, August 17, 2009, http://www.mhc.gov.rw/index.php?option=com_docman&task=cat_view&gid=81&Itemid=144&lang=en.
[35] This includes the website of opposition leader IngabireVictoireUmuhoza at http://www.victoire2010.com, as well as other sites at http://ww.iwacu1.com,http://ww.musabyimana.be,http://rwandarwabanyarwanda.over-blog.com,and http://ww.banyarwandapoliticalparty.org.
[36] "Facebook Statistics: Rwanda," Socialbakers, accessed December 29, 2010, www.socialbakers.com/facebook-statistics/rwanda.
[37] Gilbert Ndikubwayezu, "Social media defies oppression," Major Projects: Online Journalism in Rwanda, 2011, accessed January 16, 2012, http://www.journalism.ryerson.ca/grad/3715/6/.
[38] Ibid.

governance in the country. For example, Kagame was featured on YouTube's World View in 2011[39] answering questions submitted by viewers about Rwanda and life after the genocide.[40] Rwandans are also increasingly using Twitter. By the end of 2011, Rwanda was second in number of tweets throughout the Great Lakes region after Kenya.[41]

With mobile phones more widely accessible than the internet, text messages have become an important way for citizens to voice discontent with the authorities and expose abuses of power. In one widely reported example in 2009, several local officials and other well-to-do residents stole cows that had been donated by the president for needy residents in the countryside. The theft was reported to local radio stations via text messages, sparking widespread coverage by the media. As a result, the officials were forced to resign or were otherwise punished. Text messages were also used for political mobilization during the 2003 and 2008 elections. In 2010, they enabled the National Electoral Commission to improve voter education and allowed candidates and political parties to mobilize supporters. In particular, contenders from parties other than the ruling party were able to garner more votes than they might have otherwise due to the ability to reach voters via text-messaging campaigns.[42] Most recently, mobile phones have been used for initiatives such as disease detection and prevention programs where free mobile phones are distributed to health care agents who save mothers' lives by monitoring pregnant villagers and sending text messages to hospitals.[43] The ability of citizens to use digital media for organizing large-scale "real life" protests remains limited, however, due to broader restrictions on freedom of assembly, particularly regarding politically sensitive topics.

VIOLATIONS OF USER RIGHTS

The Rwandan constitution, adopted in May 2003, provides for freedom of expression. In addition, Chapter IV of the Law on Media signed in August 2009 is dedicated to "ICT or internet press" and includes language that explicitly grants freedom for online communications; however, as noted earlier, the Media Law is currently under review and

[39] "An Interview with President Paul Kagame," YouTube World View Interview, video clip, May 10, 2011, http://www.youtube.com/watch?v=hGbbK05nbJM.
[40] Emmanuel Habumuremyi, "Rwanda – Balancing Freedom of Expression: The Need for Limitations and Responsibilities," Global Information Society Watch, 2011, http://giswatch.org/sites/default/files/gisw_-_rwanda.pdf.
[41] David Kezio-Musoke, "Twitter craze in Rwanda: myth or reality?" The Chronicles, January 31, 2012, http://the-chronicles.net/index.php/business/407-twitter-craze-in-rwanda-myth-or-reality.html.
[42] Dominique Nduhura, "Rwanda: Media Coverage of the Parliamentarian Elections (September 15, 2008)," paper presented at the World Journalism Education Congress, Grahamstown/Rhodes University, July 2010, http://wjec.ru.ac.za/index.php?option=com_rubberdoc&view=doc&id=96&format=raw.
[43] Tracey Wilen-Daugenti, "Technology 2012: Four tech trends to watch," The Christian Science Monitor, January 1, 2012, http://www.csmonitor.com/Business/2012/0101/Technology-2012-Four-tech-trends-to-watch/Mobile-technologies-in-2012-will-free-us-and-save-lives.

may be amended in the near future.[44] Article 56 of the law guarantees every person the right to create a website through which he or she can publish "information to a great number of people." Article 58 extends provisions of the law on print and audiovisual materials to ICT communications, stipulating a prohibition on censorship, on the one hand, and criminal penalties for showing contempt for the president, in addition to restrictions on certain coverage of the executive, judicial, and legislative branches, on the other. The extent to which the media should have the unchecked right to free expression is often a matter of public dispute in Rwanda, with some analysts suggesting that Rwanda's history of genocide should always guide media practitioners.[45]

While there are no laws that specifically restrict internet content or criminalize online expression, Rwanda's generally restrictive legal provisions governing traditional media could be applied to the internet, particularly given the lack of a fully independent judiciary. For example, the decision to ban the online version of *Umuvugizi* was based on charges of publishing "divisive language,"[46] a category of expression that is criminalized by the 2001 Law on Discrimination and Sectarianism.[47] Similarly, penalties for criminal defamation in print and broadcast media may be applicable to the internet, though these penalties have sparked complaints from media workers, prompting discussions about amendments.[48] As of early 2012, the penalties have not yet been agreed upon or amended; nevertheless, parliament has already reduced the length of the penalty for defamation, and it is expected that sooner or later defamation will be de-penalized altogether.[49]

Although many traditional journalists view the threat of imprisonment as a key constraint on their work, such punishment has been less common for online expression. One instance of imprisonment is known, that of Idesbald Byabuze, a Congolese journalist and professor based in Rwanda who was arrested in February 2007 and held in detention for one month while awaiting trial on charges of "segregation, sectarianism, and threatening national security" for several articles he had written. These included a June 2005 piece about human rights concerns in Rwanda that was published on an overseas website. The charges were

[44] "Law on Media," *Official Gazette of the Republic of Rwanda*, August 17, 2009, available at http://www.mhc.gov.rw/index.php?option=com_docman&task=cat_view&gid=81&Itemid=144&lang=en.
[45] Daniella Waddoup, "Press Freedom in Rwanda," Think Africa Press, February 18, 2011, http://thinkafricapress.com/rwanda/press-freedom-rwanda.
[46] Media Institute, "Tabloid Website Blocked," IFEX, June 8, 2010, http://ifex.org/rwanda/2010/06/08/umuvugizi_website_blocked/.
[47] Law No. 47/2001 on Prevention, Suppression and Punishment of the Crime of Discrimination and Sectarianism, http://www.adh-geneva.ch/RULAC/pdf_state/Law-47-2001-crime-discrimination-sectraianism.pdf; Jennie E. Burnet, "Rwanda," in *Countries at the Crossroads 2007* (New York: Freedom House; Lanham, MD: Rowman and Littlefield, 2007), http://freedomhouse.org/template.cfm?page=140&edition=8&ccrpage=37&ccrcountry=167.
[48] "Law on Media," *Official Gazette of the Republic of Rwanda.*
[49] "Media Practitioners Disagree on Press Freedom in Rwanda," November 16, 2011, Igihe.com, http://en.igihe.com/spip.php?article1134.

dropped after his release, but he was quickly deported from the country.[50] Since 2007, there have been no other reported cases of imprisonment for online expression, possibly because most activities by opposition forces are carried out in foreign countries. Nevertheless, intimidation tactics are becoming more common. In one case, the editor of *Umuvugizi*, Jean-Bosco Gasasira, who fled Rwanda in 2010 to operate the online version of the paper from abroad, was sentenced in June 2011 to two and a half years in prison in his absence.[51]

Government monitoring of online communications does not appear to be widespread; however, there have been several instances in recent years of emails, phone calls, and text messages being produced as evidence in trials. This was the case during the trial of opposition leader Victoire Ingabire in which emails and proof of money transfer to FDLR (French acronym for the Democratic Forces for the Liberation of Rwanda) rebels were used as evidence.[52] These were mostly obtained via low-tech methods of confiscating suspects' mobile phones and computers rather than via service providers.

There are no restrictions on anonymous communication online in Rwanda. In May 2011, however, RURA announced plans to implement SIM card registration to curb mobile phone crimes and increase security over mobile phone commerce. Under the registration scheme, subscribers will be required to provide the details on their identifications cards, which will be stored by the operator. As of May 2012, the SIM card registration process had only just begun.[53]

In a case that signaled the possibility of violence against print journalists creeping into the online sphere, in June 2010, Jean-Leonard Rugambage, an editor for *Umuvugizi*—the above-mentioned newspaper which was banned in April 2010 but continued to publish online—was assassinated in front of his home in Kigali. Rugambage was the last of the publication's journalists to remain in Rwanda and was reportedly preparing to join colleagues in exile due to threats and intimidation.[54] In November 2010, two individuals were convicted of the killing, claiming that it was a reprisal for acts of violence Rugambage allegedly committed during the 1994 genocide. However, fellow journalists expressed skepticism over the

[50] Bureau of Democracy, Human Rights, and Labor, "Rwanda," in *2007 Country Reports on Human Rights Practices* (Washington, DC: U.S. Department of State, March 2008), http://www.state.gov/g/drl/rls/hrrpt/2007/100499.htm; International Press Institute, "Democratic Republic of Congo," May 8, 2008, http://www.freemedia.at/regions/africa/singleview/4140/.
[51] Reporters Without Borders, "Rwanda," August 2011, accessed January 16, 2012, http://en.rsf.org/report-rwanda,38.html.
[52] Didas Gasana and Ann Garrison, "Ingabire trial: Rwanda prosecution fails 'evidence test,'" Rwandinfo_ENG (blog), accessed February 10, 2012, http://rwandinfo.com/eng/ingabire-trial-rwanda-prosecution-fails-evidence-test/.
[53] Dias Nyesiga, "Rwanda: Anxiety over Mobile Money Fraud," *The New Times*, May 22, 2012, http://allafrica.com/stories/201205220060.html.
[54] Danny O'Brien, "Six Stories: Online Journalists Killed in 2010," Committee to Protect Journalists (CPJ), December 17, 2010, http://cpj.org/internet/2010/12/online-journalists-killed-in-2010.php.

handling of the case, believing the murder was punishment for critical reporting on the government.[55]

Another grave instance of violence involved the killing of Charles Ingabire, an online editor and journalist based in Uganda, who was mysteriously shot dead in Kampala in December 2011. The website for which he wrote, Inyenyerinews.org, is known for publishing critical news of current Rwandan President Paul Kagame and his government. Prior to his murder in September 2011, Ingabire was beaten by unknown perpetrators and had his computer and phones stolen. Media watchdogs have blamed the killing on the Rwandan government, which has denied responsibility for the incident.[56]

There have been no reported cases of serious cyberattacks in the country,[57] though the Rwandan police has recently noted an increasing trend in cybercrime.[58] RURA has initiated a strategy to increase awareness of such threats among business owners and ordinary users.[59]

[55] "Journalists Killed in 2010: Jean-Léonard Rugambage," Committee to Protect Journalists (CPJ), June 26, 2010, http://cpj.org/killed/2010/jean-leonard-rugambage.php.
[56] Jennifer Fierberg, "Rwandese Journalists in Distress," MSW Salem-News.com, December 27, 2011, http://salem-news.com/articles/december272011/journalists-distress-jf.php?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Salem-news+%28Salem-News.com%29.
[57] James Karuhanga, "Rwanda: Police Warns Against Cyber Crime, Human Trafficking," The New Times, March 14, 2011, http://allafrica.com/stories/201103140486.html.
[58] 'Rwanda Police Warn of Hike in Cyber Crime," The New New Internet, March 15, 2011, http://www.thenewnewinternet.com/2011/03/15/rwanda-police-warn-of-hike-in-cyber-crime/.
[59] AimableKarangwa, *Cyber Security and CIIP* (Kigali: RURA, n.d.), slides, http://www.rura.gov.rw/publication/Cyber_Security_and_CIIP.pdf, November 22, 2010.

SAUDI ARABIA

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	14	14
Limits on Content (0-35)	27	26
Violations of User Rights (0-40)	29	31
Total (0-100)	**70**	**71**

* 0=most free, 100=least free

POPULATION: 29 million
INTERNET PENETRATION 2011: 48 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

While the recent wave of protests and demonstrations in the Kingdom of Saudi Arabia has not changed the political landscape in the country as in other Arab countries such as Tunisia, Egypt, and Libya, the internet freedom landscape in the Kingdom has no doubt changed considerably over the past year. Inspired by the Arab Spring events in 2011, millions of people in Saudi Arabia flooded social media sites such as Facebook, YouTube, and Twitter, and hundreds, if not thousands, participated in political campaigns to demand political, social, and economic reforms, fostering the emergence of innumerable political activists on social media.

However, as soon as Saudis went online to express their opinions, demand actions, and organize demonstrations, the Saudi government took immediate steps to respond to what it regarded as a national security threat. The government issued warnings banning protests, reminded people via email of the ban, and threatened the youth through the BlackBerry multi-media message service (MMS) to discourage them from participating in demonstrations. The authorities also detained and intimidated hundreds of online political activists and online commentators, implemented strict filtering mechanisms to block sensitive political content from entering the Saudi internet, recruited thousands of online supporters to warn against the call for protests and demonstrations as a counter measure, and continued to apply its excessive monitoring of internet users.

OBSTACLES TO ACCESS

Saudis first gained access to the internet in 1998. In 2011, 47.5 percent of the population had access to the internet, up from 19.5 percent in 2006, according to the International Telecommunication Union (ITU).[1] While in the early years, the vast majority of Saudi users accessed the internet through dial-up connections that were often slow and frustrating, less than 22.6 percent of the internet population still uses dial-up service today, with the rest using broadband connections.[2] There were 11.9 million mobile broadband connections and 2.2 million fixed broadband connections in the country as of May 2012.[3]

Internet penetration is highest in major cities such as Riyadh and Jeddah and in the oil-rich Eastern Province. Residents of provinces like Jizan in the south and Ha'il in the north are the least likely to use the internet. The younger generations make up the majority of the user population, according to the Communications and Information Commission (CITC).[4] Arabic content is widely available on the internet, as are Arabic versions of applications like chat rooms, discussion forums, and social media sites.

Monthly expenditure on broadband services ranges between 42 SAR (US$11) and 334 SAR (US$89) on average,[5] representing a sharp drop from the 2003 price of 700 SAR (US$187) a month.[6] That said, the cost of the internet is still considered high by the vast majority of those who participated in a CITC online survey who were predominantly male (95.3 percent) and between the ages of 20 and 39 (82.7 percent).[7]

Connection speed for broadband varies between 724 Kbps and 1.22 Mbps, depending on the service purchased (i.e. DSL broadband or High-Speed Packet Access networks). While the majority of participants in the CITC survey were not satisfied with their connection speeds[8] (possibly because of excessive filtering) and a large number of those surveyed

[1] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#. According to the latest statistics in 2012 by the Communications and Information Commission (CITC), there are 14.2 million internet users, for a penetration rate of 49.1 percent as of mid-2012. Internet Services Unit (ISU), "User's Survey," King Abdulaziz City for Science & Technology, 2006, accessed July 17, 2012, http://www.isu.net.sa/surveys-&-statistics/new-user-survey-results.htm.
[2] CITC, "ICT Indicators, Q1 – 2012."
[3] CITC, "ICT Indicators, Q1 – 2012."
[4] CITC, "The State of ICT Market Development in Saudi Arabia," Kingdom of Saudi Arabia, 2010, http://www.citc.gov.sa/English/Reportsandstudies/Studies/Documents/PL-PM-015-E-The%20State%20of%20ICT%20Market%20Development%20in%20Saudi%20Arabia.pdf.
[5] Ibid.
[6] ISU, "User's Survey."
[7] CITC, "The State of ICT Market Development in Saudi Arabia."
[8] Ibid.

planned to upgrade their internet speeds, overall infrastructure is not considered a barrier to access except in remote and sparsely populated areas.

The Saudi internet is connected to the international internet through two data-services providers, the Integrated Telecom Company and Bayanat al-Oula for Network Services, up from a single gateway in years past. These providers offer service to licensed internet service providers (ISPs), which in turn sell connections to dial-up and leased-line clients. The number of ISPs in the country has risen from 23 in 2005 to 36 in 2011.[9] Broadband and mobile phone services are provided by the three largest telecommunications companies in the Middle East: Saudi Telecom Company (Saudi Arabia), Etisalat (United Arab Emirates), and Zain (Kuwait). WiMAX, a technology that allows users to access the internet wirelessly from any location through a USB modem, is widely used in Saudi Arabia because it offers affordable prepaid broadband internet.

Saudis access the internet from home, from their place of employment, or in internet cafes, which offer a cost-effective alternative, though the latter option has become less popular because the availability of prepaid broadband has made it easier to access the internet from home, and internet cafes do not offer secure access. Many Saudis also access the internet from their mobile telephones. While there were fewer than 20 million mobile phone subscriptions only five years ago, there were nearly 54 million at the end of 2011, representing a penetration rate of over 191 percent.[10] Similarly, the average number of household mobile lines is estimated at 4.6 lines per household.[11]

All forms of internet and mobile phone access are available in the country, including WiMAX broadband, third-generation (3G), and fourth-generation (4G) mobile networks, internet via satellite, and High Speed Packet Access (HSPA) technologies. While smart phones like the iPhone and Galaxy tablets are banned at security organizations for fear of being targeted by hackers,[12] they are available to the public at affordable prices. Service for BlackBerry hand-held mobile devices, however, was banned from August 1-10, 2010 due to concerns over BlackBerry's encryption services,[13] but the ban was lifted after the company

[9] CITC, "Annual Report, 2011" [in Arabic], Kingdom of Saudi Arabia, 2012, http://www.citc.gov.sa/arabic/MediaCenter/Annualreport/Documents/PR_REP_007.pdf.
[10] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[11] CITC, "ICT Indicators 2011," Kingdom of Saudi Arabia, 2011, http://www.citc.gov.sa/English/Reportsandstudies/Indicators/Indicators%20of%20Communications%20and%20Information%20Techn/2011_ICT%20Indicators%20_English.pdf.
[12] "Saudi Arabia bans iPhones and Galaxy 'tablets' at security organizations," Al-Arabiya, July 15, 2011, http://english.alarabiya.net/articles/2011/07/15/157742.html.
[13] "Saudi Ban on BlackBerry from Friday," Al-Jazeera, August 4, 2010, http://english.aljazeera.net/news/middleeast/2010/08/2010844243386999.html.

agreed to provide the Saudi authorities with the means to access the devices' encrypted messages.[14]

Major video-sharing, social-networking, and micro-blogging sites like YouTube, Facebook, and Twitter are freely available, as are international blog-hosting services. However, specific pages particularly on social media sites like YouTube, Facebook and Twitter are instantly blocked if they contain sensitive political content or call for people to join political campaigns and movements. One example is the "Constitutional Monarchy" page on Facebook, which was founded on March 5, 2011 by Ali Ashmlan and presumably blocked because it called for constitutional monarchy in the Kingdom, a taboo subject in Saudi Arabia. Another example is the Facebook page, "I want my rights…I don't want to drive," which called for reforms in public transportation for women to use instead of driving. The page was blocked for unknown reasons, according to Maha Al-Hadlaq, one of the group's members.[15]

Nevertheless, Saudis are among the largest adopters of Twitter in the Arab world, with 38 percent of all Arab tweets coming from Saudi Arabia.[16] Saudis are also well-represented on Facebook, with 4.9 million users and a penetration rate of 19.1 percent as of early 2012.[17] Similarly, millions of Saudis visit YouTube on a regular basis for alternative information on the country's current affairs that differs from official media.

The Internet Services Unit (ISU), a department of King Abdulaziz City for Science & Technology (KACST), is responsible for managing the internet infrastructure in Saudi Arabia and reports to the Vice President for Scientific Research Support. All retail ISPs, government organizations, and universities obtain access through the ISU. Established in 1998, the ISU initially acted as a regulatory body, but governance of the Saudi internet, including licensing issues, was relegated to the CITC in 2003. In addition to providing access to the internet, the CITC is responsible for regulating the broader information and communication technology (ICT) sector in the country.

[14] Reuters, "BlackBerry Agrees to Give Saudi Arabia Subscribers' Codes" [in Arabic], Al-Arabiya, August 10, 2010, http://www.alarabiya.net/articles/2010/08/10/116289.html.
[15] "Saudiat Atrhan national project an alternative to women driving a car" [in Arabic], AlAnba, June 23, 2011, http://www.alanba.com.kw/absolutenmnew/templates/print-article.aspx?articleid=206784&zoneid=194.
[16] "Saudis the biggest adopters of Twitter in the Arab world" [in Arabic], Sabq, January 25, 2012, http://sabq.org/dlbfde.
[17] "Facebook Statistics by country," Socialbakers, accessed February 6, 2012, http://www.socialbakers.com/facebook-statistics/?interval=last-week#chart-intervals.

LIMITS ON CONTENT

The Saudi government employs strict filtering over internet content, tightening its grip in 2011 and early 2012 following the revolutions in Tunisia, Egypt, Libya, Yemen, and Syria due to fears of a revolution erupting in its own backyard. For this reason, specific pages particularly on social media sites such as YouTube, Facebook and Twitter that called for protests, demonstrations, or the release of prisoners were quickly blocked throughout 2011. Pages that demanded political, social, or economic reforms or basic human or civil rights were also blocked. More generally, sites that contain "harmful," "illegal," "anti-Islamic," or "offensive" material are routinely blocked, as are those that carry criticism of Saudi Arabia, the royal family, or other Gulf States. Material providing information about drugs, alcohol, gambling, or terrorism, and sites that call for political reform or that are critical of the current political landscape, are also regularly blocked.

While the rules governing internet usage are stated on government websites, allowing internet users to discern what is expected of them, the government blocking has become increasingly erratic. The OpenNet Initiative's most recent testing results showed that Saudi Arabia also blocks human rights websites like Article19.org, Saudihr.org, and Hummum.net.[18] In 2011, Saudi Arabia blocked the Amnesty International website because it leaked a draft of the proposed anti-terrorism law.[19] Saudi Arabia also blocks the websites of the human rights organizations, Reporters without Borders and Freedom House, as well as the websites of several Saudi religious scholars.[20] The country's two data service providers must block the sites banned by the CITC,[21] and failure to abide by these bans may subject the service providers to a fine of up to 5 million SAR (US$1.33 million), according to Article 38 of the Saudi Telecommunication Act.[22]

Filtering in Saudi Arabia takes place at the country-level servers of the two data service providers. These servers, which contain long lists of blocked sites, are placed between the state-owned internet backbone and servers around the world. All user requests that arrive via Saudi ISPs travel through these servers, where they can be filtered and possibly blocked. Users who attempt to access a banned site are redirected to a page displaying the message, "Access to the requested URL is not allowed!" demonstrating the government's partial

[18] "Country Profile: Saudi Arabia," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/saudi-arabia.
[19] Jane Abell, "Saudi Government Blocks Amnesty International's Website," OpenNet Initiative, July 26, 2011, http://opennet.net/blog/2011/07/saudi-government-blocks-amnesty-international%E2%80%99s-website.
[20] Blocked websites of Saudi religious scholars include: www.almoslim.net, www.albrrak.net, and islamqa.info/ar. "Blocking some sites because they violate rules and spread bold ideas and theses" [in Arabic], AlArabiya.net, April 6, 2012, http://www.alarabiya.net/articles/2012/04/06/205754.html.
[21] CITC, "General Information on Filtering Service," accessed September 30, 2010, http://www.internet.gov.sa/learn-the-web/guides/content-filtering-in-saudi-arabia.
[22] Telecommunication Act found here [in Arabic]: http://www.citc.gov.sa/arabic/RulesandSystems/CITCSyste/Documents/LA_001_%20A_Telecom%20Act.pdf.

transparency about the content it blocks, but the list of banned sites is not publicly available. The government also responds to take down notices from members of the public, who can alert the government to undesirable material,[23] and sites can be unblocked through a similar system designated for this purpose.[24] Once an individual submits a request to unblock a site by completing a web-based form, a team of CITC employees determines whether the request is justified. The manager of public relations at the CITC said the commission receives about 200 of such requests each day, but he would not comment on how often the CITC unblocks a site based on an appeal.[25]

The CITC claims that the time lost determining whether a user's site request should be blocked or allowed is not more than half a second. However, a survey conducted by the Commission in 2008 showed that 33 percent of internet users in the country, particularly younger participants and women, found content filtering problematic.[26] These users complained that filtering denied them access to a great deal of useful information and limited their ability to browse freely.

In addition to the blocking and filtering of websites, specific content on webpages is also subject to removal. For example, at least three YouTube episodes—two from the "Sa7i" channel[27] and one from the "3al6ayer"[28] channel—were removed because the videos' critical content had ostensibly crossed the "red lines." These limitations are in addition to the work of online forum moderators, or "gate-keepers," who preemptively delete content they deem inappropriate or inconsistent with the norms of society.

The Saudi blogosphere is not as active as other online platforms for political discussion in the country. For example, while there are an estimated 10,000 Saudi bloggers, most Saudis use online public discussion forums, YouTube, Facebook, and Twitter to engage in political conversations. There are more female than male bloggers in Saudi Arabia, and most bloggers tend to focus on personal matters rather than local politics. With that said, some blogs in Saudi Arabia have become instrumental in shaping the political landscape in the country.

---

[23] The CITC block-request form is available at http://www.internet.gov.sa/resources/block-unblock-request/block/view?set_language=en.
[24] The CITC unblock request form is available at http://www.internet.gov.sa/resources/block-unblock-request/unblock/.
[25] "About 300,000 requests to block sites in Saudi Arabia annually" [in Arabic], Ajl.com.sa, January 13, 2010, http://www.burnews.com/news-action-show-id-12100.htm.
[26] CITC, "Chapter 1: Individual," *Computer and Internet Usage in the Kingdom of Saudi Arabia* (Riyadh: Kingdom of Saudi Arabia, 2009), 6-10.
[27] "Sa7i" channel, http://sa7i.com/shows/%D9%8A%D8%B7%D8%A8%D8%B9%D9%88%D9%86/%D9%8A%D8%B7%D8%A8%D8%B9%D9%88%D9%865?ctl00_phContent_gvItemsChangePage=2; Sa7ichannel, Twitter post, March 12, 2012, 8:17pm, https://twitter.com/Sa7ichannel/statuses/182682472453128192.
[28] "Idaat with Turki Al Dakheel" [in Arabic], AlArabiya.net, May 18, 2012, http://www.alarabiya.net/programs/2012/05/18/214916.html.

Internet users in Saudi Arabia, particularly those who upload humorous yet critical videos on YouTube, practice self-censorship online, which is often out of fear of "getting into trouble with the authorities," as the owner of the "3al6ayer" YouTube channel alluded to during an interview with the AlArabiya satellite station.[29] However, self-censorship is exercised mainly to avoid crossing red lines, thus it is possible to enjoy a modicum of freedom of expression online as long as the red lines are not crossed.

Another strategy the government employs to manufacture consent about its image is by being very active in online public discussion forums. The government also influences the news reported online by offering financial support to news sites such as Sabq.org in return for coordination between a site editor and the authorities. Blocking an online source from inside the country and thereby limiting the chances of making revenue from advertisements has also proven effective, as revealed by the owners of Al-Saha al-Siyasia who decided to close its website after 15 years in operation because of the block by Saudi authorities, which according to the owners, resulted in their financial ruin.[30]

Online public discussion forums enjoy immense popularity and receive unmatched attention from the public. Their effect on the political sphere has continued to be significant, even after the emergence of social media sites and blog-hosting applications. The forums give ordinary individuals from all backgrounds the opportunity to express themselves, steer the government's attention to their problems, and get their messages across even to the country's leadership. It is believed that the King responds swiftly to some of the demands made by online commentators and takes serious steps to meet those demands. For example, some of the decisions relating to the latest economic reforms, such as the recently introduced 2,000 SAR (US$533) monthly stipend for the unemployed,[31] may have been inspired by requests from members of Al-Saha al-Siyasia, the most popular online political forum in Saudi Arabia that is often read by the government to gauge public opinion or feel the pulse of the people. Nevertheless, Al-Saha al-Siyasia is not accessible from inside Saudi Arabia because of the sensitive nature of the topics discussed on it. Many Saudi internet users have become savvy at using circumvention tools such as Hotspot Shield,[32] which allows users to access a virtual private network (VPN) to bypass the proxies that block websites. Nevertheless, the blocked sites mean a great deal to many Saudis due to the dearth of other channels for free expression.

Social-networking sites like YouTube, Facebook and Twitter provide additional media platforms with minimal government control. For example, Saudis used YouTube very

[29] Ibid.
[30] "The end: Alsaha says good bye" [in Arabic], Alsaha.com, June 28, 2012, http://www.alsaha.com/sahat/17/topics/303703.
[31] This welfare scheme, which was introduced in early 2011, is called Hafiz.
[32] Saudis call this circumvention tool, "proxy breaker."

effectively during the second major floods in Jeddah in 2011 that had resulted in several deaths. Users not only posted hundreds of videos capturing the tragedy as it occurred, but also demanded action from the authorities. In response, the King ordered immediate financial compensation for the flood victims.[33] The action was viewed as significant because it is not common in Saudi society to accept responsibility for natural disasters, which are believed to be coming from Allah. While YouTube was credited with exposing the gravity of the floods, many Saudis used Facebook to organize and assist with the rescue efforts, taking an important step toward greater civic and political activism in the country.

There are also Facebook groups that organize protests and demonstrations such as the "Hunain Revolution" page, which called for demonstrations in March 2011 that unfortunately failed to trigger a true revolution. Other Facebook pages include, "the National Campaign for Social Justice," "No Injustice After Today," and "Sit-in of 21/1/1433 H." The latter two Facebook groups organized country-wide sit-ins on February 23, 2012, though they had little effect because only a few people showed up to participate.

VIOLATIONS OF USER RIGHTS

Saudi Arabia's basic law contains language that provides for freedom of speech and freedom of the press, but only within certain boundaries. The 2000 Law of Print and Press addresses freedom of expression issues, but it largely consists of restrictions rather than protections. The government treats online journalists writing for newspapers and other formal news outlets the same as print and broadcast journalists, subjecting them to close supervision. Bloggers and online commentators who write under pseudonyms face special scrutiny from the authorities who attempt to identify and punish them for critical or controversial remarks. Online writers are often arrested and detained without specific charges, though it is frequently clear which views offend the government. The Ministry of Interior has generally enjoyed impunity for abuses against bloggers and online commentators.

In response to a series of hacking attacks, including one on the Ministry of Labor in 2008,[34] the government has enacted laws that criminalize a range of internet-based offenses. The vaguely worded legislation assigns jail sentences and fines for defamation; unauthorized interception of private email messages; hacking a website to deface, destroy, modify, or deny access to it; or simply publishing or accessing data that is "contrary to the state or its system." In addition, the Ministry of Culture and Information issued new legislation in

[33] Yahya Hujairi, "An open financial account to cash all checks made for Jeddah flood victims" [in Arabic], AlEqt, February 19, 2011, http://www.aleqt.com/2011/02/19/article_505872.html.
[34] "Unemployed Man Hacks into Ministry of Labor and Parliament and Asks Private Sector to Employ Him" [in Arabic], *Al-Madina*, September 3, 2008.

January 2011 requesting all bloggers, among others, to obtain a license from the Ministry to operate online,[35] thus putting more pressure on political activists to self-regulate their content.

Many online commentators have been imprisoned under these laws after criticizing senior government officials or high profile members of the Royal Family. For example, when blogger Feras Bughnah produced a video describing poverty in Riyadh and uploaded it onto YouTube, he was instantly detained along with his colleagues Hosam al-Deraiwish and Khaled al-Rasheed.[36] The video was a part of a critical journalism series on YouTube called "Maloob Alaina" ("We have been cheated") and had been viewed 1.7 million times by the end of 2011. Feras and his colleagues were released after a couple of weeks in detention.[37]

Nevertheless, the success of humorous yet critical YouTube channels that mushroomed in 2011 indicates that there is room, within certain limits, for free speech in Saudi Arabia. There are now numerous comic channels on YouTube that use humor to address sensitive issues, including "3al6ayer," "La Yekthar," "Quarter to Nine," "Sa7i," "Masameer," "Eysh Elly," "Fe2aFala," and "Hajma Mortadda." One of the episodes on "La Yekthar" has received three million views, and many others have received up to two million views, suggesting that these channels enjoy widespread popularity. One reason for the success of these videos is their engagement in cautious rather than harsh criticism and their restraint against pushing the limits too far. While there have been no reports of arrests of anyone associated with the YouTube channels, at least three YouTube episodes were removed because the criticism crossed the red lines, as mentioned above.

On the other hand, while the government has seemed to tolerate the cautiously humorous form of critical journalism, critical journalism that broaches taboo issues such as encouraging women to drive are not tolerated. This issue came to bear in May 2011 when Manal al-Sharif posted a video of her driving on YouTube as part of a campaign to encourage women to get behind the wheel. She was consequently detained the next day[38] but released after ten days, likely as a result of the considerable attention she attracted worldwide.

Public vilification is still common in the country, despite the enactment of new legislation by the Ministry of Culture and Information that was specifically designed to curb defamation and libel. For example, at the end of the 2nd Intellectual Forum held in Riyadh in late

[35] "Internet Enemies, Saudi Arabia," Reporters Without Borders, 2012, http://en.rsf.org/internet-enemie-saudi-arabia,39745.html.
[36] Amelia Hill, "Saudi film-makers enter second week of detention," The Guardian, October 23, 2011, http://www.guardian.co.uk/world/2011/oct/23/feras-boqna-saudi-arabia-poverty.
[37] Ayman Badhman, "Maloob Alaina team has been released after their detention couple of weeks ago" [in Arabic], Sabq, October 30, 2011, http://sabq.org/UYZede.
[38] Siraj Wahab, "Manal Al-Sharif released," Arab News, May 31, 2011, http://arabnews.com/saudiarabia/article442275.ece.

December 2011, the attendee Saleh Al-Shehi tweeted that the widespread interaction he observed between male and female participants at the forum brought shame and dishonor to the culture, hinting that the event was about networking with women. His comment led to clashes among journalists and intellectuals on Twitter,[39] to the extent that the Grand Mufti during a Friday sermon criticized the site and accused it of facilitating the spread of lies. Nevertheless, no complaint was lodged against Saleh Al-Shehi in this instance. Later, Al-Shehi criticized the Saudi Finance Minister, who subsequently lodged a complaint against Al-Shehi at the Ministry of Culture and Information and won, requiring Al-Shehi to pay a 20,000 SAR (US$5,333) fine.[40] By contrast, no action was taken against an anonymous Twitter user under the nickname "Mujtahidd" when he/she launched a scathing attack on the high profile members of the Royal Family, providing very detailed descriptions of their corruption.[41] Nevertheless, it is believed that Mujtahidd is based outside the country since the government could have easily arrested him if he was writing from within Saudi Arabia. Mujtahidd has now more than 400,000 Twitter followers.

Online commentators who express support for extremism or liberal ideals, call for strikes, protests or demonstrations, argue in favor of the rights of Shiites and other minorities, call for political reform, or expose human rights violations are perceived as threats by the government. Although data on the exact number of those arrested is not publicly available, the Facebook groups that call for the release of political prisoners list hundreds of names of political activists in prison. Most of these Facebook groups emerged in 2011 after the success of the Arab Spring and include "National Campaign for Supporting Detainees in Saudi Arabia" and "Prisoner Until When?" demonstrating the increased engagement in civic and political activism in the country.

Surveillance is rampant in Saudi Arabia. Anyone who uses communication technology is subject to government monitoring, which is officially justified under the auspices of protecting national security and maintaining social order. The authorities regularly monitor websites, blogs, chat rooms, social media sites, and the content of email and mobile phone text messages. Users are not able to purchase mobile phones anonymously and are legally required to use their real names or register with the government. Furthermore, the authorities can obtain identification data from service providers without a court order or legal process.

[39] MD Al-Sulami, "Intellectuals clash on Twitter," Arab News, January 1, 2012, http://www.arabnews.com/node/402740.
[40] "Ministry of Culture and Information judges in favor of the Minister Al Assaf against the journalist Al-Shehi" [in Arabic], Sabq.org, February 2, 2012, http://sabq.org/DWcfde.
[41] Roula Khalaf, "Daring Saudi tweets fuel political debate," Financial Times, March 16, 2012, http://www.ft.com/cms/s/0/1749888e-6f5e-11e1-b368-00144feab49a.html.

The short-lived ban on BlackBerry services in August 2010, which ended when the government obtained the means to access the devices' encrypted messages, suggested that all other electronic media were already under the watchful eye of the authorities.[42] Moreover, the blocking of hundreds, if not thousands of YouTube channels, and Facebook and Twitter pages of human rights and political activists demonstrates the government's diligence in restricting content. The arrests of hundreds of human rights and political activists in 2011 are also indicative of the government's effective ability to monitor the Saudi internet.

In addition to direct government monitoring, access providers are required to monitor their customers and supply the authorities with information about their online activities. On April 16, 2009, the Ministry of Interior made it mandatory for internet cafes to install hidden cameras and provide identity records of their customers. The new security regulations also barred anyone under 18 years of age from using internet cafes. All internet cafes were ordered to close by midnight, and police were instructed to visit the businesses to ensure compliance. These measures were ostensibly designed to crack down on internet use by extremists, but in practice, they allow the police to deter any activity that the government may find objectionable such as calling for protests.

While in 2010, the authorities mainly targeted and arrested alleged extremists for their participation in online forums, in 2011, the attention and arrests shifted to human rights and political activists who the government feared would instigate an Arab Spring revolution in the country. The Ministry of Interior is believed to be the main government body responsible for monitoring extremist and political activists' content. The resulting arrests without formal charges have meant that detainees cannot defend themselves or secure legal representation. Some online commentators have reported that the authorities confiscated their computers and never returned them.

In 2011, the Ministry of Interior arrested several political activists and bloggers, including Fadhel Makki Al Manasif, Muhammed Salih Al Bijadi, and Mukhlif bin Khulaif bin Dahham AlShammari.[43] As of May 2012, Al Manasif and Al Bijadi were still in prison, while AlShammari was temporarily released and awaiting trial. Saudi Arabian authorities also detained Hamza Kashgari, a young Saudi writer, whose arrest was ordered by the King himself after Kashgari made several offensive comments on Twitter about the Prophet Mohammed. His tweets caused a huge uproar on social media and made thousands call for his execution, prompting him to flee the country to Malaysia. However, he was arrested at

[42] Souhail Karam and Asma Alsharif, "RIM to share some BlackBerry codes to Saudis: source," Reuters, August 10, 2010, http://www.reuters.com/article/2010/08/10/us-blackberry-saudi-idUSTRE6751Q220100810.
[43] Adala Centre for Human Rights, *Freedom in Shackles*, May 2012, http://www.adalacenter.net/index.php?ext=1&act=media&code=books&f=72.

the Malaysian airport and later extradited to Saudi Arabia where he is still in prison as of May 2012.

Several websites and portals have been subject to cyberattacks in recent years including the official website of the Saudi Ministry of Finance.[44] In addition, hackers attacked the Facebook and Twitter pages of the satellite television station Al-Arabiya on April 24, 2012.[45] Even high-profile journalists' pages on Twitter, like Abdu Khal's, have been hacked.[46]

[44] "Harsh punishment awaits Saudi Hackers" [in Arabic], AlArabiya.net, April 25, 2012, http://www.alarabiya.net/articles/2012/04/25/210117.html.
[45] "'AlArabiya' retrieves its hacked accounts on Facebook and Twitter" [in Arabic], AlArabiya.net, April 24, 2012, http://www.alarabiya.net/articles/2012/04/24/209849.html.
[46] "The Saudi journalist Abdu Khal page on Twitter were hacked" [in Arabic], AlArabiya.net, April 16, 2012, http://www.alarabiya.net/articles/2012/04/16/208214.html.

SOUTH AFRICA

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	7	8
Limits on Content (0-35)	9	8
Violations of User Rights (0-40)	10	10
Total (0-100)	**26**	**26**

* 0=most free, 100=least free

POPULATION: 51 million
INTERNET PENETRATION 2011: 21 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Digital media freedom is generally respected in South Africa. Political content is not censored, and bloggers and online content creators are not prosecuted for online activities. Nevertheless, the status of South Africa's internet freedom was threatened by two pieces of proposed legislation in 2011—the General Intelligence Laws Amendment Bill, which could potentially legalize the bulk monitoring of internet communications, and the Protection of State Information Bill, which would make it illegal to publish and access certain state information, affecting the traditional and digital media, bloggers, and internet users.

Access to the internet has improved, and more people have the option to access the internet from their mobile phones than from computers. Nevertheless, the majority of South Africans are unable to benefit from internet access due to high costs and the fact that most content is in English—an obstacle for those who speak one of the ten other official languages—although there is now content in some local languages, especially on social-networking platforms.

The first internet connection in South Africa was established in 1988, and the internet was commercialized in 1993. By the mid-1990s, South Africa ranked higher in internet usage than other countries at comparable levels of development. Today, however, South Africa ranks lower than some countries with similar or lower levels of human development or gross domestic product (GDP) per capita,[1] and South Africa is the thirteenth most

[1] For example, South Africa has 12.3 internet users per 100 inhabitants compared to 27.56 in Vietnam. South Africa is 123rd on the Human Development Index (HDI) for 2011 and Vietnam is 128th. Azerbaijan, Macedonia, Montenegro and Serbia (with

connected country in Africa in terms of internet penetration.[2] Kenya—a country with one-sixth of South Africa's GDP per capita and ten countries below it on the Human Development Index—has twice the number of internet users as South Africa.[3] According to many analysts, this relative decline has been attributed to the state's failed policy of managed liberalization which sought to "preserve a central role for state-owned operators in the sector and state shareholding in private companies, while gradually liberalizing the market over a period of time,"[4] as well as "a decade-long period of policy and regulatory paralysis" in the information and communications technology (ICT) sector "in which decision-making and administrative justice were ultimately abdicated to the courts."[5]

OBSTACLES TO ACCESS

By the end of 2011, 21 percent of the South African population had access to the internet,[6] up from 7.6 percent in 2006.[7] Due to the high costs of access, infrastructural limitations, and waiting periods for line installation and ADSL access in some areas, the majority of users access the internet from mobile phones or from internet cafes. In 2011, there were only 1.8 fixed-line ADSL connections per 100 inhabitants, up from 1.3 percent in 2010.[8] Those with access, especially broadband access, are concentrated in urban areas. Although the overall figures remain very low,[9] the number of South Africans accessing the internet through broadband connections grew by more than 50 percent in 2009, and wireless broadband

similar GDP per capita to South Africa) have between 42.9 and 52.4 internet users per 100 inhabitants. This is according to the International Telecommunication Union data for 2010 (http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx) and World Bank and IMF GDP PPP per capita data (http://en.wikipedia.org/wiki/List_of_countries_by_GDP_%28PPP%29_per_capita).

[2] The countries above South Africa in terms of internet users per 100 inhabitants are in descending order are: Morocco, Seychelles, Tunisia, Cape Verde, Nigeria, Mauritius, Egypt, Kenya, Sao Tomé and Principe, Libya, Rwanda, and Uganda.

[3] Kenya which is 143rd on the HDI had 25.9 as internet users per 100 inhabitants in 2010, South Africa had 12.3,

[4] Alison Gillwald, "Between two stools: Broadband policy in South Africa," *The Southern African Journal of Information and Communication* 8, 2007.

[5] Alison Gillwald, "SA fails test of network society," TechCentral, October 12, 2011, http://www.techcentral.co.za/sa-fails-test-of-network-society/26628/.

[6] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[7] Data is from the International Telecommunication Union (ITU), 2010. Another measure of internet usage could be the South African Advertising Research Foundation's all media product survey June 2011, which estimates that 10.54 percent of adults had used the internet in the last day, 15 percent in the past week, and 20.3 percent in the last month. South African Advertising Research Foundation, "AMPS Trended Media Data: Cellphone Trends," accessed March 11, 2012, http://www.saarf.co.za/amps/cellphone.asp.

[8] ITU, "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011.

[9] South Africa currently has a broadband penetration of 4 connections per 100 inhabitants. See "SA's broadband penetration: the way forward," MyBroadband, October 13, 2010, http://mybroadband.co.za/news/broadband/15804-SAs-broadband-penetration-The-way-forward.html.

access grew by 88 percent in the same period.[10] This growth has been attributed to the granting of Electronic Communications Network Service (ECNS) licenses to more than 400 organizations since a landmark August 2008 court ruling that value-added network service (VANS) providers can self-provide facilities.[11] Other positive factors include falling costs due to the arrival of the Seacom and the East African Submarine System (Eassy) undersea cables, the increasing use of updated mobile phone technology, and the laying of new fiber-optic cables within and between cities.[12]

After years of stifled competition, the market is slowly opening up. In March 2010, the internet service provider (ISP) M-Web launched an uncapped ADSL offering, unleashing a price war in the ADSL market.[13] The price war is projected to be more obvious in 2012, and its real impact is expected by 2013.[14] However, prices are still beyond the reach of the majority of the population, especially for users of prepaid services.

Fixed-line broadband (ADSL) is prohibitively expensive, with 1 gigabyte (GB) of data at 384 Kbps available for 306 rand (approximately US$37).[15] The cheapest unlimited 4 Mbps connection would cost 971 rand (approximately US$118).[16] Some mobile broadband packages offering small amounts of data are cheaper than the fixed-line alternatives. The cheapest prepaid mobile data packages are 40 rand (US$5) for 100 MB, 120 rand (US$15) for 500 MB, and 266 rand (US$32) for 2 GB.[17] A report by telecom research firm Ovum in 2011 found that South Africa had the most expensive broadband tariffs of 19 sampled emerging market countries.[18] South Africa also lags behind other countries in terms of

[10] "Broadband Speeding Ahead," World Wide Worx, news release, March 17, 2010, http://www.worldwideworx.com/archives/243.
[11] "SA Internet Growth Accelerates," World Wide Worx, news release, January 14, 2010, http://www.worldwideworx.com/archives/234.
[12] Candice Jones, "More Bandwidth Coming," ITWeb, March 30, 2010, http://www.itweb.co.za/index.php?option=com_content&view=article&id=31713:more-bandwidth-incoming&catid=147&Itemid=68.
[13] Candice Jones, "Another Salvo in Broadband War," ITWeb, May 5, 2010, http://www.itweb.co.za/index.php?option=com_content&view=article&id=32837:another-salvo-in-broadband-war&catid=147&Itemid=68.
[14] Simon Dingle, "The broadband backslide," FinWeek, February 9 2012.
[15] This package is from AXXESS (http://www.axxess.co.za) and is R15 per GB but includes 384 kbps circuit rental of R 152 as well as mandatory fixed-line rental from Telkom for R 139.97). South Africans do not currently have the option to have "naked ADSL" – that is ADSL without paying a fee for a voice line rental. Prices are from May 4, 2012.
[16] The speed would not be fully unthrottled for this option and would be "shaped," meaning that certain services or content would be slowed down. Mandatory line rental and 4 Mbps circuit rental of R139.97 and R 413 respectively are included in the price. The package is offered by Propertiere. The price was obtained from http://www.hellkom.co.za.
[17] These prepaid data bundles are from the mobile operator 8ta, which is owned by the fixed-line incumbent Telkom. Prices are from http://www.8ta.com/plans/prepaid-data/.
[18] Ovum, "Broadband Pricing in Emerging Markets in 2011," cited in Nicola Mawson, "SA's broadband most expensive," ITWeb, August 10, 2011, http://www.itweb.co.za/index.php?option=com_content&view=article&id=46078:sas-broadband-most-expensive&catid=260.

broadband speed. According to one study, South Africa is sixth in Africa for average download speeds and ranks 107th out of 174 countries measured.[19]

Less than half of urban mobile users who have internet-enabled phones actually use the internet on their phones, and those who do use internet capabilities focus on specific applications like the Mxit instant-messaging service and Facebook Mobile rather than regular browsing.[20] It is estimated that 81.8 percent of the population are mobile phone users as of December 2011, with 73.3 percent of the population using prepaid mobile services, according to the South African Advertising Research Foundation.[21] The latest ITU data notes 64 million mobile phone subscriptions in 2011, amounting to a penetration rate of nearly 127 percent.[22]

Telkom SA, a partly stated-owned company, retains a monopoly in the market for broadband access via ADSL. ADSL packages are only available through Telkom lines. Although there is competition in the ADSL market and users can choose from hundreds of ISPs, ADSL connections and telephone lines are rented from Telkom. Currently, subscribers cannot enjoy their ADSL "naked"—i.e. without also paying for voice service. Additionally, ISPs selling ADSL access need to pay Telkom charges for its IP Connect service for access to its exchanges.[23] On March 31, 2012, the Independent Communications Authority of South Africa (ICASA) regulatory body enforced a 30 percent reduction in IP Connect prices that is expected to help in lowering ADSL prices.[24]

It was hoped that the licensing of a second national operator in 2006, Neotel, would increase competition. Neotel, however, does not offer ADSL but only fixed-wireless and mobile internet packages. There are five mobile phone companies in South Africa—Vodacom, MTN, Cell-C, Virgin Mobile and 8ta—all of which are privately owned except for 8ta, which is owned by Telkom. The state previously owned a stake in Vodacom through Telkom, but the shares have since been relinquished.

---

[19] Simon Dingle, "The broadband backslide," FinWeek, February 9 2012.

[20] "Mobile Internet Booms in SA," World Wide Worx, news release, May 27, 2010, http://www.worldwideworx.com/archives/250.

[21] "AMPS Trended Media Data: Cellphone Trends," South African Advertising Research Foundation, accessed July 13, 2012, http://www.saarf.co.za/amps/cellphone.asp.

[22] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[23] Gareth Vorster, "Telkom charging twice for the same product," BusinessTech, March 6 2012, http://businesstech.co.za/news/internet/7307/telkom-charging-twice-for-the-same-product/. Weoma Wright, CEO of the ISP OpenWeb said that, "As everyone is aware, the cost of the IPConnect service is the single most expensive ingredient in the make-up of ADSL. If Telkom cut the cost of their IPConnect link by only 50 percent per month, ISP's would be able to instantly offer a less contended service that costs less."

[24] Larry Claasen, "Icasa brings prices down," Financial Mail, April 19, 2012 http://www.fm.co.za/Article.aspx?id=169993; Bonnie Tubbs, "IPC cut encourages ADSL promos," ITWeb, April 11, 2012, http://www.itweb.co.za/index.php?view=article&id=53403.

Pursuant to Section 27(A)1 of the Electronic Communications Act, ISPs and internet cafes are required to register with the Film and Publications board, which falls under the Department of Home Affairs and is a relic (albeit a reformed one) of the Apartheid publication censorship regime.

The autonomy of the regulatory body, ICASA, is protected by the South African constitution, although several incidents involving ministerial policy directives sent to the regulator have called the extent of its independence into question.[25] In 2008, after a landmark ruling that mandated the implementation of existing legislation and regulations allowing VANS providers to self-provide communications facilities, the Minister at the time tried unsuccessfully to take ICASA to court to prevent it from granting an updated ECNS license to Alltech, a VANS company.[26] ICASA has also been criticized by operators for delays in the allocation of 4G mobile spectrum and local loop unbundling.[27] In November 2011, the regulator announced that it had completed its local loop unbundling study and was ready to begin implementing the process. Meanwhile, Minister of Communications Dina Pule announced that to the contrary, ICASA had not begun its study and was not ready to begin the implementation of local loop unbundling, which led some to question the independence of ICASA in these processes.[28]

A proposed ICASA Act amendment introduced as a bill to parliament in 2010 aimed to limit the independence of the ICASA by requiring the CEO of ICASA to approach parliament through the Minister of Communications, rather than directly. The initial bill was withdrawn in November 2011, and a revised draft will be introduced to parliament in 2012.[29] In November 2011, the government proposed amendments to the Electronic Communications Act that would transfer the ICASA's power over spectrum management to the Minister of Communications, going against worldwide trends of spectrum management being delegated to regulators.[30] Nevertheless, access providers and other internet-related groups are self-organized and quite active in lobbying the government for better legislation and regulations, including measures that would upgrade the independence and capacity of ICASA.

[25] Open Society Initiative for Southern Africa, *South Africa*, Public Broadcasting in Africa Series (Johannesburg: Open Society Initiative for Southern Africa, 2010).
[26] Belinda Anderson, "Ivy takes ICASA to court," Fin24, October 20, 2008, http://www.fin24.com/Business/Ivy-takes-Icasa-to-court-20081019.
[27] "MTN warns of "regulatory failure," Tech Central, March 2, 2012, http://www.techcentral.co.za/mtn-warns-of-regulatory-failure/29927/.
[28] Randolph Muller, "LLU: get ready to lose your cool," MyBroadband, February 14, 2012, http://mybroadband.co.za/news/telecoms/43089-llu-get-ready-to-lose-your-cool.html.
[29] "Icasa Amendment Bill under fire," Tech Central, March 7 2010, http://www.techcentral.co.za/icasa-amendment-bill-under-fire/15353/; Nicola Mawson, "DOC to issue amendment Acts," ITweb, February 28, 2012, http://www.itweb.co.za/index.php?option=com_content&view=article&id=52046:doc-to-issue-amendment-acts.
[30] "More criticism of telecom law amendments," Tech Central, November 15, 2011.

LIMITS ON CONTENT

While internet content remains free of government censorship, a 2009 amendment to the Films and Publications Act of 1996 has raised concerns that certain types of controversial content could be restricted. The amendment requires that every print and online publication that is not a recognized newspaper be submitted for classification to the government-controlled Film and Publications Board[31] if it includes depictions of "sexual conduct which violates or shows disrespect for the right to dignity of any person, degrades a person, or constitutes incitement to cause harm; advocates propaganda for war; incites violence; or advocates hatred based on any identifiable group characteristic and that constitutes incitement to cause harm." Exemptions are provided for artistic and scientific speech, but the board has the discretion to grant or deny these exemptions.[32]

In a positive development, a High Court in October 2011 ruled in favor of an application by Print Media South Africa (PMASA) and the South African National Editors Forum (SANEF) to have the 2009 amendments to the Films and Publications Act declared unconstitutional. The judged agreed that the prescreening of "publications" (including internet content) would affect the value of news and be an unjustifiable limitation on the right to freedom of expression. During the time of writing, the amendment was being reviewed by the constitutional court.[33]

In May 2010, the deputy Minister of Home Affairs, Malusi Gigaba, announced that he had approached the country's Law Reform Commission to ask for a complete ban on digitally-distributed pornography at the first tier of service providers through an internet and mobile phone pornography bill developed by the Justice Alliance of South Africa (JASA). The bill used a very broad definition of pornography found in a law outlawing sexual offenses.[34] In September 2011, a revised draft of the proposed bill was presented to the new Minister of Home Affairs by JASA, but the revised bill would still make internet pornography illegal. As of early 2012, the bill has not yet been introduced to parliament.

Under the Electronic Communications and Transactions Act of 2002 (ECTA), ISPs are required to respond to and implement take-down notices (TDNs) regarding illegal content, such as child pornography, material that could be defamatory without justification, or

[31] The Film and Publications Board, is part of the Ministry of Home Affairs. According to the Film and Publications Amendment Act of 2003, all ISPs are required to register with the board.
[32] Films and Publications Amendment Act, No. 3 of 2009, accessed June 4, 2010, http://www.info.gov.za/view/DownloadFileAction?id=106329.
[33] "Film and Publications Act amendments declared unconstitutional," BizCommunity, November 3, 2011, http://www.bizcommunity.com/Article/414/466/66617.html.
[34] Criminal Law (Sexual Offences and Related Matters) Amendment Act, No. 32 of 2007, accessed June 4, 2010, http://www.info.gov.za/view/DownloadFileAction?id=77866.

copyright violations. There is no procedure for appealing take down notices, thus ISPs often have to err on the side of caution by taking down the content once a TDN is received in order to avoid court cases.[35]

The government does not restrict material on contentious topics such as corruption and human rights. Citizens are able to access a wide range of viewpoints, and there are no government efforts to limit discussion. Online content, however, does not match the diverse interests within society, especially with respect to race and local languages. There are a number of political and consumer-activist websites, though the internet is not yet a key space for social or political mobilization. Radio, followed by television, continue to be the main sources of news and information for most South Africans, but there are increasing efforts to extend mainstream news outlets to online platforms. All major media groups now have an online presence.

Individuals and groups can engage in peaceful expression of views via the internet using email, instant messaging, chat rooms, and social media. YouTube, Facebook, and international blog-hosting services are freely available. The South African blogosphere has been highly active in promotion of AIDS awareness and the discussion of environmental issues, in addition to more general political coverage. The internet and mobile phones have been used for political organization, especially during recent developments like the protest and activism against the 2011 Protection of State Information Bill and around environmental issues at COP17, the Durban Climate Change Conference in November 2011. The main political parties have developed online campaigns to attract young voters and are very active in social media.

VIOLATIONS OF USER RIGHTS

The constitution guarantees "freedom of the press and other media; freedom to receive or impart information or ideas; freedom of artistic creativity; and academic freedom and freedom of scientific research." However, it also includes constraints, and freedom does not extend to "propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender, or religion and that constitutes incitement to cause harm."[36] The judiciary in South Africa is independent and has issued at least two rulings protecting freedom of expression online. Libel is not a criminal offense, but civil laws have

[35] Ant Brooks from the ISP Association says: "If an ISP gets a TDN targeting your content, they will either take it down, or require that you provide them with an undertaking to cover any legal costs they might incur by leaving it up."
[36] Constitution of the Republic of South Africa, May 8, 1996, Bill of Rights, Chapter 2, Section 16.

been applied to online content. Criminal law has been invoked on at least one occasion to prosecute for injurious material.[37]

Threats to media freedom have also extended to the online content of newspapers. In May 2009, the country's public broadcaster, the South African Broadcasting Corporation (SABC), filed a charge of "stolen property" after the *Mail & Guardian* posted on its website a documentary on political satire that the broadcaster had refused to air. The documentary explored the fact that award-winning cartoonist Zapiro was being sued by President Jacob Zuma for portraying him about to rape Lady Justice. The newspaper's editor, Nic Dawes, argued that he and his colleagues had a professional duty to make such material public and accused the SABC of censorship.[38] In May 2010, the South African Council of Muslim Theologians attempted to stop the *Mail & Guardian* from publishing another cartoon by Zapiro that depicted the prophet Muhammad, arguing that the image was insulting to Muslims. A court injunction, which would have extended to the online version of the newspaper, was not granted.[39]

In March 2011, a businesswomen and fashion label owner, Inge Peacock, submitted an application to the Western Cape High Court to compel the magazine *Noseweek* to remove an allegedly defamatory article from its website. The article was about the challenges facing the South African clothing and textile industry and revealed how major stores were not discriminating enough about whom they chose to do business with. Peacock's refusal to settle an account with a garment factory was cited in the article. A judge dismissed the case seeing the issue as involving two clashing constitutional rights—the right to freedom of expression and the right to dignity. [40]

Recent legislation potentially allows for extensive monitoring and has been in force since June 2009. One such piece of legislation, the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA), requires ISPs to retain customer data for an undetermined period of time and bans any internet system that cannot be monitored. RICA also requires mobile subscribers to provide extensive personal information to service providers, which is then made available to the government. An identification number is legally required for any SIM card purchase, and people already in the possession of SIM cards are required to register with a proof of residence and an identity

[37] See Freedom of the Net 2011, "South Africa."
[38] Matthew Burbidge, "SABC Lays Charge of 'Theft' over Zapiro Doccie," Mail & Guardian, May 28, 2009, http://www.mg.co.za/article/2009-05-28-sabc-lays-charges-of-theft-over-zapiro-doccie.
[39] "Anger Mounts Over Zapiro Cartoon," Mail & Guardian, May 22, 2010, http://www.mg.co.za/article/2010-05-22-anger-mounts-over-zapiro-cartoon.
[40] "Fashion victim," Noseweek, March 1, 2012, http://www.noseweek.co.za/article/2696/Fashion-victim; Sapa, "'Fashion victim' bid to gag Noseweek fails," Times Live, March 6, 2012, http://www.timeslive.co.za/lifestyle/2012/03/06/fashion-victim-bid-to-gag-noseweek-fails.

document.[41] There have been reports of criminals circumventing registration laws and that illegal unregistered SIM cards can be purchased quite easily. In November 2011, the police seized about 60,000 pre-registered SIM cards, "all registered to one untraceable person."[42]

While RICA obliges ISPs to send communications in question to an interception center, the Act explicitly prohibits the interception of communications, except when granted permission from a judge designated to rule on the practice. The Criminal Procedures Act allows law enforcement agencies to apply to a high court judge or regional court magistrate for mobile phone records or the location of a cell phone. RICA also requires judicial oversight and includes guidelines for judges to establish whether the interception is justified in terms of proportionality and narrowly defined standards. Reports by the *Mail & Guardian* however suggest that "[s]tate intelligence agencies can—and do—access citizens' private communications illegally," and that "it is a common occurrence, especially in police crime intelligence."[43]

Another law that potentially restricts anonymous communication is the Electronic Communications and Transactions Act of 2002 (ECTA), which created a legion of inspectors trained to "inspect and confiscate computers, determine whether individuals have met the relevant registration provisions, as well as search the internet for evidence of 'criminal actions.'"[44] The law also states that ISPs "do not have an obligation to monitor," exempting them from liability if proscribed content is found on their service but taken down once a notice is received. However, this exemption only applies if the ISPs are members of a recognized representative organization, such as the Internet Service Providers' Association of South Africa (ISPA).

The Ministry of Communications has recognized the ISPA as an industry representative body under the ECTA. The ISPA acts as an agent on behalf of its 160 members and provides the ministry with annual information about the total number of TDNs issued, the actions taken

[41] Nicola Mawson, "'Major' RICA Threat Identified," ITWeb, May 27, 2010, http://www.itweb.co.za/index.php?option=com_content&view=article&id=33518:major-rica-threat-identified&catid=69&Itemid=58.
[42] Yogas Nair, "60k pre-Rica'd SIMS found," Daily News, November 8, 2011, http://www.iol.co.za/news/south-africa/kwazulu-natal/60k-pre-rica-d-sim-cards-found-1.1173774.
[43] Heidi Swart, "Secret state: How the Government spies on you," Mail & Guardian, October 14, 2010, http://mg.co.za/article/2011-10-14-secret-state/.
[44] Privacy International, "South Africa," in *Silenced: An International Report on Censorship and Control of the Internet* (London: Privacy International, 2003), accessed June 24, 2010, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-103781.

in response, and the final results.[45] Most of the complaints lodged are resolved amicably, with ISPA's clients agreeing to take down the offending content.[46]

Reports indicate that the government conducts some bulk surveillance of mobile phone conversations, short-message service (SMS), and emails through the National Communications Center (NCC), a government agency which houses interception facilities. The NCC targets "foreign signals intelligence" and intercepts communications in bulk. The NCC reportedly has the technical capabilities and staffing to monitor both SMS and voice traffic originating outside South Africa.[47] Calls from foreign countries to recipients in South Africa can allegedly be monitored for certain keywords; the NCC then intercepts and records flagged conversations. While most interceptions involve reasonable national security concerns, such as terrorism or assassination plots, the system allows the NCC to record South African citizens' conversations without a warrant.[48]

Although the NCC operates outside the boundaries of the law, a current bill in Parliament—the General Intelligence Laws Amendment Bill, previously shelved in 2008 but reintroduced in 2011—would legalize the interception of "any communication that emanates from outside the borders of the republic, or passes through or ends in the republic." This presents the possibility that the mass monitoring of internet communication could be legalized and that sending messages from an email address with a foreign company or through social-networking platforms like Facebook could potentially count as interceptable communication.[49]

Current threats to the traditional media in South Africa may in the future have an impact on the online world, especially with regards to the right to information. The proposed Protection of State Information Bill in 2011, passed by the National Assembly (the first house of parliament) and currently under discussion at the National Chamber of Provinces (the second house of parliament), would impose sentences on journalists of up to 25 years for reporting on classified information. If passed, this bill would have chilling effects on the media, as well as on internet users. For example, under the bill internet users could face sentences of up to ten years in prison for intentionally accessing classified South African state information on whistleblower websites.

[45] Paul Vecchiatto, "Content Disputes Settled Amicably," ITWeb, March 12, 2010, http://www.itweb.co.za/index.php?option=com_content&view=article&id=31260%3Acontent-disputes-settled-amicably&catid=182%3Alegal-view&Itemid=58.
[46] "Nyanda Recognises ISPA as Industry Representative Body," BizCommunity.com, May 21, 2009, http://www.bizcommunity.com/Article/220/16/36156.html.
[47] Moshoeshoe Monare, "Every Call You Take, They'll Be Watching You," Independent, August 24, 2008, http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20080824105146872C312228.
[48] Moshoeshoe Monare, Op cit.
[49] Drew Forrest and Stefaans Brümmer, "Spooks bid for new powers," Mail & Guardian, February 3, 2012, http://mg.co.za/article/2012-02-03-spies-bid-for-new-powers/.

There have been no reports of extralegal intimidation targeting online journalists, bloggers, or other digital technology users by state authorities or any other actor. Politically-motivated hacking attacks are not significant in South Africa; however the website of the African National Congress Youth League's website was hacked and defaced twice in 2011.[50] Spam and malware are a significant problem in South Africa, and a report by MessageLabs revealed that in September 2010, South Africa was the most targeted country by email borne malware with 1 out of every 99 emails infected.[51]

[50] Stuart Thomas, "ANC Youth League website hacked," Memburn, July 24 2011, http://memeburn.com/2011/07/anc-youth-league-website-hacked-2/.
[51] OECD Communications Outlook 2011, http://www.oecd.org/document/44/0,3746,en_2649_34225_43435308_1_1_1_1,00.html

SOUTH KOREA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	3	3
Limits on Content (0-35)	12	12
Violations of User Rights (0-40)	17	19
Total (0-100)	**32**	**34**

* 0=most free, 100=least free

POPULATION: 49 million
INTERNET PENETRATION 2011: 84 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

South Korea boasts of being one of the most connected countries in the world, as well as a fledgling, vibrant democracy. Recent years, however, have been marked by increased policing of the online environment. The UN Special Rapporteur on Freedom of Expression, international journalists, and human rights groups have voiced concerns that the space for free expression in the country has been diminishing since 2008.[1] In 2011, the push and pull between forces wishing to control the internet and those urging greater openness and privacy intensified. Censorship and detentions related to dissemination of content sympathetic to North Korea or critical of the current administration continued, and in some aspects increased. By early 2012, however, the relevant authorities relaxed restrictions on the use of social media for election campaigns and announced they would consider phasing

[1] Frank La Rue, "Full Text of Press Statement Delivered by UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Frank La Rue, After the Conclusion of His Visit to the Republic of Korea," United Nations Office of the High Commissioner for Human Rights, May 17, 2010, http://www2.ohchr.org/english/issues/opinion/docs/ROK-Pressstatement17052010.pdf; Chico Harlan, "In S. Korea, a shrinking space for speech," Washington Post, December 22, 2011, http://www.washingtonpost.com/world/asia_pacific/in-s-korea-a-shrinking-space-for-speech/2011/12/21/gIQAmAHgBP_story.html; Reporters Without Borders, *Internet Enemies Report 2012* (Paris: Reporters Without Borders, March 12, 2012), http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf; Irene Khan, "Statement by Irene Khan, Amnesty International Secretary General, on the Completion of Her Visit to South Korea," Amnesty International, November 24, 2009, http://www.amnesty.org/en/library/asset/ASA25/013/2009/en/81c8df37-c1d9-4d49-aa8c-825cd7ce9203/asa250132009en.pdf.

out the Internet Real-Name Registration System, which had limited anonymity and contributed to self-censorship in South Korean cyberspace since 2004.[2]

South Korea's high internet penetration rate is widely attributed to a series of state-led initiatives implemented since the 1990s, such as Cyber Korea 21 (1999–2002), the e-Korea Vision 2006 (2002–2006), and the U-Korea Master Plan (2006–2010). The government's rationale for this policy of nationwide promotion of information and communication technologies (ICTs) is that a country with few natural resources like South Korea must move quickly toward a knowledge-based economy if it is to compete with established economic powers.[3] Cyber Korea 21 was well received by the Korean public, partly because such a rationale appealed to them in the aftermath of the Asian financial crisis of 1997, and partly because a foundation of computer-mediated communications had already been laid with the thriving use of early, text-based online communication via *PC tongshin* (PC communication).

OBSTACLES TO ACCESS

South Korea is one of the most wired countries in the world, in terms of both levels of usage and connection speeds. According to the International Telecommunications Union (ITU), approximately 82 percent of South Koreans accessed the internet in 2011.[4] When internet access via mobile phones, televisions, and game consoles is also included, an estimated 97 percent of households have access, leading the Organization for Economic Co-operation and Development (OECD).[5]

Several factors have contributed to the country's high degree of connectivity. First, high-speed access is relatively affordable. Most residences have connections capable of reaching 100 Mbps for under KRW 30,000 (US$26) per month.[6] Second, the population is densely concentrated in urban areas. Roughly 70 percent of South Koreans live in cities dominated

[2] In a development beyond the coverage period of this report, the Constitutional Court ruled in August 2012 that the real-name registration system was unconstitutional and violated freedom of speech. Evan Ramstad, "South Korea Court Knocks Down Online Real-Name Rule," Wall Street Journal, August 24, 2012, http://online.wsj.com/article/SB10000872396390444082904577606794167615620.html.

[3] National Computerization Agency, *Informatization White Paper 2002: Global Leader e-Korea* (Seoul: NCA, 2002), http://www.itglobal.or.kr/_file/m_board/download.asp?file=%BF%B5%B9%AE_b2002eng.pdf.

[4] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[5] Organization for Economic Co-operation and Development, *OECD Key ICT Indicators: Households with access to the Internet 2000–10*, http://www.oecd.org/dataoecd/19/45/34083073.xls.

[6] John D. Sutter, "Why Internet Connections Are Fastest in South Korea," CNN Tech, March 31, 2010, http://articles.cnn.com/2010-03-31/tech/broadband.south.korea_1_broadband-plan-south-korea-broadband-internet?_s=PM:TECH.

by high-rise apartment buildings that can easily be connected to fiber-optic cables.[7] Finally, the government has implemented programs to expand internet access, including subsidies for low-income groups.[8]

In terms of mobile phone penetration, as of the end of 2011, there were 52.5 million subscriptions, exceeding the total population.[9] The number of smartphone users has been growing significantly, reaching 20 million in 2011 and expected to increase by at least another 50 percent in 2010.[10]WiFi coverage also increased rapidly in 2011 to accommodate the growing number of people using smartphones and tablet computers.[11] For example, the government in the capital Seoul launched a US$44 million project in June to blanket the city—including parks and public transportation—with free outdoor wireless internet access by 2015.[12]

There is no significant gap in access to ICTs with respect to gender or income level, although differences in computer literacy across generational and professional lines persist.[13] Besides high household penetration rates and widely available WiFi, the absence of a large digital divide is attributable to the omnipresence of cybercafes. Known as *PC bangs* (PC rooms) in Korean, the facilities offer broadband access at a price of approximately US$1 per hour, and also serve as venues for social interaction, particularly among youth, who frequent cybercafes to play online games.

Despite such widespread connectivity, some obstacles to access remain. In an effort to tackle a growing phenomenon of internet addiction, since 2010, the government has enacted a number of laws and regulations aimed at restricting youngsters from playing online games

[7] J. C. Herz, "The Bandwidth Capital of the World," Wired, August 2002, http://www.wired.com/wired/archive/10.08/korea.html?pg=1&topic=&topic_set.
[8] John D. Sutter, "Why Internet Connections Are Fastest in South Korea," CNN Tech.
[9] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[10] Hee-jong Kang, "Convergence to be the only solution to the already saturated telecommunications market," Digital Times, January 8, 2012, http://www.dt.co.kr/contents.html?article_no=2012010902010531742002 (link discontinued).
[11] Hee-jong Kang, "240 thousand Wi-Fi zones by end year," [in Korean] Digital Times, June 14, 2011, http://www.dt.co.kr/contents.html?article_no=2011061502010351742002 (link discontinued).
[12] "Seoul to offer free wifi in public areas," The Independent, June 20, 2011, http://www.independent.co.uk/travel/news-and-advice/seoul-to-offer-free-wifi-in-public-areas-2300048.html; Hyeon-jeong Jeong, "3 mobile carriers agree to build 1,000 joint Wi-Fi spots [at public places]," [in Korean] ZDNet Korea, July 18, 2011, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20110718125845.
[13] Du-jin Choi, Yeong-dal Ryu, et al., *The 2010 Digital Divide Index* [in Korean] (Seoul: National Information Society Agency, 2011), www.nia.or.kr/Extra/Module/Common/Lib/Attach/DownLoad.aspx?Seq=21197.

for long periods of time, including throughout the night.[14] In addition, foreign residents face difficulties accessing many online services, both governmental and commercial. This is largely due to language barriers, but a more significant factor is the Internet Real-Name Registration System[15] adopted in 2004 under an amendment to the Public Official Election Act.[16] Users are required to verify their identities by submitting their Resident Registration Numbers (RRNs) when they wish to join and contribute to web portals and other major sites. As RRNs are assigned only to Korean citizens at birth, foreign nationals must individually contact webmasters to confirm their identities. This may change in the near future, as the government and private firms are in the process of discussing alternatives to RRNs—such as mobile phone numbers or internet-specific IDs—as the basis for the real name system.

In 2007, the Internet Real-Name Registration System was expanded to apply to any website with more than 100,000 visitors per day.[17] This included the video-sharing website YouTube, but the site's U.S.-based parent company, Google, refused to ask its Korean customers for their RRNs. Instead, it has blocked users from uploading content onto YouTube Korea. Users are able to bypass the restriction by simply switching their location setting to "worldwide." Even the Korean presidential office maintains its YouTube channel in this way.[18] Other popular applications, such as the social-networking site Facebook and the microblogging service Twitter, are available and currently exempt from the identity verification requirement. Although subject to the online real name system, locally-based social networking sites like Cyworld and web portals like Naver and Daum are also popular among Korean users.

[14] Critics have questioned the effectiveness of the regulations. For example, a study commissioned by a video game website found that after one month of the law coming into effect, many youngsters were finding ways to continue late night game playing despite the restriction. For instance, using parents' logins or resorting to offline games. "Young S. Koreans face midnight ban for online games," France 24, December 1, 2010, http://www.france24.com/en/20101202-young-skoreans-face-midnight-ban-online-games-0 (site discontinued); Greg Collins, "South Korean government shutting down online gaming," Tech Digest, November 15, 2011, http://www.techdigest.tv/2011/11/south_korean_go.html. ; Yeon-jin Choi, "The Shutdown Law now boomerangs: Sony denies gaming access to all Korean youngsters," [in Korean] *Hankook Ilbo*, November 16, 2011, http://news.hankooki.com/lpage/economy/201111/h2011111602314821540.htm; Tori Floyd, "Korean kids banned from late-night gaming, but it's not working," Yahoo! News Right Click (blog), January 7, 2012, http://ca.news.yahoo.com/blogs/right-click/korean-kids-banned-night-gaming-not-working-172635302.html; Alt, "Triple Regulation Coming True After all," This Is Game Global, February 7, 2012, http://www.thisisgame.com/en/2012/02/07/triple-regulation-coming-true-after-all.

[15] Korea Internet Security Agency, *2011 Survey on the Internet Usage of Foreign Residents in Korea* [in Korean] (Seoul: KISA, November 2011), http://isis.kisa.or.kr/board/fileDown.jsp?pageId=040100&bbsId=7&itemId=777&athSeq=1.

[16] The amendment became Article 82, Provision 6 of the act.

[17] The expansion was a result of the Act on Promotion of Information and Communications Network Utilisation and Data Protection.

[18] "Cheong WaDae/ Korea & President Lee Myung-bak," YouTube Video Channel, posted by "PresidentMBLee," last updated July 23, 2012, http://www.youtube.com/user/PresidentMBLee.

The telecommunications sector in South Korea is relatively diverse and open to competition, with 121 internet-service providers (ISPs) operating as of May 2012.[19] Nevertheless, the market remains dominated by three companies: Korea Telecom (43.5 percent), SK Telecom (18.9 percent), and LG Telecom (16.0 percent). The same firms share the country's mobile phone service market, with 31.6 percent, 50.5 percent, and 17.8 percent, respectively.[20] All three are publicly traded companies (Korea Telecom was state-owned until privatization in 2002), but they are part of the country's *chaebol*—large, family-controlled conglomerates—which are in turn closely connected by marriage ties to the political elite.[21] This has given rise to speculation that favoritism was at play in the privatization process and in the selection of bidders for mobile phone licenses.

One of the first priorities of the conservative government that took office in February 2008 was to restructure regulatory institutions dealing with ICTs. The Ministry of Information and Communication (MIC) and the Korean Broadcasting Commission (KBC) were merged to create the Korea Communications Commission (KCC), tasked with overseeing both telecommunications and broadcasting to improve policy coherence.[22] The KCC consists of five commissioners, with the president appointing two (including the chairman) and the National Assembly choosing the remainder. The KCC has struggled to earn credibility as its first chairman Choi See-joong was a close associate of the president, causing some observers to view the restructuring as a government effort to tighten control over the media and ICT sectors.[23] The president reappointed Choi as chairman in March 2011 over objections of opposition lawmakers who claimed he had politicized the agency via his personnel choices and had favored conservative media outlets in licensing decisions. In January, Choi resigned after prosecutors began investigating him in connection with several bribery scandals, including one that involved allegations that a former aide of his had received millions of won in bribes from the Korea Broadcasting and Art School in return for business favors.[24] Choi was arrested in April 2012 and expected to stand trial later in the year.[25] In February 2012,

[19] Korea Internet and Security Agency, Infrastructure Statistics: ISPs (2011) [in Korean], http://isis.kisa.or.kr/sub01/?pageId=010302.
[20] Korea Communications Commission "Wired/Wireless Subscriptions November 2011."
[21] Hyeok-cheol Kwon, "Is *Chojoongdong* one big family?" [in Korean] Hankyoreh, July 29, 2005, http://www.hani.co.kr/kisa/section-002009000/2005/07/002009000200507291742668.html.
[22] Jong Sung Hwang and Sang-hyun Park, "Republic of Korea," in *Digital Review of Asia Pacific 2009–2010* (London: Sage Publications, 2009), 234–240.
[23] Ji-nam Kang, "Who's Who Behind Lee Myung-bak: Choi See-joong the Chairman of the KCC (Appointed)," [in Korean] *Shindonga* (583, 2008), 48–49, http://shindonga.donga.com/docs/magazine/shin/2008/04/12/200804120500019/200804120500019_1.html.
[24] Yonhap News, "Ex-aide of KCC chief under bribery probe," The Korea Herald, January 4, 2012, http://www.koreaherald.com/national/Detail.jsp?newsMLId=20120103000879; Tae-gyu Kim and Jun-beom Hwang, "Choi See-joong's protégé Jeong Yong-uk bags a huge bribe and flees to Canada?" [in Korean] Hankyoreh, January 3, 2012, http://www.hani.co.kr/arti/society/society_general/513250.html.
[25] Sung-jin Yang, "Chief of telecom regulator resigns," The Korea Herald, January 27, 2012, http://www.koreaherald.com/national/Detail.jsp?newsMLId=20120127001130; Lee Joo-hee, "Lee's fraternity faces breakdown," The Korea Herald, June 5, 2012, http://view.koreaherald.com/kh/view.php?ud=20120506000416.

President Lee Myung-bak named Lee Kye-cheol, a former vice minister for ICTs, as KCC chairman.

LIMITS ON CONTENT

Although the South Korean blogosphere is vibrant and creative, there are a number of restrictions on the free circulation of information, including content of public interest or criticism of government figures. Some of these measures have intensified since early 2011, though they were partly offset by an important Constitutional Court decision that prompted a significant relaxation of restrictions on election-related online communications.

Two types of censorship are particularly evident in South Korea: technical filtering of websites and social media accounts,[26] and the administrative deletion of certain content on the orders of the Korea Communications Standards Commission (KCSC) or the National Election Commission (NEC).

The KCSC was established in 2008 to maintain ethical standards in broadcasting and internet communications. It is technically an independent statutory organization, but its nine members are appointed by the president.[27] One of its primary tasks is to monitor online content for possible content violations, including obscenity, defamation, and threats to national security. Citizens can also submit petitions against content they believe has violated their privacy or harmed their reputation. The KCSC then makes recommendations to bulletin board operators or ISPs to implement corrective measures, which range from deletion of postings to blocking of designated internet protocol (IP) addresses. Such recommendations are not legally binding in themselves. However, under the Comprehensive Measures on Internet Information Protection issued in 2008, the KCC may step in and impose heavy fines on service providers in cases of noncompliance. Consequently, the vast majority of censorship recommendations are implemented.

Given the political tensions with North Korea, the South Korean government has imposed restrictions on access to content produced by the north or otherwise sympathetic to it. A series of tests conducted in 2008 and 2010 by the OpenNet Initiative found that a significant number of websites containing North Korean propaganda or writings promoting reunification of the two Koreas were explicitly and consistently blocked in South Korea.[28]

[26] OpenNet Initiative, "Country Profile: South Korea," December 26, 2010, http://opennet.net/research/profiles/south-korea.
[27] Six members are nominated by the president and the party with a parliamentary majority, while three are nominated the opposition. See, Jeong-hwan Lee, "A private organisation under the president? The KCSC's structural irony," [in Korean] Media Today, September 14, 2011, http://www.mediatoday.co.kr/news/articleView.html?idxno=97350.
[28] Besides North Korea-related content, a small number of gambling and Korean-language pornographic sites were found to be filtered. OpenNet Initiative, "Country Profile: South Korea."

The National Intelligence Service and the Korean National Police Agency can ask the KCSC to have websites carrying pro-North Korean content rendered inaccessible. Examples include the blocking of North Korea's official Twitter account "@uriminzok" and official web portal Naenara (www.naenara.com.kp). The justification given is that these violate the 1948 National Security Law, which classifies content that "praises, promotes, and glorifies North Korea" as "illegal information."

The KCSC process has been criticized for its vaguely defined standards and the wide discretionary power this single entity possesses to determine what information should be censored.[29] Concerns have also been expressed over the lack of transparency and accountability in the decision-making process, including the fact that administrators of censored URLs are given no opportunity to defend themselves before the commission. In 2011, criticism emerged from within the commission as well. One of its nine members, Park Kyung-shin, challenged the KCSC's deliberation criteria and rulings by starting a blog on which he posted samples of content that had been censored by the commission and then discussed the factors to consider in making such a determination. In July 2011, he posted non-sexual pictures of human male anatomy, such as those found in sex education books.[30] This prompted the KCSC to begin proceedings for evaluating his blog as a candidate for removal, stirring public debate. Park eventually removed the content deemed offensive and the commission issued him a warning. However, in February 2012, prosecutors indicted him for possible violation of obscenity laws.[31] Park's blog is still available, and he continues to voice his concerns regarding freedom of expression there.[32]

The KCSC intermittently publishes on its website statistics of the corrective measures taken.[33] These statistics show that the KCSC had 4,731 websites/pages blocked[34] and 6,442 items deleted[35] in 2008, its first year of operation. The figures have seen a considerable rise since. Throughout 2011, 31,357 websites/pages were blocked[36] and 9,058 items were reportedly deleted for offenses such as "encouraging gambling," "obscenity," "violating

[29] Jillian York and Rainey Reitman, "In South Korea, the Only Thing Worse Than Online Censorship is Secret Online Censorship," Electronic Frontier Foundation, September 6, 2011, https://www.eff.org/deeplinks/2011/08/south-korea-only-thing-worse-online-censorship; Jeong-hwan Lee, "A private organisation under the president? The KCSC's structural irony," [in Korean] Media Today, September 14, 2011, http://www.mediatoday.co.kr/news/articleView.html?idxno=97350.

[30] R. Jai Krishna and Evan Ramstad, "'Offensive' Web Content Targeted in Asia," The Wall Street Journal, December 6, 2011, http://online.wsj.com/article/SB10001424052970204770404577082080244171866.html; York and Reitman, "In South Korea, the Only Thing Worse Than Online Censorship is Secret Online Censorship."

[31] Evan Ramstad, "Prosecutors Target Censorship Critic," The Wall Street Journal, March 8, 2012, http://blogs.wsj.com/korearealtime/2012/03/08/prosecutors-target-censorship-critic/.

[32] K.S. Park's Writings (blog), blog.naver.com/kyungsinpark.

[33] Available at http://www.kocsc.or.kr/02_infoCenter/info_Communition_List.php [in Korean].

[34] 3,816 for "encouraging gambling," 549 for "disturbing social order," and 366 for "obscenity."

[35] 3,238 for "disturbing social order,"1,460 for "obscenity," 1,201 for "violating others' rights," 424 for "violence, cruelty and hatred," and 119 for "encouraging gambling."

[36] 14,951 for "encouraging gambling," 12,064 for "disturbing law and order," 3,998 for "obscenity," 319 for "violating others' rights," and 25 for "violence, cruelty and hatred."

others' rights," and "disturbing law and order" (which would include items blocked or removed under the National Security Law).[37]

In 2011, the KCSC sought to expand the scope of censorship to social networking services, mobile phone applications, and podcasts.[38] Among the targets of censorship were some social media accounts of people engaging in criticism of the government. In December, the commission created a team to more systematically monitor Web 2.0 platforms, such as Twitter and Facebook, for violations. In one high-profile example, the KCSC reportedly warned that a popular, satirical anti-government podcast titled *Naneun Kkomsuda* or in short *Nakkomsu* (which can be translated into "I'm a petty trickster")[39] could be subject to censorship, particularly if anyone mocked during the program files a complaint; as of May 2012, however, the podcast was freely available.[40] In another example, in May 2011, the KCSC ordered the blocking of the Twitter account "@2MB18nomA," whose ID consists of the current president's nickname "2MB" and a reference to a common Korean curse word.[41] After the KCSC denied the user's appeal challenging the block, he turned to the Seoul Administrative Court, but lost the case in May 2012.[42]Meanwhile, the same user was fined one million Korean won (approximately US$880) for violating the election law over tweets he had posted in May 2011 criticizing the ruling party. That decision was overturned, however, when he successfully appealed in March 2012 after a change in election regulations (see below).[43]

Blocked social media accounts are still accessible from smartphones, but the ruling conservative party initiated an amendment to the Telecommunications Business Act in

[37] 7,191 for "disturbing law and order."1,449 for "obscenity," 348 for "violating others' rights," 49 for "encouraging gambling," and 21 for "violence, cruelty and hatred."

[38] Matt Brian, "South Korea may begin censoring social networking, mobile apps from next week," The Next Web, December 1, 2011, http://thenextweb.com/asia/2011/12/01/south-korea-may-begin-censoring-social-networking-mobile-apps-from-next-week/.

[39] Banyan, "Sneaky tricksters, unite!" The Economist, January 16, 2012, http://www.economist.com/blogs/banyan/2012/01/satire-south-korea.

[40] The podcast was one of ten apps that in January 2012 the commander of the Sixth Army Corps ordered subordinates to delete from their smartphones because they contained content that was either pro-North Korean or critical of the Lee Myung-bak administration. Soon-taek Kwon, "*Nakkomsu* too would be up for consideration if a complaint was filed," [in Korean] Mediaus, December 5, 2011, http://www.mediaus.co.kr/news/articleView.html?idxno=21548; "Army unit orders 'pro-N. Korea' apps be deleted, inspects individual phones," Yonhap News, February 6, 2012, http://english.yonhapnews.co.kr/national/2012/02/06/56/0301000000AEN20120206001200315F.HTML.

[41] Chico Harlan, "In S. Korea, a shrinking space for speech," The Washington Post, December 22, 2011, http://www.washingtonpost.com/world/asia_pacific/in-s-korea-a-shrinking-space-for-speech/2011/12/21/gIQAmAHgBP_story.html; Louisa Lim, "In South Korea, Old Law Leads To Crackdown," National Public Radio (NPR), December 1, 2011, http://www.npr.org/2011/12/01/142998183/in-south-korea-old-law-leads-to-new-crackdown.

[42] Jeong-min Yang, "Owner of the Twitter ID 'cursing MB' lost his case, but why?" [in Korean] Money Today, May 4, 2012, http://www.mt.co.kr/view/mtview.php?type=1&no=2012050407583397741&outlink=1.

[43] Seung-mo Kim, "Posting on Twitter a list of candidates to be rejected is not illegal, says court," [in Korean] The Law Times, March 20, 2012, http://www.lawtimes.co.kr/LawNews/News/NewsContents.aspx?serial=63156.

November 2011 that would require mobile operators to enforce filtering orders.[44] The KCSC also announced in January 2012 that it would introduce a warning system to recommend users voluntarily delete posts on social-networking sites if the information in them is deemed false or harmful. Failure to delete the post in question within a day of receiving the warning would result in the commission asking ISPs to block access from within South Korea to the account.[45] As of May 2012, these systems did not appear to be in place yet.

Restrictions on online expression surrounding elections have generally been more stringent in South Korea than in other democracies, though this gap shrank after a landmark Constitutional Court ruling in December 2011. Although the initial measures adopted were to ensure fair electoral competition, their broad scope raised concerns that they limited political speech important for voters and candidates. Article 93 of the Public Official Election Act, in particular, prohibits individual voters from distributing or displaying "an advertisement, letter of greeting, poster, photograph, document, drawing, printed matter, audio tape, video tape, or the like" during the 180 days prior to election day if it contains an endorsement of or opposition to a candidate or a political party. The NEC initially interpreted this article as also applying to blog posts, user comments on news websites, and user-generated content in social media. Commissioners could demand that websites or blog-hosting services delete postings that carry such content. In a positive development, however, on December 29, 2011, the Constitutional Court ruled that the NEC's ban on social media—especially Twitter—being used in campaigning was unconstitutional.[46] The NEC subsequently announced on January 13, 2012 that it would henceforth allow online campaigns.[47] The court decision was especially timely given parliamentary and presidential elections scheduled for April and December 2012, respectively.

Prior to the above changes, two important by-elections took place in 2011, one in April and the other in October. In both instances, the ruling party was defeated after a high turnout of young voters, many of whom typically favor independent or opposition candidates. In the run-up to the elections, the NEC reminded voters of the limits of permissible online

[44] Jin-shik Song, "The government and the ruling party looking to block access to SNS from smartphones," [in Korean] Kyunghyang Shinmun, November 9, 2011, http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201111091740061&code=910402.
[45] Ji-hyun Cho, "Criticism escalates over SNS censorship," The Korea Herald, January 29, 2012, http://www.koreaherald.com/business/Detail.jsp?newsMLId=20120129000285.
[46] Yonhap News, "Constitutional Court OKs Twitter for election campaigns," The Korea Times, December 29, 2011, http://www.koreatimes.co.kr/www/news/nation/2011/12/113_101835.html; Akira Nakano, "S. Korea allows campaigning on social networking sites," The Asahi Shimbun, December 30, 2011, http://ajw.asahi.com/article/asia/AJ201112300023.
[47] AFP, "S. Korea lifts ban on Internet for electioneering," AsiaOne, January 13, 2012, http://www.asiaone.com/News/Latest%2BNews/Science%2Band%2BTech/Story/A1Story20120113-321714.html; Yonhap News, "Election regulator allows Internet election campaigns," The Korea Times, January 13, 2012, http://www.koreatimes.co.kr/www/news/nation/2012/01/311_102798.html.

campaigning, though many continued to express their support for candidates anyway. This dynamic was especially evident for the October by-election, which resulted from the abrupt departure of the Mayor of Seoul in August 2011. Going beyond restrictions on users' ability to express support for a particular candidate in their posts, the NEC warned so-called "influential Twitter users," including celebrities, not to encourage people to exercise their right to vote in general.[48] The commission argued that most of these influential users were known to favor the independent candidate Park Won-soon (the eventual winner of the election) over the conservative candidate Na Kyung-won; therefore, their encouraging people to go to the polls would equate to showing support for Park, which was not allowed under the interpretation of the regulations at the time.[49] Despite this warning, many of these users encouraged people anyway, often using sarcastic or implicit language. Some subsequently faced reprisals. In December, prosecutors called a TV presenter and a law professor in for questioning for encouraging people to vote after the aide of a former member of the conservative party filed a complaint against them.[50]

The aforementioned regulations, in addition to real name registration and occasional prosecution of bloggers and social media users, have contributed to an atmosphere of self-censorship, particularly on topics like North Korea. The regulations have also led some service providers and websites to institute their own registration or content monitoring policies so as to preempt censorship orders from government agencies and avoid violation of existing laws. For example, the popular web portal Naver has been suspected of manipulating the "real-time hot queries" list displayed on its main page by excluding certain frequently searched words—such as the controversial KORUS FTA (Korea-U.S. Free Trade Agreement)—if they conflict with government interests.[51]

Nevertheless, South Koreans continue to enthusiastically embrace online technology and mobile phones for civic engagement and political mobilization. One high-profile example in 2011 related to a one-woman sit-in by labor activist Kim Jin-suk atop a crane to protest layoffs at Hanjin Heavy Industries. During her 309-day protest, Kim regularly posted messages to over 27,000 Twitter followers, some of whom organized offline demonstrations

[48] Yoo Eun Lee, "South Korea: Warning to Twitter Influencers Fails to Discourage Voters," Global Voices (blog), October 27, 2011, http://globalvoicesonline.org/2011/10/27/south-korea-tweeting-elections-against-all-odds/.
[49] Sang-man Kim, "So, Jo Sumi can encourage you to vote but Lee Oisoo cannot?" [in Korean] Media Today, October 26, 2011, http://www.mediatoday.co.kr/news/articleView.html?idxno=98063.
[50] Mi-deob Cho and Hyeong-gyu Kim, "Kim Je-dong and Cho Kuk called in for questioning for encouraging people to vote; Twitter flooded with criticisms," [in Korean] Kyunghyang Shinmun, December 9, 2011, http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201112092134415&code=940301.
[51] In-seong Kim, "Sorry, Naver, I am on Google's side," [in Korean] OhmyNews, May 25, 2011, http://www.ohmynews.com/NWS_Web/view/at_pg.aspx?CNTN_CD=A0001571141.

in support of her cause.[52] With the loosening of restrictions on the use of social media surrounding elections, candidates and voters across the political spectrum began making significant use of these applications in advance of the 2012 polls. Many observers believed this could benefit the opposition, as young, tech-savvy voters tend to favor opposition and independent candidates over those of the ruling conservative party.[53] In the April 2012 parliamentary polls, however, the first elections conducted after the aforementioned change in campaigning rules, the conservative party ultimately emerged victorious, though with a slimmer majority than previously.[54]

VIOLATIONS OF USER RIGHTS

The South Korean constitution guarantees freedom of speech, the press, assembly, and association to all citizens, but it also enables restrictions by stating that "neither speech nor the press may violate the honor or rights of other persons nor undermine public morale or social ethics." South Korea has an independent judiciary and a national human rights commission that have taken decisions upholding freedom of expression. Nonetheless, a continued rise in criminal cases brought for online speech has generated a chilling effect and international criticism.[55] Meanwhile, several large-scale hacking attacks in 2011 that exposed millions of users' personal information have led the government and major internet companies to reassess the real-name registration system in place since 2004.

Several laws in South Korea have been used to restrict freedom of expression in traditional media as well as for online communications. The 1948 National Security Law allows prison sentences of up to seven years for praising or expressing sympathy with the North Korean regime. In April 2010, the Ministry of Unification issued a notice reminding citizens that the Act on Exchanges and Collaboration Between South and North Korea applies to online communications as well as offline encounters, and that any visit to websites or pages

[52] Jeremy Laurence and Ju-min Park, "After 309 days, South Korean protester climbs down from crane," Reuters, November 10, 2011, http://www.reuters.com/article/2011/11/10/us-korea-strike-idUSTRE7A930G20111110; Jaeyeon Woo, "After 309 Days, She Touched the Ground," The Wall Street Journal, November 10, 2011, http://blogs.wsj.com/korearealtime/2011/11/10/after-309-days-she-touched-the-ground/; Shin-jae Yoo & Gyeong-hwa Song, "From 176 to 7,282 to 17,106 to 61,061—#Hanjin tweets that have changed the world," [in Korean] Hankyoreh, January 9, 2012, http://www.hani.co.kr/arti/society/society_general/514067.html.

[53] Jack Kim and Ju-Min Park, "South Korea's Twitter generation may give liberals upset win," Reuters, April 9, 2012, http://uk.reuters.com/article/2012/04/09/uk-korea-politics-socialmedia-idUKBRE83804C20120409.

[54] Yongwook Ryu, "South Korea's 2012 national assembly elections," East Asia Forum, April 25, 2012, http://www.eastasiaforum.org/2012/04/25/south-korea-s-2012-national-assembly-elections/; Woo Jung-yeop, "April 2012 South Korean Parliamentary Elections: Surprise Results and Implications," Council on Foreign Relations, May 2012, http://www.cfr.org/south-korea/april-2012-south-korean-parliamentary-elections-surprise-results-implications/p28145.

[55] La Rue, "Full Text of Press Statement."

maintained by people of North Korea must be reported to the government in advance. Anyone failing to do so faces a fine of up to one million won (US$880).[56]

Prosecutions under the law, including for online communications, have dramatically increased since 2008 under the conservative party's administration. According to media reports, the number of people prosecuted for online activities deemed sympathetic to the North Korean regime increased from 5 in 2008 to 82 in 2010, a trend that appeared to continue into 2011.[57] In September 2011, police raided the studio of a young photographer, Park Jung-geun, after he re-tweeted posts from the North Korean Twitter account "@uriminzok."[58] Park claimed that he had done so with the aim of making fun of the regime. Nevertheless, police subsequently interrogated him five times and in January 2012, he was arrested and remained in custody for one month until bail was granted; as of May, the case was pending with the next court date set for July 2012.[59] In another set of cases, after Kim Jong-il's death, prosecutors reportedly investigated several people who created pages on social networking sites to express condolences, prompting many to shut the groups in order to avoid punishment.[60]

Defamation remains a criminal offence, with penalties of up to five years' imprisonment or a fine up to 10 million won (US$8,800). Defamation via ICTs draws heavier penalties—seven years in prison or a fine up to 50 million won (US$43,850)—under the 2005 Act on the Promotion of Information and Communications Network Utilization and Data Protection.[61] In one high-profile case, former lawmaker Chung Bong-ju, who was also one of the four contributors to the popular satirical *Nakkomsu* podcast, was convicted of spreading false rumors connecting President Lee to accusations of stock fraud. In December 2011, the Supreme Court upheld an earlier verdict sentencing Chung to one year in prison, stating

[56] Ministry of Unification, "Notice on the Use of North Korean Internet Sites," [in Korean] News & Statements, April 8, 2010, http://www.unikorea.go.kr/CmsWeb/viewPage.req?idx=PG0000000346&boardDataId=BD00000186451&CP0000000002_BO0000000033_Action=boardView&CP0000000002_BO0000000033_ViewName=board/BoardView&curNum=12.

[57] Sang-Hun Choe, "Sometimes, It's a Crime to Praise Pyongyang," The New York Times, January 5, 2012, http://www.nytimes.com/2012/01/06/world/asia/06iht-korea06.html?pagewanted=all.

[58] Lim, "In South Korea, Old Law Leads To New Crackdown"; Sang-Hun Choe, "South Korean Law Casts Wide Net, Snaring Satirists in a Hunt for Spies," The New York Times, January 7, 2012, http://www.nytimes.com/2012/01/08/world/asia/south-korean-law-casts-wide-net-snaring-satirists-in-a-hunt-for-spies.html?pagewanted=1&_r=1; "Amnesty urges release of S. Korean Twitter user," France 24, February 2, 2012, http://www.france24.com/en/20120202-amnesty-urges-release-korean-twitter-user.

[59] Paula Hancocks, "South Korean 'joke' may lead to prison," CNN, July 4, 2012, http://edition.cnn.com/2012/07/03/world/asia/south-korea-north-joke/index.html.

[60] Sujin Park and Il-hoon Hyeon, "The Prosecution starts investigation into some 100 treasonous items 'in memory of Kim Jong-il'," [in Korean] Munhwa Ilbo, December 20, 2011, http://www.munhwa.com/news/view.html?no=2011122001071627233002O; Chico Harlan, "In S. Korea, a shrinking space for speech," The Washington Post, December 22, 2011, http://www.washingtonpost.com/world/asia_pacific/in-s-korea-a-shrinking-space-for-speech/2011/12/21/gIQAmAHgBP_story.html.

[61] See Article 61: Republic of Korea, *Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.*, Article 61, Amended December 30, 2005, http://www.worldlii.org/int/other/PrivLRes/2005/2.html.

that he had violated election and defamation laws by disseminating the unconfirmed allegations.[62] In an effort to curb online smear campaigns surrounding elections, in January 2012, prosecutors warned that anyone posting false information about election candidates more than thirty times for the purpose of defaming the person's reputation would be arrested.[63] Touching more directly on online content is Article 44(7) of the Act on Promotion of Information and Communications Network Utilization and Data Protection, which lists "obstruction of business" as a punishable crime.

A copyright law that restricts file sharing was passed in May 2009 and came into effect two months later. Often referred to as the "three-strikes rule," it allows the government to shut down an entire online bulletin board after a third warning to take down pirated content. Internet companies and civil liberties advocates have raised concerns that this is an excessive scheme, which could threaten fair use and free expression.[64] In November 2010, the Ministry of Culture, Sports, and Tourism announced that it had issued over 450 warnings between March and September 2010 and had disabled 11 accounts of individuals who failed to cease uploading large amounts of copyrighted materials.[65]

Anonymous communication online is significantly compromised in South Korea, given the aforementioned real name registration system, though in 2011, the government came under increasing pressure to revise or abandon the system. While users must register their real identities before posting, they are permitted to choose pseudonyms that will appear to the public next to their comments. The system has encouraged some Korean users to leave domestic services in favor of their international counterparts.[66] Mobile phone purchase also requires users to provide their RRNs.

Beyond its chilling effect for online expression, the risk of such widespread real name registration became evident in July 2011 when a hacking attack, allegedly originating from China, targeted the popular portal Nate and its social networking service Cyworld. The hackers reportedly stole the personal details of 35 million users, or 70 percent of the country's population. The stolen data included users' real names, passwords, RRNs, mobile phone numbers, and e-mail addresses. The parent company SK Communications assured the

[62] Sang-hun Choe, "A Leading Critic of South Korea's President Is Jailed," The New York Times, December 26, 2011, https://www.nytimes.com/2011/12/27/world/asia/a-leading-critic-of-south-koreas-president-is-jailed.html.
[63] Hee-yeon Kim, "Anyone posting false information online more than 30 times will be arrested," [in Korean] ZDNet Korea, January 16, 2012, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20120116182822.
[64] B. H. Ahn, "The New Copyright Law and 'the Three-Strikes Rule'," [in Korean] Digital Times, August 12, 2009, http://www.dt.co.kr/contents.html?article_no=2009081302011869718001.
[65] "First three-strikeouts for 'heavy uploaders'. 11 accounts ordered to be suspended," [in Korean] http://news.mk.co.kr/newsRead.php?year=2010&no=596419
[66] Bon-kwon Koo, "Legislator Choi Moon-soon Lists 5 'Backward' Regulations in the Digital Environment," [in Korean] Hankyoreh, June 24, 2010, http://www.hani.co.kr/arti/economy/it/427362.html.

affected users that their RRNs and passwords were encrypted,[67] but the incident renewed public concern about internet users' right to privacy.[68]

Subsequently, the KCC expressed its intention to gradually amend the relevant laws, possibly towards the abolition of the internet real-name registration regime.[69] In April 2012, the KCC, the Ministry of Public Administration and Security, and the Financial Services Commission jointly put forward a policy whereby online service providers would be banned from collecting and storing users' RRNs—unless specific legal provisions require otherwise—and would be penalized more heavily in cases of data leaks; the plan was reportedly approved and intended to take effect in August 2012.[70] This change did not necessarily imply abolition of the real name registration system, which remained in place as of May 2012, though some companies had begun using methods other than RRNs for linking users' identities to their online profile. The KCC continues to explore implementing such alternatives on a wider scale in order to avoid use of RRNs, but still enable users' real identities to be confirmed.[71]

Individual users' personal information may be made available to the police and the prosecution upon request for investigative purposes, under Article 83(3) of the Telecommunications Business Act (TBA). There have been incidents in which the authorities have failed to follow the appropriate protocol when obtaining such information, raising concerns about internet users' right to privacy. In September 2011, a scandal broke out revealing that the National Intelligence Service had the capacity to intercept the content of a Gmail account of an individual accused of violating the National Security Law.[72] Information also emerged that the government had in recent years increased its purchases of interception equipment.[73] Moreover, in March 2012, a scandal resurfaced over the activities of the Civil

[67] "Nate, Cyworld Hack Stole Information From 35 Million Users: SKorea Officials," The Huffington Post, July 28, 2011, http://www.huffingtonpost.com/2011/07/28/south-korea-nate-cyworld-hack-attack_n_911761.html.
[68] Eric Pfanner, "Naming Names on the Internet," The New York Times, September 4, 2011, http://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html.
[69] Ja-young Yoon, "Online ID system faces overhaul," The Korea Times, December 23, 2011, http://www.koreatimes.co.kr/www/news/biz/2011/12/123_101459.html.
[70] Ji-yoon Lee, "Korea to ban online collection of resident numbers," The Korea Herald, April 20, 2012, http://view.koreaherald.com/kh/view.php?ud=20120420000712&cpv=0; Kate Jee-hyung Kim, "Lessons Learned from South Korea's Real-Name Policy," Korea IT Times, January 17, 2012, http://www.koreaittimes.com/story/19361/lessons-learned-south-koreas-real-name-verification-system.
[71] Bon-kwon Koo, "Internet real name confirmation system to be abolished," [in Korean] The Hankyoreh, December 30, 2011, http://english.hani.co.kr/arti/english_edition/e_national/512617.html.
[72] Hyeon-ung Roh, "Even Gmail is under surveillance of NIS," [in Korean] The Hankyoreh, September 16, 2011, http://www.hani.co.kr/arti/society/society_general/496439.html.
[73] Jieun Lee, "Under MB administration purchases of packet eavesdropping equipment increase each year," [in Korean] The Hankyoreh, September 21, 2011, http://www.hani.co.kr/arti/politics/politics_general/497155.html. ; Sang-man Kim, "Somebody Is Watching You: From 'Big Brother' to 'Big Browser'," [in Korean] Media Today, February 3, 2010, http://www.mediatoday.co.kr/news/articleView.html?idxno=85800; "NIS confirms increasing packet eavesdropping equipment supply," [in Korean] The Hankyoreh, November 17, 2009, http://english.hani.co.kr/arti/english_edition/e_national/388103.html.

Service Ethics Division, established in 2008. The division reports directly to the prime minister and is tasked with identifying corruption among civil servants. However, a major television station posted online over 2,600 documents containing the alleged results of monitoring conducted on a wide range of citizens, including politicians, journalists, and civic activists. Seven division members were convicted in 2010 for carrying out illegal surveillance against two civilians, including one who had posted online a video critical of the president. The 2012 revelations sparked renewed calls for a more comprehensive investigation of the entity's activities.[74]

There have been no reports of physical violence against bloggers, but a notable increase in technical disruptions in 2011 highlighted vulnerabilities in the country's ICT infrastructure.[75] Besides the above-mentioned attack on Nate/Cyworld, high-profile attacks also targeted Hyundai Capital (in April 2011, compromising the data of 23 percent of its 1.8 million customers), the Agricultural Cooperative Bank (reportedly launched by North Korea in April 2011, resulting in paralysis of the system for weeks[76]), the news satire website Ddanzi Ilbo (allegedly carried out by politically motivated contract hackers in July 2011, resulting in complete deletion of its data[77]), and the online gaming company Nexon (in November 2011, exposing the personal information of over 13 million subscribers[78]).

Perhaps the most politically significant attack, however, was a distributed denial of service (DDoS) attack on a section of the NEC website on the day of the mayoral by-election in October. Information on polling stations was made unavailable during morning hours when a large proportion of young, liberal-leaning constituents were expected to vote en route to work. This gave rise to speculation that the attacks were politically motivated and intended to rig the elections in favor of the ruling conservative party. In December 2011, the personal assistant of ruling party lawmaker Choi Gu-shik was arrested for involvement in

[74] Christian Oliver, "South Korean 'Watergate' rocks election campaign," FT.com, April 2, 2012, http://www.ft.com/intl/cms/s/0/ab0de5f4-7ca8-11e1-8a27-00144feab49a.html#axzz21ejqwo1j; Choe Sang-Hun, "In South Korea Scandal, Echoes of Watergate," The New York Times, April 9, 2012, http://www.nytimes.com/2012/04/10/world/asia/government-spying-charges-complicate-korean-vote.html?pagewanted=all. ; Asian Human Rights Commission, "South Korea: Korean style of 'Watergate Scandal'?," Scoop World News, March 31, 2012, http://www.scoop.co.nz/stories/WO1203/S00663/south-korea-korean-style-of-watergate-scandal.htm.

[75] Reuters, "South Korea discovers downside of high speed internet and real-name postings," The Guardian, December 6, 2011, http://www.guardian.co.uk/technology/2011/dec/06/south-korea-hacking-problems.

[76] "North Korea 'behind South Korean bank cyber hack'," BBC News, May 3, 2011, http://www.bbc.co.uk/news/world-asia-pacific-13263888.

[77] Yong-in Jeong, "Who's behind hacking Ddanzi Ilbo?" [in Korean] Weekly Kyunghyang, August 2, 2011, http://newsmaker.khan.co.kr/khnm.html?mode=view&code=115&artid=201107271904571&pt=nv.

[78] Ja-young Yoon, "Online ID system faces overhaul," The Korea Times, December 23, 2011, http://www.koreatimes.co.kr/www/news/biz/2011/12/123_101459.html.

the attack, reinforcing such suspicions and sparking calls for further investigation despite police claims the assistant acted alone.[79]

[79] John Leyden, "Row over Korean election DDoS attack heats up," The Register, December 7, 2011, http://www.theregister.co.uk/2011/12/07/korean_election_ddos_row/; Sun-hui Yu, "GNP secretary arrested on charges of Election Day DDoS attack," [in Korean] The Hankyoreh, December 3, 2011, http://english.hani.co.kr/arti/english_edition/e_national/508382.html; Yoo Eun Lee, "South Korea: Anger and Suspicion Grows Over Election Rigging," Global Voices (blog), January 10, 2012, http://globalvoicesonline.org/2012/01/10/south-korea-anger-and-suspicion-grows-over-election-rigging/.

SRI LANKA

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access (0-25)	n/a	16
Limits on Content (0-35)	n/a	18
Violations of User Rights (0-40)	n/a	21
Total (0-100)	**n/a**	**55**

* 0=most free, 100=least free

POPULATION: 21 million
INTERNET PENETRATION 2011: 15 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Since coming into power in 2005, the ruling United People's Freedom Alliance (UPFA) has pursued an ambitious information, communications, and technology (ICT) policy characterized by the widespread provision of internet access and improvement in digital literacy. The new government's initiatives have also led to the adoption and further development of the decade-old e-Sri Lanka project, which is geared towards building "information infrastructure and an enabling environment, developing ICT human resources… leveraging ICT for economic and social development,"[1] and providing access to "diverse and unrestricted sources of information and means of communication."[2]

Despite recognition of the internet's value and impact on economic growth, the military campaign against the Liberation Tigers of Tamil Eelam (LTTE, or Tamil Tigers)—which ended in May 2009—hindered adequate investment in the ICT sector and expansion of the internet across the country. Furthermore, the empowering impact of the internet in Sri Lanka has been undermined by the government's efforts to arbitrarily block, filter, and regulate online content that provides dissenting views and reportage on sensitive political issues.

[1] "Programmes," Information Communication Technology Agency (ICTA), accessed July 13, 2012, http://www.icta.lk/en/programmes.html.
[2] "Establishment of Nenasalas," Nenasala, accessed July 13, 2012, http://www.nanasala.lk/.

In January 2007, internet access and mobile phone connections in the northern and eastern regions of the country were disconnected on account of national security concerns.[3] In the same year, the government made its first attempt to clamp down on online content in response to reportage on the military campaign against the LTTE and civilian casualties.[4] While there is a clear trend with respect to the restriction of online content under the current government, since 2007 there has also been an incremental growth in the number of online news sites, new media initiatives, and the leveraging of social media for socioeconomic and political activism. However, in a post-war context, the arbitrary blocking of websites has continued in 2011—a trend that contradicts the government's own recognition of the role of ICTs in promoting access to information and free of expression—and the government has expressed a need for greater regulation of online content.[5]

OBSTACLES TO ACCESS

The internet was first introduced in Sri Lanka in 1995, but penetration remained low for many years. Fifteen percent of the population had access to the internet in 2011, up from 2.5 percent in 2006.[6] Government expenditure and private investment in the information technology (IT) sector has gradually increased, leading to the implementation of several projects for the development of an island-wide telecommunications infrastructure.[7] In July 2011, it was announced that WiFi zones would be established with a focus on providing internet access in schools, government buildings, and public transport areas.[8]

Notwithstanding a literacy rate of 94.2 percent—the second highest in the region—and increased investment in the sector, a critical barrier to the penetration of ICTs is digital literacy, which stood at 35 percent in 2011 according to the Department of Census and Statistics.[9] Digital literacy is higher in urban over rural areas due to unaffordable personal computers and/or laptops, which affects lower-income families, the lack of a substantive IT

[3] "Cutting off Telecoms in Sri Lanka Redux…," Groundviews, January 30, 2007, http://groundviews.org/2007/01/30/cutting-off-telecoms-in-sri-lanka-redux/.
[4] "Tamilnet blocked in Sri Lanka," BBC, June 2007, http://www.bbc.co.uk/sinhala/news/story/2007/06/070620_tamilnet.shtml.
[5] Sarath Kumara, "Sri Lankan government prepares new Internet restrictions," World Socialist Web Site, February 15, 2010, http://www.wsws.org/articles/2010/feb2010/slmd-f15.shtml.
[6] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[7] Ministry of Finance and Planning: Sri Lanka, "Annual Report 2010," March 31, 2011, p.89, http://www.treasury.gov.lk/reports/annualreport/AnnualReport2010-eng.pdf; "Sri Lanka Dialog to invest US$150mn in expansion," Lanka Business Online, February 11, 2011, http://www.lankabusinessonline.com/fullstory.php?nid=754125283.
[8] Damith Wickremasekara, "Lanka to get WiFi zones," The Sunday Times, July 31, 2011, http://sundaytimes.lk/110731/News/nws_14.html.
[9] Department of Census and Statistics, Sri Lanka, "Computer Literacy Survey – 2009," December 2009, http://www.statistics.gov.lk/CLS/BuletinComputerLiteracy_2009.pdf.

literacy program instituted at all schools with adequate IT facilities, and the unavailability of software compatible with the Sinhala and Tamil language. However, as part of the e-Sri Lanka project, the government has supported the Nenasala (Knowledge Centre) project through the Information Communication Technology Agency (ICTA) to address the issue of literacy and access in rural areas.[10] Furthermore, the availability of computers in households both within urban and rural areas is increasing, with higher acquisition rates reported between 2005 and 2009, particularly in rural areas.[11]

There are additional concerns about the extent to which broadband penetration, which is the lowest in the region at 6 percent of the population, will increase given relatively high market prices and a low penetration of computers.[12] Nevertheless, reports in March 2011 indicate that the price of commercial broadband had been reduced as service providers lowered leased line prices in order to attract foreign ICT and business process outsourcing firms.[13] In a country with an estimated 16 million mobile phone users and a mobile penetration rate of over 87 percent in 2011,[14] increasing internet access through mobile broadband is also a challenge, limited primarily by expensive 3G/3.5G mobile handsets.[15]

In addition to the requirements of an expanding economic sector, the demand for internet access is driven by a growing youth population and its engagement with YouTube, Facebook, Twitter and international blog-hosting services, which are all freely available and widely-used. As of March 2012, there are over 1.2 million Facebook users in Sri Lanka and 1,084 blogs syndicated on the blog aggregator www.kottu.org.[16]

The two largest internet service providers (ISPs) are Dialog Axiata and Sri Lanka Telecom (SLT). The latter commands more than 50 percent of the market, and a majority of its

[10] Objectives of the Nenasala initiative: "…to establish multi-service community information centres which provide access to internet, e-mail, telephones, fax, photocopy, computer training classes and other ICT services as well act as a hub of local, national and global information resources to provide an catalytic effect for the rural communities in poverty reduction, social and economic development and peace building while aiming at providing these services in a long-term, sustainable manner." Source: ICTA's 1000 Nenasala (Knowledge Centre) Project, http://www.nanasala.lk/.

[11] Department of Census and Statistics, Sri Lanka, "Computer Literacy Survey – 2009," December 2009; "Computer Literacy among Sri Lankans is in the ascension," Media Center for National Development of Sri Lanka, June 23, 2010, http://www.development.lk/news.php?news=620.

[12] "Sri Lanka broadband use weak due to costs, low PC penetration: Fitch study," Lanka Business Online, May 25, 2011, http://www.lankabusinessonline.com/fullstory.php?nid=1415055027.

[13] Rohan Samarajiva, "Sri Lanka: Leased line prices to be lowered to encourage BPO business and Internet use," Lirne Asia, March 9, 2011, http://lirneasia.net/2011/03/sri-lanka-leased-line-prices-to-be-lowered-to-encourage-bpo-business-and-internet-use/.

[14] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[15] Zulfath Suaheed, "Sri Lanka mobile internet usage poised for growth: Nielsen," Lanka Business Report, March 4, 2011, http://www.lbr.lk/fullstory.php?nid=201103041615077468.

[16] For the information on Facebook availability, see: "Sri Lanka Facebook Statistics," Socialbakers, accessed July 13, 2012, http://www.socialbakers.com/facebook-statistics/sri-lanka/last-week#chart-intervals.

shares is owned by the state. The broadband market is competitive and a few firms dominate wholesale access; however, SLT has the largest fiber-optic national backbone.[17] While there is no legal monopoly of the market, there is also absolutely no legal requirement for SLT to sell backbone access to its competitors. In contrast, Dialog Axiata has allowed wholesale access to its backbone network.[18] For mobile phones, the main service providers in the country are Dialog Axiata, which has the largest customer base of over six million subscribers, Mobitel (a subsidiary of SLT with a customer base of 3.8 million[19]), Bharti Lanka (with 1.8 million customers), Etisalat (with 3.5 million customers), and Hutchison Telecommunication (with under one million customers).

The regulatory environment under the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) has led to concerns about transparency, independence, and overt politicization.[20] Following the ratification of Eighteenth Amendment to the Constitution in October 2011, which removed term limits to the executive presidency and allows the president to appoint the heads and members of all commissions,[21] any legislative guarantees for the independence of the TRCSL (and other statutory institutions) were subverted. The TRCSL now falls under the ambit of President Rajapaksa,[22] who appointed his permanent secretary as the Commission's chairman. The regulatory body's interventions to restrict online content and pronouncements on strengthening online regulation have been viewed as partisan, extralegal, and overly repressive.[23]

LIMITS ON CONTENT

Since 2007, there have been numerous cases of arbitrary blocks on websites that report on human rights violations, corruption, and governance issues. These instances have occurred alongside the consistent failure by authorities to provide a legal basis for the blocks, follow due process in terms of judicial intervention in order to legitimize any move to restrict

[17] Helani Galpaya, *Broadband in Sri Lanka: Glass Half Full or Half Empty?* (Washington, D.C,: infoDev/The World bank, 2001), http://www.broadband-toolkit.org/.
[18] Ibid.
[19] Bandula Sirimanna, "Mobitel reached 3.8 million subscribers by Nov. 2010," The Sunday Times, January 9, 2011, http://sundaytimes.lk/110109/BusinessTimes/bt46.html.
[20] Under the Telecommunications Act No. 21 of 1994, the Minister of Telecommunications and Information Technology has sole discretion in issuing licenses and imposition of license conditions based on the recommendations of the TRCSL.
[21] Eighteenth Amendment to the Constitution, October 2010, http://www.priu.gov.lk/Cons/1978Constitution/18th%20Amendment%20To%20Sri%20Lanka%20Constitution%20(2).pdf.
[22] "Statutory Institutions and Ministries under the Executive President," Democratic Socialist Republic of Sri Lanka, accessed July 13, 2012, http://www.president.gov.lk/about_presidency.php.
[23] Sarath Kumara, "Sri Lankan government prepares new Internet restrictions," World Socialist Web Site, February 15, 2010, http://www.wsws.org/articles/2010/feb2010/slmd-f15.shtml.

content, or protect partisan interests when it comes to content that is critical of government policies and actions.[24]

It is not clear whether the government possesses the expertise and funds to implement sophisticated methods of online content restriction—such as deep-packet inspection (DPI), real time filtering, and offline filtering—although there are unofficial reports that one or two Sri Lankan telecoms might have DPI programs for the enhancement of mobile data services. There were also reports in 2010 of IT experts from China's military intelligence division assisting the government in blocking "offensive" websites.[25]

The current system of censoring online content involves monitoring websites that publish sensitive political content and blacklisting them under the TRCSL, which requests ISPs to block access to blacklisted websites in the country. Any legal requirement for ISPs to comply to requests from the TRCSL to block websites are based on either specific license conditions—which is difficult to confirm given the lack of transparency in licensing—or political pressure. However, existing license conditions for ISPs also involve compliance with directions to act with the consent of the TRCSL and to address any matter that the ministry may find "…requisite or expedient to achieving the objectives" of the TRCSL.[26]

In the absence of an independent body for redress, a fundamental rights application challenging the blocking of a website or the imposition of any other restrictions remains the only method for appealing online freedom of expression violations. However, the application is rarely pursued due to a lack of trust in the country's politicized judiciary and fears of setting a repressive precedent.[27]

Since 2007, the regime's efforts at web censorship have focused primarily on targeting websites that report on human rights issues, government accountability, corruption, and political violence. The frequency with which websites are blocked increased considerably after 2009 when the government began restricting pornographic websites and the police sought to ban access to pornography on mobile phones.[28] However, instances of blocks on websites have not been properly coordinated or comprehensive, with some targeted

[24] "Chapter 4: Restriction of Content on the Internet," *Freedom of Expression on the Internet*, Centre for Policy Alternatives, November 2011, http://www.scribd.com/doc/73393066/Freedom-of-Expression-on-the-Internet-in-Sri-Lanka.
[25] Bandula Sirimanna, "Chinese here for cyber censorship," The Sunday Times, February 14, 2010, http://sundaytimes.lk/100214/News/nws_02.html.
[26] *Freedom of Expression on the Internet in Sri Lanka*, Centre for Policy Alternatives, November 2011, pg. 30, http://www.scribd.com/doc/73393066/Freedom-of-Expression-on-the-Internet-in-Sri-Lanka,
[27] International Crisis Group, "Sri Lanka's Judiciary: Politicised Courts, Compromised Rights," Asia Report No.172, January 30, 2009, http://www.crisisgroup.org/en/regions/asia/south-asia/sri-lanka/172-sri-lankas-judiciary-politicised-courts-compromised-rights.aspx.
[28] Indika Sri Aravinda, "Police seek mobile porn ban," Daily Mirror, May 12, 2010, http://www.dailymirror.lk/news/3705-police-seeks-mobile-porn-ban.html.

websites available at times on one or more ISPs and at other times inaccessible on all ISPs. One particular case is Tamilnet.com, which has been blocked since 2007 and continues to be blocked in 2011, but not uniformly across all fixed-line and mobile broadband networks.[29] In 2009, SLT blocked access to most of the Tamil news websites that operate outside the country, but most of these sites were accessible throughout 2010 and 2011. In June 2011, the citizen media sites, Groundviews.org and Vikalpa.org, were temporarily blocked for a day on SLT broadband services but remained accessible on other ISPs,[30] and in October 2011, the news website Lankaenews.com was blocked allegedly due to coverage of intra-party violence associated with the Sri Lanka Freedom Party (SLFP), President Mahinda Rajapaksa's ruling party.[31]

In November 2011, five popular news websites known for their reporting on human rights, governance issues, and corruption were arbitrarily blocked.[32] Prior to this incident, the government and the TRCSL had never admitted to blocking websites but did so in this case on the premise of concerns about defamation and the violation of privacy. In December 2011 and intermittently in November 2011, Colombotelegraph.com, a news and commentary website run by exiled Sri Lankan journalists, was also blocked with absolutely no justification provided by authorities,[33] but is accessible as of early 2012. The authorities have occasionally blocked website domains hosted on the servers of blogging platforms rather than specific blogs themselves,[34] although only a few of the most popular blogs publish political content and dissenting narratives.

In addition to its blocking activities, the government has been intensifying its efforts to restrict internet and mobile phone content. For example, the government announced in December 2011 plans to introduce more comprehensive legislation to control internet use, including the use of Facebook, ostensibly to crackdown on child abuse online.[35] On March 9, 2012, the Media Centre for National Security (MCNS) announced that mobile phone SMS news alerts on matters related to "…national security and security forces, the

[29] Sanjana Hattotuwa, "Tamilnet.com accessible once more in Sri Lanka via SLT ADSL," ICT for Peacebuilding (blog), August 5, 2010, http://ict4peace.wordpress.com/2010/08/05/tamilnet-com-accessible-once-more-in-sri-lanka-via-slt-adsl/.
[30] "Groundviews blocked and unblocked," ICT for Peacebuilding (blog), June 22, 2011, http://ict4peace.wordpress.com/2011/06/22/groundviews-blocked-and-unblocked/.
[31] "In Sri Lanka, anti-government website blocked," Committee to Protect Journalists, October 19, 2011, http://www.cpj.org/2011/10/in-sri-lanka-access-to-anti-government-website-blo.php.
[32] The following five websites were blocked on the 5th of November 2011: www.lankanewsweb.com, www.srilankamirror.com, www.srilankaguardian.com, www.lankawaynews.com, www.lankaenews.com.
[33] "We are blocked but will not be stopped," Colombo Telegraph, December 26, 2011, http://www.colombotelegraph.com/index.php/we-are-blocked-but-we-will-not-be-stopped/.
[34] "More websites including ghs.google.com blocked in Sri Lanka?" ICT for Peacebuilding (blog), July 29, 2009, http://ict4peace.wordpress.com/2009/07/29/more-websites-including-ghs-google-com-blocked-in-sri-lanka/.
[35] Indika Sri Aravinda, "Government to Monitor Internet," The Sunday Leader, December 18, 2011, http://www.thesundayleader.lk/2011/12/18/government-to-monitor-internet/.

police…" must be approved by the MCNS[36] prior to dissemination,[37] which could result in the censorship of news related to the security establishment. The MCNS, however, did not delineate the possible consequences of failing to comply with this directive and the legal basis upon which it could issue such an order.

A majority of the alternative news websites—such as Srilankaguardian.org, Colombotelegraph.com, and Tamilnet.com—are operated by exiled journalists and publish news covering human rights violations, political violence, and corruption, while online news sites of the mainstream media are more likely to self-censor controversial content out of fear of reprisals. In fact, self-censorship "on matters that would damage the integrity of the island" is actually encouraged by the current government.[38] The few pro-government websites in existence are the online platforms of the main state-run newspaper, a broadcasting network, and other news initiatives that are inclined towards the incumbent government.[39]

Despite the restrictions on certain ICT content, there are still diverse, free, and widely accessible sources of information, particularly on socioeconomic and political issues written in English, Sinhala, and Tamil. Notwithstanding the intermittent blocking of the Human Rights Watch website during the height of civil war in 2009,[40] all other websites of major international media institutions, human rights organizations, and media rights groups were freely accessible in the country in 2011. The emergence of blogs and social media has contributed to creating a space for the anonymous and pseudonymous critique of governance, development, political process, human rights and policymaking within government. The impact of citizen media initiatives such as Groundviews.org and Vikalpa.org is a demonstration of the increased engagement of human rights activists,[41] political commentators,[42] citizens,[43] and local as well as international journalists[44] who bear

[36] The MCNS and Secretary of Defense issued a similar directive in 2006: "Any news gathered by your institution through your own sources with regard to national security and defense should be subjected to clarification and confirmation from the MCNS in order to ensure that correct information is published, telecast or broadcast" – "Sri Lankan defence authorities impose unofficial censorship," World Socialist Web Site, October 11, 2006, http://www.wsws.org/articles/2006/oct2006/sri-o11.shtml.
[37] "New censorship of SMS news in Sri Lanka," Groundviews, March 12, 2012, http://groundviews.org/2012/03/12/new-censorship-of-sms-news-in-sri-lanka/.
[38] Dinidu De Alwis, "Media should exercise self-censorship," Ceylon Today, March 23, 2012, http://www.ceylontoday.lk/16-3780-news-detail-media-should-exercise-self-censorship-lakshman-yapa.html.
[39] "Namal's disclosure of family embarrassment," The Island, December 21, 2011, http://www.island.lk/index.php?page_cat=article-details&page=article-details&code_title=41622.
[40] Reporters Without Borders, "Internet Enemies - Countries under surveillance: Sri Lanka," March 12, 2009, http://www.unhcr.org/refworld/country,,RSF,COUNTRYREP,LKA,,4a38f97fc,0.html.
[41] "Jaffna: Brutal Assault of Civilians in Navanthurai," Groundviews, August 25, 2011, http://groundviews.org/2011/08/25/jaffna-brutal-assault-of-civilians-in-navanthurai/.
[42] "Jaffna and the Vanni today: Reality beneath the rhetoric," Groundviews, March 17, 2011, http://groundviews.org/2011/03/17/jaffna-and-the-vanni-today-the-reality-beneath-the-rhetoric/.
[43] "First images: The flooding in Menik Camp and the increasingly dire situation for IDPs," Groundviews, August 15, 2009, http://groundviews.org/2009/08/15/first-images-the-flooding-in-menik-camp-and-the-increasingly-dire-situation-for-idps/.

witness to critical post-war issues and provide reportage on topics that would otherwise not be covered by mainstream media in the country.

VIOLATIONS OF USER RIGHTS

The right to freedom of speech, expression and publishing is guaranteed under Article 14 (1)(a) of the Constitution but is subject to numerous restrictions for the protection of national security, public order, racial and religious harmony as well as morality. The Supreme Court has recognized the "indispensability" of freedom of expression to the "operation of a democratic system" and the importance of wide dissemination from "diverse and antagonistic sources."[45] However, there is no specific provision under the Constitution that recognizes access to the internet as a fundamental right or guarantees online freedom of expression. Further, the Supreme Court has never had the opportunity to consider the applicability of existing freedom of expression guarantees to the internet.

The laws that impact the use of ICTs in the country are focused primarily on computer crimes and intellectual property rights violations, and they allow information contained within computers to be admissible in civil and criminal proceedings. It is also an offense to report on or publish official secrets, information about parliament that may undermine its work, malicious content and any content that could be considered an incitement to violence or cause disharmony.[46] As a result, online content that can be deemed an incitement to ethnic and religious violence, or poses a threat to national security, runs the risk of restriction and/or criminalization.

A key issue with the existing legislation is its overly broad scope and lack of detailed definitions, which may be used to prosecute or restrict legitimate forms of online expression. For example, in October 2011, the Ministry of Justice announced that it would introduce new legislation on obscenity in order to prevent the circulation of pornography with specific mention of regulating obscene content on "electronic media."[47] However, as with previous legislation on obscenity, the ministry failed to provide an exact definition of what is constituted as "obscene."

[44] "Northern Local Government Elections," Groundviews, July 23, 2011, http://groundviews.org/2011/07/23/local-government-elections-in-jaffna/; Charles Haviland, "A question Sri Lanka's leader's keep dodging: Where are the disappeared?" Groundviews, March 21, 2012, http://groundviews.org/2012/03/21/a-question-sri-lankas-leaders-keep-dodging-where-are-the-disappeared/.

[45] Joseph Perera v AG (1992) 1 SLR 199, at 202 per Sharvananda CJ.

[46] Respective legislation: Official Secrets Act No. 32 of 1955; Parliament (Powers and Privileges) (Amendment) 1997; Prevention of Terrorism (Temporary Provisions) Act No. 48 of 1979.

[47] "Tough new laws against porn," Daily Mirror, October 24, 2011, http://www.dailymirror.lk/news/14318-tough-new-laws-against-porn.html.

The Lessons Learnt and Reconciliation Commission[48] (LLRC)—a key post-war commission of inquiry appointed by President Rajapaksa in May 2010—highlighted the importance of freedom of expression and the right to information[49] in its final report, which was released in November 2011.[50] As of March 2012, the government had still not put forward a roadmap or time frame for the implementation of the recommendations detailed in the LLRC's report.

A culture of impunity, circumvention of the judicial process through arbitrary action, and a lack of adequate protection compound the poor enforcement of freedom of expression guarantees. Furthermore, online journalists and bloggers are not afforded the same rights and protection as broadcast and print journalists. In November 2009, the Criminal Investigations Department (CID) arrested a blogger for using the internet to make offensive comments about the president and secretary of defense.[51] No information was provided about the legal basis of the arrest, exact nature of the content, and why this specific case resulted in such action. There have also been arrests based on the content of text messages, revealing the possible existence of a sophisticated surveillance regime. During the 2010 presidential election, the authorities detained opposition supporters who had accused the government of electoral fraud via text messages[52] and other supporters for sending out text messages to organize protests following the announcement of the election results.[53]

Despite the fact that extrajudicial surveillance of personal communications is prohibited under the Telecommunications Act No.27 of 1996, this law can be circumvented by an order from a minister or by an employee of a telecommunication service acting in "pursuance of his official duty."[54] Additionally, there is no provision under the legislation that requires officials to notify a user that s/he is under surveillance. For example, in 2010, there were reports of Facebook and Twitter users being monitored in an effort to clamp

[48] The Lessons Learnt and Reconciliation Commission (LLRC) website: http://www.llrc.lk/.
[49] An attempt by the United National Party, the main opposition party in the country, to put forward a Right to Information bill was defeated in Parliament in June 2011: "Govt. rejects our right to know," Sunday Times, June 26, 2011, http://sundaytimes.lk/110626/Columns/political.html.
[50] The report further recommended that legislation be enacted "to ensure the right to information" and that steps need to be taken in order to "prevent the harassment and attacks on media personnel and institutions." *Report of the Commission of Inquiry on Lessons Learnt and Reconciliation*, The Official Website of the Government of Sri Lanka, 2011, pp.197-8, http://www.priu.gov.lk/news_update/Current_Affairs/ca201112/FINAL%20LLRC%20REPORT.pdf.
[51] "Blogger arrested in Sri Lanka for 'offensive' comments regarding President and Defense Secretary?" ICT for Peacebuilding (blog), November 1, 2009, http://ict4peace.wordpress.com/2009/11/01/blogger-arrested-in-sri-lanka-for-offensive-comments-regarding-president-and-defense-secretary/.
[52] Sarath Kumara, "Sri Lankan government prepares new Internet restrictions," World Socialist Web Site, February 15, 2010, http://www.wsws.org/articles/2010/feb2010/slmd-f15.shtml.
[53] "Fonseka plotted against President: Hulugalle," Campaign for Free & Fair Elections, January 29, 2010, http://caffesrilanka.org/Present%20Election-2----119.html.
[54] Interception of personal communications by a telecommunications officer can also occur under the direction of a Minister, as directed by the Court and in connection with the investigation of a criminal offence, as provided under the Telecommunications Act No. 27 of 1996, October 23, 1996, http://www.trc.gov.lk/images/pdf/ACT_27_1996.pdf.

down on dissent against the government, raising suspicions that the authorities were either hacking into user accounts or setting up fake accounts for infiltration.[55]

The threat to user rights in the country is further exacerbated by the lack of substantive laws for the protection of individual privacy and data respectively, which is extremely problematic given the government's proclivity for pervasive surveillance.[56] The involvement of Chinese telecoms, such as ZTE[57] and Huawei,[58] in the development and maintenance of Sri Lanka's ICT infrastructure has also raised concerns about the possibility of backdoor espionage and surveillance,[59] which is in line with international reportage about Chinese telecoms assisting Central Asian states with surveillance or "eavesdropping" technologies.[60] Nevertheless, it is not clear what exact technology or a prospective technical framework for it has been transferred in order to buttress the country's censorship and surveillance regime.

In November 2011, the Government Information Department instituted a registration policy for certain websites, stating that sites "carrying any content relating to Sri Lanka or the people of Sri Lanka" should register with the Ministry of Mass Media and Information.[61] The request was criticized for its lack of clarity and necessity as well as infeasibility, particularly in terms of the possible imposition of liability for content published, the categories of websites that are required to register, and the legal framework under which registration could be imposed.[62] There was also concern expressed about the compliance of ISPs to arbitrary requests for blocking websites without the requirement of judicial intervention. A similar announcement was made in 2010 by the Ministry of Defense concerning the registration of mobile phone users to collect user information for the purpose of "curbing negative incidents," which included "raising unnecessary alarm or

[55] Sarath Kumara, "Sri Lankan government prepares new Internet restrictions," World Socialist Web Site, February 15, 2010, http://www.wsws.org/articles/2010/feb2010/slmd-f15.shtml.
[56] "It's ok for government to infiltrate online privacy of Sri Lankan citizens?" ICT for Peacebuilding (blog), April 17, 2010, http://ict4peace.wordpress.com/2010/04/17/its-ok-for-government-to-infiltrate-online-privacy-of-sri-lankan-citizens/.
[57] ZTE Corporation signed an agreement with Mobitel to develop its 4G(LTE) network and carried out successful trials in May 2011: "Sri Lanka's Mobitel and ZTE Corporation Carry Out the First Successful 4G(LTE) Trial in South Asia," ZTE, May 17, 2011, http://wwwen.zte.com.cn/en/press_center/news/201105/t20110517_234745.html; Pamela Weaver, "Sri Lanka hits the LTE road with trials, rollouts," Telecoms, May 10, 2011, http://www.telecoms.com/27530/sri-lanka-hits-the-lte-road-with-trials-rollouts/.
[58] Sri Lanka Telecom's (SLT) ADSL infrastructure is supported by Huawei Technologies: Ranjith Wijewardena, "SLT tie up with Huawei to expand Broadband Internet coverage," Nanasala, September 29, 2006, http://www.nanasala.lk/article_more.php?id=10.
[59] Sanjana Hattotuwa, "Are Chinese Telecoms acting as the ears for the Sri Lankan government?" Groundviews, February 16, 2012, http://groundviews.org/2012/02/16/are-chinese-telecoms-acting-as-the-ears-for-the-sri-lankan-government/.
[60] Deirdre Tynan, "Central Asia: Are Chinese Telecoms Acting as the Ears for Central Asian Authoritarians?" Eurasianet, February 15, 2012, http://www.eurasianet.org/node/65008.
[61] "Website ban further broadened on News Director General notification," Lanka-e-news, November 5, 2011, http://www.lankaenews.com/English/news.php?id=12427.
[62] "Arbitrary Blocking and Registration of Websites: The Continuing Violation of Freedom of Expression on the Internet," Centre for Policy Alternatives, November 9, 2011, http://cpalanka.org/arbitrary-blocking-and-registration-of-websites-the-continuing-violation-of-freedom-of-expression-on-the-internet/.

creating panic."[63] While the directive and penalty of disconnection for users failing to register was never enforced, real name registration and the provision of identity and banking documents has been a standard policy for mobile phone subscription.

In December 2011, the operator of a website who challenged the blocking of his site through a fundamental rights petition at the Supreme Court agreed to a settlement with the TRCSL and other institutions. In return for lifting the block on the website, the settlement required compliance with several terms and conditions that included the immediate registration of the website with the TRCSL and Ministry of Mass Media and Information. The website was also required to "delink" other sites blocked by the TRCSL.[64]

While the possibility of legal penalties threatens freedom of expression online, online reporters and web users in Sri Lanka have faced various forms of physical intimidation and violence. On January 24, 2010, the Lankaenews.com online journalist and cartoonist, Prageeth Ekneligoda, was abducted and little progress has been made on his case despite widespread international pressure for progress with investigations.[65] It is speculated that Ekneligoda was abducted because of his anti-government writing, and at present, the government appears to have very little concern about the case, opting instead to accuse Ekneligoda of seeking asylum and living in hiding in another country.[66] Sri Lanka is ranked fourth on the Committee to Protect Journalists Impunity Index with nine unsolved murders.

In January 2011, over a year after the abduction of Ekneligoda, there was an arson attack on the offices of Lankaenews.com,[67] which was followed a few months later by the arrest of the website's editor and another journalist on charges of intimidation and contempt of court, respectively.[68] The attack and increased restrictions on websites as well as the continuing

[63] Bandula Sirimanna, "Sri Lanka to tighten mobile phone regulations," The Sunday Times, October 31, 2010, http://sundaytimes.lk/101031/BusinessTimes/bt32.html.
[64] S.S Selvanayagam, "Website previously blocked now permitted to operate by SC," DailyFT, December 16, 2011, http://webcache.googleusercontent.com/search?q=cache:rItgZngzetsJ:www.ft.lk/2011/12/16/website-previously-blocked-now-permitted-to-operate-by-sc/+website+previously+blocked+now+permitted+to+operate+by+SC&cd=1&hl=en&ct=clnk&gl=lk.
[65] T. Farook Thajudeen, "Prageeth Eknaligoda disappearance case still going on," Daily Financial Times, December 24, 2011, http://www.ft.lk/2011/12/24/prageeth-eknaligoda-disappearance-case-still-ongoing/; "UN heard Eknelygoda's cry for help; husband still missing," Committee to Protect Journalists, May 21, 2011, http://cpj.org/blog/2011/03/un-heard-eknelygodas-cry-for-help-her-husband-stil.php#more.
[66] Chris Kamalendran, "Eknaligoda case: Focus on Ex-AG," Sunday Times, December 11, 2011, http://sundaytimes.lk/111211/News/nws_24.html.
[67] "United Nations must intervene to protect Sri Lanka's media," Committee to Protect Journalists, January 31, 2011, http://cpj.org/2011/01/united-nations-must-intervene-to-protect-sri-lanka.php.
[68] "Another Lankaenews journalist arrested," Committee to Protect Journalists, April 25, 2011, http://www.cpj.org/2011/04/another-lanka-enews-journalist-arrested.php.

intimidation[69] and assault[70] of mainstream journalists reinforce the chilling effect on freedom of expression in the country and widespread self-censorship.

An additional threat to internet freedom is the rise of cyber-threats, particularly with regard to privacy breaches on social media and email accounts.[71] The issue of technical violence such as cyberattacks against websites is largely focused on the activities of cyber-terrorist networks associated with the LTTE that have attempted to hack into national security networks and carry out web defacement attacks.[72] The government has recognized the need to strengthen its defensive capability in order to prevent further cyberattacks and combat web propaganda campaigns, leading to the purchase of more sophisticated surveillance technology, which could in turn be used to restrict legitimate forms of expression on the internet.

[69] "Sunday Leader Editor Threatened Again," The Sunday Leader, December 11, 2011, http://www.thesundayleader.lk/2011/12/11/sunday-leader-editor-threatened-again/.
[70] Chris Kamalendran, "Uthayan news editor brutally attacked," The Sunday Times, July 31, 2011, http://sundaytimes.lk/110731/News/nws_06.html.
[71] "681 SL cyber security incidents so far in 2011," The Sunday Times, October 16, 2011, http://www.sundaytimes.lk/111016/BusinessTimes/bt31.html.
[72] "Sri Lanka Army Commander says Cyber War still continues," ColomboPage, February 22, 2011, http://www.colombopage.com/archive_11/Feb22_1298388902CH.php.

SYRIA

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Not Free**
Obstacles to Access (0-25)	n/a	23
Limits on Content (0-35)	n/a	25
Violations of User Rights (0-40)	n/a	35
Total (0-100)	**n/a**	**83**

* 0=most free, 100=least free

POPULATION: 23 million
INTERNET PENETRATION 2011: 23 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/I USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

The regime of President Bashar al-Assad has maintained tight control over information and communication technologies (ICTs) in Syria for many years, dominating key networks via government-linked service providers and engaging in extensive blocking of websites. The internet was first introduced to Syria in 2000, reaching only 30,000 users that year. By the end of 2010, more than one-fifth of the population was online. It is in the context of such growing access that the internet and social media have played an important role in a civic protest movement, which began in February 2011 calling for the end of al-Assad's rule and which by early 2012 had turned into a full-fledged armed conflict.

Amidst deadly repression and barred entry to foreign correspondents, citizen journalists using mobile phone devices and video-sharing websites have been a critical channel for informing Syrians and the international community about events in the country. In response, the government censorship and retaliation against internet users dramatically intensified. Among the tactics employed have been periodic shutdowns of the internet and mobile phone networks, intensified filtering of websites, and various sophisticated means of monitoring and tracking internet users' online activities. In addition, Syria has emerged as one of the most dangerous countries in the world for citizen journalists and bloggers, with an untold number arrested and several killed.

OBSTACLES TO ACCESS

Syria's telecommunications infrastructure is one of the least developed in the Middle East, with broadband connections being among the most difficult and expensive to acquire.[1] This dynamic only worsened in 2011 and 2012, as inflation and electricity outages increased dramatically following public protests and the government's corresponding repression. The communications infrastructure was badly damaged, especially in cities like Homs that were subject to particularly severe shelling by the Syrian armed forces. By the end of 2011, the International Telecommunications Union (ITU) estimated that 22.5 percent of the population—around five million people—had used the internet.[2] However, the number of broadband subscribers was only 121,300.[3] Mobile phone penetration was notably higher, reaching about 63 percent of the population at the end of 2011.[4]

In 2009, mobile phone companies began providing 3G services in Syria, though the number of subscribers had reached only 80,000 by late 2010 due to the relatively high prices (almost US$25 for 4 MB or US$200 for unlimited data usage).[5] In addition, MTN, one of two main providers, only offers the service in large cities. Most other users connect to the internet via a dial-up connection and a fixed-line telephone subscription. Most internet users are restricted to speeds of only 256 Kbps, which severely limits their ability to download or view multimedia content. During peak times, the speed is even slower.[6] Broadband ADSL service remains limited for two reasons: a lack of necessary infrastructure in rural areas and relatively high prices, which remain beyond the reach of most Syrians. For example, according to a price list published by the Syrian Computer Society, the monthly cost for a connection speed of 1 Mbps was SYP 1650 (approximately US$30) as of May 2012, in a country where the average monthly per capita income does not exceed US$200.[7]

[1] "Syria - Telecoms, Mobile, Broadband and Forecasts," BuddeComm, accessed March 8, 2012, http://www.budde.com.au/Research/Syria-Telecoms-Mobile-Broadband.html.

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[3] Ibid.

[4] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[5] "Projects to transform Syria into a regional anchor point in the communication" [in Arabic], Alhayat, September 1, 2010, http://international.daralhayat.com/internationalarticle/177606; "What are SURF Postpaid Packages?" [in Arabic], SURF Wireless Broadband, accessed March 8, 2012, http://www.surf.sy/Sitemap/Home/Prices/tabid/214/language/ar-SY/default.aspx.

[6] "Internet Enemies," Reporters Without Borders, March 2011, http://www.reporter-ohne-grenzen.de/fileadmin/rte/docs/2011/110311_Internetbericht_engl.pdf.

[7] "Services and price" [in Arabic], Syrian Computer Society Network (SCS-NET), accessed March 8, 2012 http://www.scs-net.org/portal/OurConnection/OurConnections/SCSADSL/PlansPrices/tabid/493/Default.aspx.

At least eleven internet service providers (ISPs) have entered the market since the end of 2005, raising the total number of ISPs to 14.[8] In practice, however, the country's connection to the international internet remains centralized and tightly controlled by the government. This is done under the purview of the Syrian Information Organization (SIO) and the state-owned Syrian Telecommunications Establishment (STE), which owns all fixed-line infrastructure. Private ISPs like Aya, as well as mobile phone internet providers, are required to sign a memorandum of understanding to connect via the gateways controlled by the SIO.[9] Independent satellite connections are prohibited.[10] This centralization has also contributed to connectivity problems, as the weak and overburdened infrastructure often results in slow speeds and periodic outages.

An ISP can begin operating after procuring a license from the Telecommunications Department and obtaining approval from the security services.[11] Opening a cybercafe has become very difficult, as owners must first obtain approval from the STE and pass security vetting by the Ministry of Interior. Moreover, owners are required to monitor visitors and record their activities. There are two main mobile phone providers in Syria—Syriatel (which is owned by Rami Makhlouf, a cousin of President Bashar al-Assad) and MTN (a subsidiary of the South African company MTN).

Since early 2011, the Syrian government has repeatedly used its centralized control over the internet infrastructure to obstruct connectivity, at times shutting down the internet and mobile phone networks entirely (either nationwide or at particularly sites of unrest). A nationwide shut down was imposed in June 2011 and lasted one day.[12] More localized, but longer lasting cut-offs were reported in Kurdish regions in September 2011, in Aleppo in November, in Daraa and parts of Damascus in December, and in Homs in January 2012.[13] According to activists, every time pro-regime forces begin to besiege a city, the broadband bandwidth is simultaneously reduced to a crawl and 3G services are shut off.[14] In other

[8] "STE is shifting into company in June" [in Arabic], Alwatan, June 12, 2012, http://www.alwatan.sy/dindex.php?idn=124296.
[9] Jaber Baker, "Internet in Syria: experimental goods and a field of a new control," White and Black Magazine, posted on Marmarita website, August 10, 2008, http://www.dai3tna.com/nuke/modules.php?name=News&file=article&sid=6019.
[10] "Online Syria, Offline Syrians," The Initiative For an Open Arab Internet, accessed March 8, 2012; "One Social Network With A Rebellious Message," The Initiative For an Open Arab Internet, accessed March 8, 2012, http://old.openarab.net/en/node/1625.
[11] Ayham Saleh, "Internet, Media and Future in Syria" [in Arabic], The Syrian Center for Media and Free Expression, November 14, 2006, http://alayham.com/%D9%85%D9%82%D8%A7%D9%84%D8%A7%D8%AA/%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA%D8%8C-%D8%A5%D8%B9%D9%84%D8%A7%D9%85-%D8%A7%D9%84%D9%85%D8%B3%D8%AA%D9%82%D8%A8%D9%84-%D9%8A%D9%88%D8%A1%D8%AF-%D9%81%D9%8A-%D8%B3%D9%88%D8%B1%D9%8A%D8%A7.
[12] Christopher Rhoads, "Syria's Internet Blockage Brings Risk of Backfire," Wall Street Journal, June 3, 2011, http://online.wsj.com/article/SB10001424052702304563104576363763722080144.html?mod=googlenews_wsj.
[13] "News From the Ground," [in Arabic], Telecomix: Syria, December 9, 2011, http://syria.telecomix.org/f689d2faa8c9a5ce29216c00152c8c7b
[14] Interviews with several activists in Syria wishing to remain anonymous, August 2011to March 2012.

instances—such as in Daraa in March 2012—the entire electrical grid has been shut down for hours at a time. The government's deliberate use of such measures was evident from a leaked document issued by the General Head of the National Security Office in May 2011 explicitly ordering that "the internet is to be completely disconnected in Daraa, Homs, and the eastern provinces starting on Wednesday at 14:00."[15] It was widely believed that such steps aimed at preventing citizen journalists from charging communication devices or transmitting updates to the outside world.[16]

The Syrian government regulates and controls the internet via the state-owned Syrian Telecommunication Establishment (STE), which owns all telecommunications infrastructure.[17] The STE is a government body established in 1975 as a part of the Ministry of Telecommunications and Technology.[18] In addition to its regulatory role, the STE also serves as an ISP.[19]

LIMITS ON CONTENT

The Syrian government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs, and such censorship has expanded in recent years. Tests conducted by the OpenNet Initiative (ONI) in 2008-2009 found pervasive blocking of websites related to opposition to the Assad regime, human rights groups, the Muslim Brotherhood, and activism on behalf of the Kurdish minority.[20] A range of websites related to regional politics were also found to be blocked, including several Lebanese newspapers and the websites of groups campaigning to end Syrian influence in Lebanon, as well as the prominent London-based Arabic newspapers *Al-Quds al-Arabi* and *Al-Sharq al-Awesat*. Access to the entire Israeli domain name ".il" was also restricted.

Internet censorship continued to worsen in 2011 and early 2012. Activists and average users consistently complained about the extensive and unprecedented blocking of circumvention tools, internet security software, and applications that enable anonymous communications. Websites used to mobilize people for protests or resistance against the regime, including

[15] "Leaked Syrian document shows how Assad banned internet access and satellite phones," The Telegraph, June 27, 2011. http://blogs.telegraph.co.uk/news/michaelweiss/100093908/leaked-syrian-document-shows-how-assad-banned-internet-access-and-satellite-phones/.
[16] "Syria - a country that can no longer communicate," Bambuser (blog), March, 1, 2012, http://blog.bambuser.com/2012/03/syria-country-that-cannot-longer.html.
[17] "Syria," OpenNet Initiative, August 7, 2009, http://opennet.net/research/profiles/syria.
[18] See the Ministry of Telecommunications and Technology's website (in Arabic) at: http://www.moct.gov.sy/moct/?q=ar/node/58.
[19] See STE's website at: http://www.in-ste.gov.sy/inindex_en.html.
[20] "Syria," OpenNet Initiative; Guy Taylor, "After the Damascus Spring: Syrians search for freedom online," Reason, February 2007, http://www.reason.com/news/show/118380.html.

those of the network of Local Coordination Committees (LCCs) that emerged as the uprising progressed, were blocked.[21] Online initiatives to gather information and raise public awareness, such as the Mondaseh website, were blocked as well.[22] However, the websites of most international news sources and human rights groups have remained accessible.

Censorship is implemented by the STE with the use of various commercially available software programs. Independent reports in recent years pointed to the use of ThunderCache software, which is capable of "monitoring and controlling a user's dynamic web-based activities as well as conducting deep packet inspection."[23] In 2011, evidence emerged that the Syrian authorities were also using censorship and surveillance software manufactured by the U.S. firm Blue Coat Systems. Blue Coat had reportedly sold 14 devices to an intermediary in Dubai, thinking they were to be given to the Iraqi government, but logs obtained by the activist hacking group Telecomix in August revealed evidence of their use in Syria instead. In October, Blue Coat acknowledged that 13 of the above 14 devices had been redirected to the Syrian government, an inadvertent violation of a U.S. trade embargo, and that the company was cooperating with the relevant investigations.[24] Analysis of the exposed Blue Coat logs revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites.[25] The *Wall Street Journal* identified efforts to block or monitor tens of thousands of attempts to access opposition websites or online forums covering the uprising. Out of a sample of 2,500 attempts to visit Facebook, the logs revealed that three-fifths were blocked and two-fifths were permitted but recorded.[26]

The Syrian government also engages in filtering of mobile phone text messages. Beginning in February 2011, such censorship was periodically reported around dates of planned protests. In February 2012, the news service *Bloomberg* reported that a series of interviews and leaked documents revealed that a special government unit known as Branch 225 had ordered Syriatel and other mobile phone providers to block text messages containing key words like "revolution" or "demonstration." The providers reportedly implemented the directives with

[21] Email communication with activists in Syria, wishing to remain anonymous, December 2011. Local coordination committees of Syria: http://www.lccsyria.org/.
[22] Email communication with activists in Syria, wishing to remain anonymous, December 2011. The Mondaseh: http://the-syrian.com/.
[23] Syria," OpenNet Initiative; Reporters Without Borders, "Syria," *Internet Enemies 2010* (Paris: Reporters Without Borders, March 18, 2010), http://www.unhcr.org/refworld/publisher,RSF,,SYR,4c21f66e28,0.html; "ThunderCache Overview," Platinum, Inc., accessed August 14, 2012, http://www.platinum.sy/index.php?m=91.
[24] Blue Coat, "Update on Blue Coat Devices in Syria," news statement, December 15, 2011, http://www.bluecoat.com/company/news/statement-syria.
[25] "Blue Coat device logs indicated the levels of censorship in Syria," Hellias.github.com, accessed August 14, 2012, http://hellais.github.com/syria-censorship/.
[26] Jennifer Valentino-Devries, Paul Sonne, and Nour Malas, "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web," Wall Street Journal, October 29, 2011, http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html.

the help of technology purchased from two Irish firms several years earlier for the alleged purpose of restricting spam.[27]

In an unexpected turn of events, the Syrian government lifted a four-year block on the social-networking site Facebook in February 2011, resulting in a doubling of the number of users within three months.[28] The video-sharing website YouTube was also unblocked, though it was not usable from mobile phone devices.[29] By March 2012, both were within the top-five most visited websites in the country.[30] Some activists suspected, however, that rather than a sign of openness, the regime's motive for unblocking the sites was to be able to more easily track citizens' online activities and identities. Other social media platforms like Twitter are freely available but Syrian users have a minimal presence on them.

Despite the renewed access to Facebook and YouTube, a range of Web 2.0 applications remain inaccessible in Syria, including the blog-hosting platform Blogger and the VoIP service Skype. The Arabic blog-hosting service Maktoob has also been sporadically blocked, but was available as of May 2012. In February 2012, the government also began restricting access to certain applications for mobile phone devices that activists had been using to circumvent other blocks. Among the applications reportedly blocked were the live video-streaming service Bambuser[31] and WhatsApp, an application that allows users to send mobile phone text messages via the internet.[32] Instant messenger services such Ebuddy, Nimbuzz, and MiG-33 have been blocked as well. In other cases, certain online services—such as Google maps or the photo-sharing tool Picasa—have been rendered inaccessible from Syria by the U.S.-based service providers due to restrictions related to economic sanctions against the country.[33]

Decisions surrounding online censorship lack transparency and ISPs do not publicize details of how blocking is implemented or which websites are banned, though government officials have publicly admitted engaging in internet censorship. When a user seeks to access a

[27] Ben Elgin and Vernon Silver, "Syria Disrupts Text Messaging of Protesters With Made-in-Dublin Equipment," Bloomberg, February 14, 2012, http://www.bloomberg.com/news/2012-02-15/syria-blocks-texts-with-dublin-made-gear.html.
[28] Jennifer Preston, "Seeking to Disrupt Protesters, Syria Cracks Down on Social Media," New York Times, May 22, 2011, http://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html.
[29] Interview with activist in Syria wishing to remain anonymous, December 2011.
[30] "Top Sites in SY," Alexa.com, accessed August 14, 2012, http://www.alexa.com/topsites/countries/SY.
[31] "Bambuser now blocked in Syria," Bambuser (blog), February 17, 2012, http://blog.bambuser.com/2012/02/live-video-streaming-service-bambuser.html.
[32] Stuart Thomas, "Syrian government blocks access to WhatsApp," Memeburn.com, March 3, 2012, http://memeburn.com/2012/03/syrian-government-blocks-access-to-whatsapp/.
[33] On May 23, 2012, Google announced that it made Google Earth, Picasa and Chrome available for download in Syria. Yet, Google said that "As a U.S. company, we remain committed to full compliance with U.S. export controls and sanctions." Activists and internet users in Syria describe Google's step as insufficient, saying that there are tens of Google services still blocked in Syria including the entire Google Play App store on Android phones. See, "Software downloads in Syria," Official Google Blog, May 23, 2012, http://googleblog.blogspot.com/2012/05/software-downloads-in-syria.html?m=1.

blocked website, an error message appears implying a technical problem rather than deliberate government restriction. Decisions on which websites or keywords should be censored are made by parts of the security apparatus, including the abovementioned Branch 225, or by the executive branch.

In an environment of extreme violence and arbitrary "red lines," self-censorship is widespread. Sensitive topics include criticizing President Assad, his father, the military, or the ruling Baath party. Publicizing problems faced by religious and ethnic minorities or corruption allegations related to Rami Makhlouf, the president's cousin, are also off limits. Most Syrian users are careful not only to avoid such sensitive topics when writing online, but also to avoid visiting blocked websites.[34] Those who do choose to use circumvention tools typically do so at cybercafes rather than at their home or workplace out of a belief that surveillance and tracking of their browsing is easier for authorities at the latter.[35]

For news websites and other online forums based in the country, it is common to receive phone calls from government officials offering "directions" for how to cover particular events.[36] The Syrian government also pursues a policy of supporting and promoting websites that publish pro-government materials in an attempt to popularize the official version of events. These sites typically cite the reporting of the official news agency SANA, with the same exact wording often evident across multiple websites. Since early 2011, this approach has also been used to promote the government's perspective about the uprising and subsequent military campaign.[37]

Social media has played a crucial role in the Syrian uprising, though their primary utility has been information sharing rather than planning street protests. The "Syrian Revolution 2011" Facebook page, which by June 2012 had over 500,000 members from both inside and outside the country, has been a vital source of information for dissidents.[38] What has especially stood out in the Syrian context has been citizen journalists' creative and courageous use of mobile phone devices and video-sharing websites to document both demonstrations and human rights abuses—including regime security forces firing on unarmed civilians—and disseminate them to the outside world after most foreign correspondents were forced to leave the country.[39] For example, by March 2012, activists and citizen journalists had posted over 40,000 video clips to YouTube, many of which were

[34] Email communication from a Syrian blogger. Name was hidden.
[35] "Syria," OpenNet Initiative.
[36] Guy Taylor, "After the Damascus Spring: Syrians search for freedom online."
[37] Ibid.
[38] "The Syrian Revolution 2011 Facebook Statistics," Socialbakers.com, accessed August 14, 2012, http://www.socialbakers.com/facebook-pages/420796315726-the-syrian-revolution-2011.
[39] "Iranians were creative in using Twitter, Egyptians preferred Facebook, and Syrians are the masters of You Tube," Interview with Dr. Radwan Ziadeh, Director of the Damascus Center for Human Rights Studies, Washington, D.C., February 2012.

subsequently rebroadcast by leading news outlets like Al-Jazeera, the CNN, and the BBC, reaching tens of millions of viewers.[40]

Responding to the growing circulation of such footage and first-hand accounts, pro-regime forces have employed a range of tactics to manipulate online content and discredit the reports or those posting them, though a direct link between those carrying out these activities and the government is not always evident. Most notable has been the emergence of the Syrian Electronic Army (SEA) since April 2011, a pro-government activist and hacking group operating with at least tacit regime approval.[41] Among the tactics used by the SEA is to spam popular Facebook pages—like those of U.S. President Barack Obama or French President Nicolas Sarkozy—with highly orchestrated pro-Assad comments.[42] In other instances, misinformation is the tactic of choice. For example, in early 2012, a fake Twitter account was launched in the name of British-Syrian activist Danny Abdel Dayem, whose reports on a massacre in Homs had drawn international attention. The fake account's tweets combined plausible criticism of the Assad regime with comments seeming to incite sectarian hatred or ask for Israeli intervention; once discovered, Twitter closed the account.[43]

VIOLATIONS OF USER RIGHTS

Syria's constitution provides for freedom of opinion and expression, but these are severely restricted in practice, both online and offline. Laws such as the penal code, the 1963 State of Emergency Law, and the 2001 Press Law are used to control traditional media and arrest journalists or internet users based on vaguely worded violations such as threatening "national unity" or "publishing false news that may weaken national sentiment."[44] Defamation can carry criminal penalties if comments target the president (punishable by up to one year in prison) or other government officials, including judges, the military, or civil servants (punishable by up to six months in prison).[45] The judiciary lacks independence and its decisions are often arbitrary. Some civilians have been tried before military courts.

Since anti-government protests broke out in February 2011 the authorities have detained hundreds of internet users, including several well-known bloggers and citizen journalists. The reasons for someone's arrest are often unclear and among those targeted have been

[40] Robert Mackey, "Syria's Losing Battle to Control the News," The Lede (blog), *New York Times*, March 13, 2012, http://thelede.blogs.nytimes.com/2012/03/13/syrias-losing-battle-to-control-the-news/.
[41] Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," OpenNet Initiative, accessed August 14, 2012, http://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army.
[42] "Assad's Shadow Army," Al Jazeera, September 7, 2011, http://www.stream.aljazeera.com/story/assads-shadow-army.
[43] Robert Mackey, "Syria's Losing Battle to Control the News."
[44] Articles 285, 286, 287 of the Syrian Penal Code.
[45] Article 378 of the Syrian Penal Code.

individuals not known for their political activism. This arbitrariness has raised fears that users could be arrested at any time for even the simplest online activities—posting on a blog, tweeting, commenting on Facebook, sharing a photo, or uploading a video—if it is perceived to threaten the regime's control. For example, veteran blogger Ahmad Abu al-Khair was taken into custody in February 2011 while traveling from Damascus to Banias. [46] He was released one week later, but arrested again the following month on charges of "inciting demonstrations." He was held in custody for 24 days without being brought before a judge. Shortly after his release, he went into hiding. Security forces subsequently detained his brother twice—the second time for 60 days—in an effort to pressure al-Khair to turn himself in; as of May 2012, he remained in hiding.[47] In July, prominent tech blogger Anas Maarawi was detained and held for 59 days until his release after an online campaign on his behalf.[48] In February 2012, civil rights blogger Razan Ghazzawi and Mazen Darwich, the head of the Syrian Center for Media and Freedom of Expression, along with 12 others were arrested in a raid on the organization.[49] Gazzawi and six other female detainees were released after several days though they continue to face charges.[50] Darwich was still under incommunicado detention as of May 2012.[51]

Very few detainees have been brought before a judge. However, in a high-profile decision in February 2011, the Damascus State Security Court convicted 19-year-old student and blogger Tal al-Mallouhi to five years in prison for allegedly "divulging information to a foreign state," a charge she denied and for which no evidence was presented; al-Mallhouhi was not known to be politically active, but had posted poetry and commentary on political and social issues to her blog.[52]

Once in custody, citizen journalists, bloggers, and other detainees reportedly suffered severe torture. Though the precise number is unknown, it is estimated that dozens of individuals have been tortured to death after being caught filming protests or abuses and

[46] Anas Qtiesh, "Syrian Blogger Ahmad Abu al-Khair Arrested This Morning," Global Voices Online, February 20, 2011, http://advocacy.globalvoicesonline.org/2011/02/20/syrian-blogger-ahmad-abu-al-khair-arrested-this-morning/.
[47] Email communication with activist in Syria who wished to remain anonymous, April 2012.
[48] "Syria: Bloggers Rally for Anas Maarawi," Censorship in America, July 10, 2011, http://censorshipinamerica.com/2011/07/10/syria-bloggers-rally-for-anas-maarawi/; "Anas Maarawi is Free! Thank you all for your support!" Freeanas.pen.io, accessed August 14, 2012, http://freeanas.pen.io/.
[49] "Syria arrests iconic blogger Razan Ghazzawi and leading activists," The Telegraph, February 16, 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9086741/Syria-arrests-iconic-blogger-Razan-Ghazzawi-and-leading-activists.html.
[50] Email communication from Razan Gazzawi. See also: Syrian Blogger Razan Gazzawi denies the charges against him and confirm that his activity is 'guaranteed by the Syrian Constitution" [in Arabic], Asharq Al-Awsat, accessed June 15, 2012, http://www.aawsat.com/details.asp?section=4&article=654226&issueno=12069.
[51] "Syrian activist Razan Ghazzawi is freed by authorities for a second time," Al Arabiya News, February 20, 2012, http://english.alarabiya.net/articles/2012/02/20/195939.html.
[52] "Syria: Tal Al-Mallouhi," PEN, accessed August 14, 2012, http://www.pen.org/viewmedia.php/prmMID/5499/prmID/174.

then uploading them to YouTube.[53] In one high-profile case from November 2011, freelance journalist and photographer Ferzat Jarban from Homs was arrested and killed by security forces after filming a demonstration in al-Qasir; his body was mutilated and his eyes gouged out.[54] In some cases, the Syrian army appeared to deliberately target online activists and photographers in Homs, using the signal from their satellite phones to track their location. During the bombardment of Bab Amr in Homs in February 2012, government forces fired on a team of photographers who were live-streaming the assault using a satellite internet connection. Rami al-Sayed, who had run the live stream and previously uploaded over 800 videos to YouTube, was injured during the shelling and died several hours later.[55] In response to such brutality, hundreds of activists have gone into hiding and dozens have fled the country, fearing that arrest may not only mean prison, but also death under torture.[56]

Anonymous communication is possible but increasingly restricted. Registration is required upon purchasing a cell phone, though over the past year, activists have begun using the SIM cards of friends killed in clashes with security forces in order to shield their identities. Meanwhile, activists and bloggers released from custody reported being systematically asked or forced by security agents to provide the passwords for their Facebook, Gmail, Skype, and other online accounts.[57]

A new "Law for the Regulation of Network Communication against Cyber Crime" was passed in February 2012 and requires websites to clearly publish the names and details of the owners and administrators.[58] The owner of a website or online platform is also required "to save a copy of their content and traffic data to allow verification of the identity of persons who contribute content on the network" for a period of time to be determined by the government.[59] Failure to comply may cause the website to be blocked, and is punishable by a fine of between 100,000 and 500,000 SYP (US$1,700 to US$8,600). If the violation is found to have been deliberate, the website owner or administrator may face punishment of three months to two years imprisonment and a fine of 200,000 to 1 million SYP (US$3,400

[53] Interview via Skype with A.A, Human Rights Lawyer in Damascus, December 12, 2011. Name is hidden.
[54] "Ferzat Jarban," Committee to Protect Journalists, November 19 or 20, 2011, http://cpj.org/killed/2011/ferzat-jarban.php.
[55] Ahmed Al Omran, "Rami Al-Sayed, Syrian Citizen Journalist, Is Killed During Attack On Homs," The Two-Way (blog), NPR, February 21, 2012, http://www.npr.org/blogs/thetwo-way/2012/02/21/147224200/rami-al-sayed-syrian-citizen-journalist-is-killed-in-attack-on-homs.
[56] Interviews with two photographers who have taken refuge in Turkey, December 2011.
[57] Interviews with released bloggers, names were hidden.
[58] "Law of the rulers to communicate on the network and the fight against cyber crime" [in Arabic], Articles 5-12, accessed March 8, 2012, http://www.sana.sy/ara/2/2012/02/10/pr-399498.htm (site discontinued). Informal English translation: https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html.
[59] "Law of communicating on the network and fighting against cyber crime" [in Arabic], Article 2, accessed March 8, 2012, http://www.sana.sy/ara/2/2012/02/10/pr-399498.htm.

to US$17,000).[60] As of May 2012, however, the authorities were not vigorously enforcing these regulations.

Surveillance is widespread in Syria, as the government capitalizes on the centralized internet connection to intercept user communications. In early November 2011, *Bloomberg* reported that the Syrian government had contracted Area SpA, an Italian surveillance company, in 2009 to equip them with an upgraded system that would enable interception, scanning, and cataloging of all email, internet, and mobile phone communication flowing in and out of the country. According to the report, throughout 2011, employees of Area SpA had visited Syria and begun setting up the system that, when complete, would include flat-screen workstations displaying user communications in near real-time alongside graphics mapping users' contacts.[61] The exposé sparked protests in Italy and, at the end of November, Area SpA announced that it would not be completing the project.[62] As of May 2012, it remained unclear what the project's status was or whether any of the equipment was operational.

In a potential indication that the Syrian authorities were seeking an alternative to the incomplete Italian-made surveillance system, in March 2012 reports emerged of sophisticated phishing and malware attacks targeting online activists and their account information. Though it was impossible to trace the attacks back to the Syrian government, it was widely believed that the regime or those linked to it were behind them. The U.S.-based Electronic Frontier Foundation (EFF) reported that malware called Darkcomet RAT and Xtreme RAT had been found on activists' computers and were capable of capturing webcam activity, logging keystrokes, stealing passwords and more. Both sent the data back to the same IP address in Syria and were circulated via email and instant message programs.[63] A few weeks later, EFF reported the appearance of a fake YouTube channel carrying Syrian opposition videos that requested users' login information and urged them to download an update to Adobe Flash, which was in fact a malware program that enabled the stealing of data from their computer. Upon its discovery, the fake site was taken down.[64]

[60] "Law of communicating on the network and fighting against cyber crime" [in Arabic], Article 8, accessed March 8, 2012, http://www.sana.sy/ara/2/2012/02/10/pr-399498.htm. English translation: https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html.

[61] Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," Bloomberg, November 3, 2011, http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html.

[62] Vernon Silver, "Italian Firm Said To Exit Syrian Monitoring Project," Bloomberg, November 28, 2011, http://www.bloomberg.com/news/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says.html.

[63] Eva Galperin and Morgan Marquis-Boire, "How to Find and Protect Yourself Against the Pro-Syrian-Government Malware on Your Computer," Electronic Frontier Foundation, March 5, 2012, https://www.eff.org/deeplinks/2012/03/how-find-syrian-government-malware-your-computer-and-remove-it.

[64] Eva Galperin and Morgan Marquis-Boire, "Fake YouTube Site Targets Syrian Activists With Malware," Electronic Frontier Foundation, March 15, 2012, https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware.

Though present previously, cyberattacks have become increasingly common in Syria since February 2011, with many carried out by the Syrian Electronic Army (SEA). Though the group's precise relationship to the regime is unclear, evidence exists of government links or at least tacit support. These include the SEA registering its domain[65] in May 2011 on servers maintained by the Assad-linked Syrian Computer Society,[66] a June 2011 speech in which the president explicitly praised the SEA and its members,[67] and positive coverage of the group's actions in state-run media.[68]

The SEA's key activities include hacking and defacing Syrian opposition websites and Facebook accounts, as well as targeting Western or other news websites perceived as hostile to the regime. However, some foreign websites from the academic, tourism, or online marketing sectors have also been targeted.[69] Among other means of communication, the SEA has itself used Facebook to share information, coordinate attacks, and publicize their results. It has opened several Facebook pages, where it repeatedly issued calls to hack the emails of activists and to provide the obtained information to the security apparatus; most pages used to post such calls have subsequently been closed by Facebook for violating its terms of use. In other instances, the SEA has endangered anti-government activists by making public their phone numbers and addresses.[70] In April 2012, the personal email and Facebook accounts of Burhan Ghalioun, then-President of the opposition Syrian National Council were hacked. Two weeks later, his personal email communications began being published in the pro-Syrian Lebanese newspaper *al-Akhbar* in an effort termed "Ghalioun leaks."[71]

Activist-hacker groups in Syria and elsewhere have responded by hacking and defacing government websites. In August and September 2011, Anonymous and RevoluSec hacked at least 12 Syrian government websites replacing their content with interactive maps and statements detailing violence by security forces against peaceful protesters.[72] In another

[65] The Syrian Electronic Army, http://syrian-es.com/.
[66] Haroon Siddique and Paul Owen, "Syria: Army retakes Damascus suburbs," Middle East Live (blog), *The Guardian*, January 30, 2012, http://www.guardian.co.uk/world/middle-east-live/2012/jan/30/syria-army-retakes-damascus-suburbs.
[67] "Speech of H.E. President Bashar al-Assad at Damascus University on the situation in Syria," official Syrian news agency (SANA), June 21, 2011, http://www.sana.sy/eng/337/2011/06/21/353686.htm.
[68] See positive coverage on state-run websites [in Arabic]: Thawra.alwedha.gov.sy, May 15, 2011, http://thawra.alwehda.gov.sy/_print_veiw.asp?FileName=182170880201105161220 43; Wehda.alwedha.gov.sy, May 17, 2011, http://wehda.alwehda.gov.sy/_archive.asp?FileName=18235523420110517121437.
[69] Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army."
[70] Zeina Karam, "Syrian Electronic Army: Cyber Warfare From Pro-Assad Hackers," Huffington Post, September 27, 2011, http://www.huffingtonpost.com/2011/09/27/syrian-electronic-army_n_983750.html.
[71] "Pipe Lex," Al-Akhbar, accessed June 14, 2012, http://al-akhbar.com/taxonomy/term/3858.
[72] Zeina Karam, "Syrian Electronic Army: Cyber Warfare From Pro-Assad Hackers"; Amir Ahmed, "Apparently hacked, Syrian government website condemns president," CNN, August 8, 2011, http://articles.cnn.com/2011-08-08/world/syria.ministry.site.hacked_1_bashar-al-assad-syrian-people-syrian-flag?_s=PM:WORLD.

reaction, in November 2011, three members of the SEA were added to the European Union's list of individuals subject to financial sanctions.[73]

[73] "Consolidated List of Financial Sanctions Targets in the UK," Department of Treasury of UK, July 24, 2012, http://www.hm-treasury.gov.uk/d/syria.htm.

THAILAND

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	12	11
Limits on Content (0-35)	23	21
Violations of User Rights (0-40)	26	29
Total (0-100)	**61**	**61**

* 0=most free, 100=least free

POPULATION: 70 million
INTERNET PENETRATION 2011: 24 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/I USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Although Thai citizens have been posting online commentary for well over a decade,[1] internet communications have taken on a particularly significant role since a military coup took place in September 2006. Topics of discussion restricted or censored in traditional print and broadcast media have been openly addressed via the internet, especially issues related to the monarchy. Moreover, both the red-shirted United Front for Democracy Against Dictatorship (UDD) and the yellow-shirted supporters of the People's Alliance for Democracy (PAD) have utilized digital media and online resources to mobilize constituents for popular protests.[2]

This has provoked greater efforts by the government to control the free flow of information over the internet and via social media tools, particularly of expression related to the monarchy, a sensitive topic in a society where the king is revered, but debates about the role and future of the institution have fueled political polarization. Since 2009, tens of thousands of webpages have been blocked and several people sentenced to long prison terms for disseminating information or views online or via mobile phone text messages. Those expecting that a new opposition-led government elected in July 2011 would loosen internet restrictions were disappointed. Instead, censorship has continued apace under the

[1] Phansasiri Kularb, "Communicating to the Mass on Cyberspace: Freedom of Expression and Content Regulation on the Internet," in *State and Media in Thailand During Political Transition*, ed. Chavarong Limpattanapanee and Arnaud Leveau (Bangkok: Institute de Recherche sur l'Asie du Sud-Est Contemporaine, 2007).
[2] The PAD is comprised of a grouping of royalists, business elites, and military leaders with support in the urban middle class, while the UDD generally draws its support from the north, northeast, and rural areas, among whose residents former Prime Minister Thaksin Shinawatra remains popular.

administration of Yingluck Shinawatra and in some respects, become more institutionalized. In a highly polarized political environment, the fact that any citizen can lodge a lèse-majesté complaint against any other has opened the door for the charges to become a tool used by various actors against political opponents or to curb civic advocacy. Disturbingly, vague wording and lax adherence to due process have led to several disproportionately harsh punishments given to ordinary users based on questionable evidence.

Ironically, these measures have further deepened the politicization of the monarchy in the eyes of many Thais, while the increased content restrictions and legal harassment have contributed to greater self-censorship in online discussions. Simultaneously, these developments have helped inspire a burgeoning movement of politically conscious internet users, who favor greater protections for freedom of expression and amendment of laws used to suppress internet freedom.

The first internet connection in Thailand was made in 1987 between the Asian Institute of Technology (AIT), the University of Melbourne, and the University of Tokyo. The following year, the Australian International Development Plan (IDP) assisted Prince of Songkhla University (PSU) to set up a dial-up email connection. By 1991, five universities had established internet connectivity, and by 1995, the technology was commercialized and made available to the general public.[3]

OBSTACLES TO ACCESS

According to the National Electronics and Computer Technology Center (NECTEC), the number of internet users in Thailand increased from 3.5 million in 2001 to 18.3 million in 2009, or 27 percent of the country's roughly 66 million people.[4] The International Telecommunications Union (ITU) estimated a similar penetration rate of about 24 percent in 2011.[5] Mobile telephony is more widespread, with over 75 million mobile phone subscribers in 2011, and a penetration rate of about 112 percent.[6]

[3] Sirin Palasri, Steven Huter and Zita Wenzel, *The History of the Internet in Thailand* (Eugene: University of Oregon, 1999), http://www.nsrc.org/case-studies/thailand/english/index.html.

[4] National Electronics and Computer Technology Center (NECTEC), "Internet User in Thailand," accessed July 3, 2010, http://internet.nectec.or.th/webstats/internetuser.iir?Sec=internetuser.

[5] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[6] National Broadcasting and Telecommunications Commission (NBTC), "Thailand ICT Info," October 19, 2011, http://www2.nbtc.go.th/TTID/ [in Thai]; See also International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

A growing proportion of Thais has access to a desktop or tablet computer, with an estimated 25 percent of households reportedly owning a computer in 2011. Meanwhile, smartphone use has notably increased in recent years. By late 2011, smartphone sales surpassed feature phones for the first time and an estimated four million people subscribed to third-generation (3G) services.[7] Declining prices for the devices were a key factor, falling to 3,000 baht (US$94) by early 2012.[8]

For these and other reasons, broadband usage has expanded since 2010, particularly in the greater Bangkok area. Most internet users have access to high-speed connections, with download speeds averaging 6 to 7 Mbps,[9] though users often complain that connections are slower than advertised.[10] The National Broadcasting and Telecommunications Commission (NBTC), Thailand's main regulatory body, reported that Thailand had over 3.6 million broadband subscribers as of October 2011, representing a 21 percent increase over the previous year.[11] These gains have been driven by dynamics that entice Thais to spend more time online, such as declining prices, increased demand for alternative sources of information, and growing usage of social-networking tools. When connecting at home, an ADSL broadband subscription costs US$20 per month,[12] which can be costly for rural residents or those working at the minimum daily wage of about US$7, but is relatively affordable for the urban, educated middle class.[13] High-speed internet is available and affordable in cybercafes, which are used mostly by young people to play online games.

The main factor contributing to low penetration rates is a long-standing lack of government effort to improve the fixed-line infrastructure and boost the development of information and communication technologies (ICTs). Although lessening the digital divide was a notable part of the Pheu Thai party's platform ahead of the July 2011 elections, since taking office, the government has had limited success implementing this upgrade. This was due in part to the extensive flooding that struck Thailand in October 2011, the worst in decades.

In recent years, the Thai telecommunications market has liberalized and diversified. Prior to 2006, the country only had one international internet gateway controlled by the

[7] Business Monitor International, "Thailand Telecommunications Report Q3 2012," June 12, 2012, http://www.marketresearch.com/Business-Monitor-International-v304/Thailand-Telecommunications-Q3-7027556/.
[8] Suchit Leesa-nguansuk, "Smartphones to rule the roost," Bangkok Post, May 15, 2012, http://www.bangkokpost.com/business/telecom/293824/smartphones-to-rule-roost.
[9] "Download Index," Net Index, accessed June 21, 2012 http://www.netindex.com/download/2,23/Thailand/.
[10] "Civic Sector Submitted a Complaint to TCI to Solve Problem on Telecommunications Services," Telecommunications Consumer Protection Institute (TCI), December 14, 2010, http://www.tci.or.th/newshot_detail.php?id=23#newshot [in Thai].
[11] NBTC, "Thailand ICT Info."
[12] "ADSL Internet Prices in Thailand-November 2010," Select IT, accessed February 16, 2011, http://www.select.co.th/2010/11/adsl-internet-prices-in-thailand/ (site discontinued).
[13] Petchanet, "Thailand Raises Minimum Wage," Thailand Business News, December 10, 2010, http://thailand-business-news.com/economics/27852-thailand-raises-minimum-wage.

government-run Communication Authority of Thailand (CAT).[14] Today, out of nine National Internet Exchanges (NIXs), CAT Telecom operates only two, including the country's largest.[15] As of mid-2012, there were over 100 ISPs with active licenses, though ten provided most of the connection services for individual consumers and households.[16] Among them, True Internet had the largest market share for high-speed internet services, with 36 percent in mid-2011,[17] surpassing the state-owned Telephone Organization of Thailand (TOT) (34.4 percent)[18] and the private 3BB (26.5 percent).[19] The three main mobile phone service providers are the Singaporean-owned Advanced Info Service (AIS), the Norwegian-controlled DTAC, and True Corporation's True Move. The first two operate under concessions from TOT and CAT, an allocation system that does not entirely enable free-market competition. Opening a cybercafe involves a relatively simple registration process and is regulated by the Film and Video Act.

Political and legal disputes have repeatedly delayed the licensing process for 3G mobile phone service and wireless broadband. By May 2012, however, the auction of the 3G spectrum appeared imminent. In April, the National Broadcast and Telecommunications Commission (NBTC), a new regulatory body, proposed a plan for auctioning the spectrum, which the industry greeted with approval.[20] While awaiting the completion of the licensing process, TOT and CAT reached partnership agreements to lease part of their spectrum to private providers so they could begin offering 3G services to customers, though the National Anti-Corruption Commission questioned the legality of the arrangement.[21] Observers predicted that with the auction expected to conclude by the end of 2012, the prevalence of mobile web use would increase dramatically in the coming years.[22]

Legislation creating a single regulatory body for both the broadcast and telecommunications sectors passed parliament in late 2010. After a long and dispute-filled selection process, the

[14] World Bank, "Telecommunications Sector," *Thailand Infrastructure Annual Report 2008*, World Bank, accessed May 1, 2012, http://siteresources.worldbank.org/INTTHAILAND/Resources/333200-1177475763598/3714275-1234408023295/5826366-1234408105311/chapter4-telecommunication-sector.pdf.
[15] Internet Information Research Network Technology Lab, "Thailand Internet Map," NECTEC, accessed July 4, 2012, http://internet.nectec.or.th/webstats/internetmap.current.iir?Sec=internetmap_current [in Thai].
[16] NBTC, "List of Licensed Telecommunications Businesses," accessed July 4, 2012, http://apps.nbtc.go.th/license/ [in Thai].
[17] True Internet is a subsidiary of the communications conglomerate True Corporation, which also controls Thailand's largest cable TV provider True Visions and its third-largest mobile phone operator True Move.
[18] Both CAT Telecom and TOT are supervised by the Ministry of Information and Communication Technology (MICT).
[19] NBTC, "Telecommunication Market Report Q2 2011," accessed July 4, 2012, http://nbtc.go.th/wps/portal/NTC/TDC/telecommunications_market [in Thai].
[20] Komsan Tortermvasana, "3G auction plan lauded," Bangkok Post, April 26, 2012, http://www.bangkokpost.com/business/telecom/290487/3g-auction-plan-lauded.
[21] Business Monitor International, "Thailand Telecommunications Report Q2 2012," March 20, 2012, http://www.marketresearch.com/Business-Monitor-International-v304/Thailand-Telecommunications-Q2-6869918/; Komsan Tortermvasana, "NACC: True-CAT deal breaches law," Bangkok Post, April 24, 2012, http://www.bangkokpost.com/business/telecom/290130/nacc-true-cat-deal-breaches-law.
[22] Leesa-nguansuk, "Smartphones to rule the roost."

Senate appointed the members of the new NBTC in September 2011. From among the 11 commissioners, five are from the military, reflecting the army's deep interests in the communications sector. The remaining members are three former bureaucrats, two civil society representatives, and one police officer.[23] Some observers have complained that the NBTC lacks commissioners with industry experience, that the regulatory structure is incapable of dealing with converging communications platforms, and that coordination across different parts of the commission is weak.[24] Despite these shortcomings, the NBTC's decisions and proposed plans regarding the telecommunications sector have largely been viewed as fair thus far and an improvement over its predecessor.[25]

LIMITS ON CONTENT

Although the Thai government has been blocking some internet content since 2003, restrictions have expanded in recent years in both scale and scope. This trend continued, and to an extent accelerated, under the new government elected in July 2011. In December, the ICT Minister attributed the intensified censorship to the growing popularity of social media tools, which allow users to share information more widely and rapidly than before.[26]

Most of the websites blocked by the Thai authorities prior to 2007 involved pornography, online gambling, or circumvention tools, although some politically oriented websites were also found to be inaccessible.[27] Since then, the number of blocked websites has grown exponentially, particularly those with content perceived as critical of the monarchy.[28] A 2010 academic study reported that between 2007 and 2010 there were 117 court orders

[23] Usanee Mongkolporn, "Strong military role in NBTC," The Nation, September 6, 2011, http://www.nationmultimedia.com/home/Strong-military-role-in-NBTC-30164583.html.
[24] Don Sambandaraksa, "Thai regulator lacks unity," Telecomasia.net (blog), October 7, 2011, http://www.telecomasia.net/blog/content/thai-regulator-lacks-unity.
[25] Komsan Tortermvasana, "NBTC approves spectrum, broadcasting master plans," Bangkok Post, March 22, 2012, http://www.bangkokpost.com/business/telecom/285448/nbtc-approves-spectrum-broadcasting-master-plan; Tortermvasana, "3G auction plan lauded."
[26] "MICT: More cyber offenders to be arrested soon," Prachatai, December 3, 2011, http://www.prachatai.com/english/node/2930.
[27] They included an anti-coup site (www.19sept.com) and sites related to the Patani region in the south, including the Patani Malay Human Rights Organization (www.pmhro.org). Several individual URLs selling texts critical of the monarchy were found to be blocked on the online bookseller Amazon.com. See, OpenNet Initiative, "Country Profile: Thailand," May 9, 2007, http://opennet.net/research/profiles/thailand.
[28] Freedom Against Censorship Thailand (FACT), "Thai Website Censorship Jumps by More Than 500% Since Coup!" news release, January 1, 2007, http://facthai.wordpress.com/2007/01/15/thai-website-censorship-jumps-by-more-than-500-since-coup/.

issued to block access to nearly 75,000 URLs.[29] On average, 690 URLs were blocked daily. The research also showed that the vast majority of the websites (57,330 URLs) were blocked due to lèse-majesté content, while a much smaller number were blocked for containing material involving pornography (16,740 URLs), abortion (357 URLs), gambling (246 URLs), or other matters.[30]

Online censorship intensified after April 7, 2010, when the government declared a state of emergency and created a mechanism allowing the authorities to suddenly block—without a court order—any website considered to be publishing politically sensitive or controversial information. A large number of websites focused on the opposition red-shirt movement were blocked. These included individual YouTube videos, Facebook groups, and Google groups. Also filtered were less clearly partisan online news outlets or human rights groups, such as Freedom Against Censorship Thailand (FACT), the online newspaper Prachatai, the Political Prisoners in Thailand blog, and Asia Sentinel.[31] International news websites and human rights groups remained accessible.

In December 2010, the state of emergency was repealed and in July 2011, a new, opposition-led and democratically elected government took office. However, hopes that the new government would loosen internet censorship were quickly dashed.[32] In August 2011, the deputy prime minister explicitly vowed to curb the activities of websites with lèse-majesté content.[33] This approach was strengthened after massive flooding struck the country in October 2011. The government was criticized for its inept handling of the situation, while the military's role was perceived as positive in the public eye. Observers believed this left the government in a weaker political position to challenge the military and its royalist supporters on an issue as sensitive as lèse-majesté content.[34]

As of May 2012, some of the websites blocked in 2010 were accessible, including FACT and the Political Prisoners in Thailand. Also unblocked were websites related to the red-shirt movement, a key constituency of the new ruling Pheu Thai party. However, many other

[29] Sawatree Suksri, Siriphon Kusonsinwut, and Orapin Yingyongpathana, *Situational Report on Control and Censorship of Online Media, Through the Use of Laws and the Imposition of Thai State Policies* (Bangkok: iLaw Project, 2010), http://www.boell-southeastasia.org/downloads/ilaw_report_EN.pdf [henceforth iLaw Project Report].
[30] Ibid.
[31] Pavin Chachavalpongpun, "Thailand's Massive Internet Censorship," Asia Sentinel, July 22, 2010, http://asiasentinel.com/index.php?option=com_content&task=view&id=2601&Itemid=164.
[32] Joshua Kurlantzick, "Is Thailand Regressing on Lese-Majeste?" Asia Unbound (blog), Council on Foreign Relations, September 12, 2011, http://blogs.cfr.org/asia/2011/09/12/is-thailand-regressing-on-lese-majeste/.
[33] "Chalerm warns lese majeste websites," Bangkok Post, August 26, 2011, http://www.bangkokpost.com/news/politics/253608/chalerm-to-curb-lese-majeste-websites.
[34] Joshua Kurlantzick, "U.S. Citizen Sent to Jail in Thailand for Insulting the King," Asia Unbound (blog), Council on Foreign Relations, December 12, 2011, http://blogs.cfr.org/asia/2011/12/12/6649/.

websites—including Prachatai and Asia Sentinel—remained partially or fully blocked.[35] Moreover, according to media reports citing government officials, thousands of webpages have been added to the blacklist under the new administration. In March 2012, a police spokeswoman announced that 5,000 webpages had been blocked between December and March for containing content critical of the royal family.[36] In December 2011, the ICT Minister told reporters that during the previous three-month period, the ministry had overseen the blocking of over 60,000 pages, stating that this demonstrated the government's loyalty to the king. It remained difficult to confirm these statistics due to a lack of publicly available information on the precise list of blocked sites. In addition, according to one source in the MICT, the minister may have inflated the scale of censorship for political gains by misrepresenting the method of counting.[37]

In addition to blocking, the Thai government engages in administrative and political pressure to limit the spread of certain information online, particularly via social media applications. This includes reaching out to international providers and requesting that they delete content. Google reported that between January and December 2011, the Thai government (under two prime ministers) sent six requests without a court order to remove a total of 374 clips from the YouTube video-sharing platform for allegedly insulting the monarchy. Google largely complied, restricting Thai users from accessing 80 percent of them.[38] In a similar vein, the MICT claimed in November that Facebook had responded to its complaints by eliminating over 10,000 URLs and 50 user accounts, though the social-networking site did not confirm this assertion.[39] In January 2012, when the microblogging service Twitter announced a new feature enabling country-specific censorship of tweets,[40] MICT officials welcomed the announcement, the first government to do so.[41] In an incident unrelated to

[35] Freedom House tests conducted in mid-2012 on access to *Prachatai* and *Asia Sentinel* indicated that the sites loaded more slowly than others and that some pages were inaccessible, with the user redirected to a message stating that it had been blocked by the MICT, though other pages were available.

[36] AFP, "Thailand blocks 5,000 'royal insult' web pages.

[37] For example, according to one source inside the MICT, the 60,000 figure actually included the number of "shares" that a post received as counted within the total number of pages blocked in addition to the original post or page. For example, if a hyperlink was "shared" ten times, this would count as eleven "blocks." Interview with mid-ranking MICT employee who requested to remain anonymous, December 2011.

[38] The above statistics take into account Google's two separate reports for January to June 2011, and July to December 2011. Interestingly, the two segments correspond closely to the timing of the change in government, reflecting the continuation of lèse-majesté censorship policies under the Shinawatra administration. "Government requests," Google Transparency Report – Thailand, accessed September 19, 2012, https://www.google.com/transparencyreport/governmentrequests/TH/?p=2011-06; Google Transparency Report – Thailand; "Removals," Google Transparency Report – Thailand, accessed September 19, 2012, https://www.google.com/transparencyreport/removals/government/TH/?p=2011-12.

[39] Bangkok Pundit, "Thailand: Is a lese majeste crackdown around the corner? UPDATE: ICT asks FB to block thousands of sites," Asian Correspondent, November 25, 2011, http://asiancorrespondent.com/70492/is-a-lese-majeste-crackdown-around-the-corner/; "MICT has requested Facebook to delete over 10,000 pages offensive to the monarchy," Prachatai, November 24, 2011, http://www.prachatai.com/english/node/2913.

[40] "Tweets still must flow," Twitter (blog), January 26, 2012, http://blog.twitter.com/2012/01/tweets-still-must-flow.html.

[41] Jon Russel, "Thailand is the world's first government to endorse Twitter's censorship feature," The Next Web, January 30, 2012, http://thenextweb.com/asia/2012/01/30/thailand-is-the-worlds-first-government-to-endorse-twitters-censorship-feature/.

lèse-majesté rules, the citizen journalist website Thaiflood—which hundreds of thousands of Thais were following for updates on high-water warnings and relief efforts—complained in October 2011 that the official relief agency it had been working alongside had tried to censor its updates by seeking the right to screen them before publication.[42]

Internet censorship in Thailand is carried out through judicial orders, extrajudicial blocking decisions by the executive branch, and preemptive action by ISPs and content hosts. Judicial orders are typically issued under the 2007 Computer Crime Act (CCA). The law was passed by a military-appointed legislature less than a year after the 2006 coup. It groups broad content-regulation issues with more straightforward criminal activities like hacking, email phishing, uploading personal content without consent, and posting obscene material. A range of civil society groups and scholars opposed the law on the grounds that it infringes on the right to privacy, the right to access information, and freedom of expression.[43] For example, provisions in Articles 14 and 15 allow the prosecution of any content providers or intermediaries—such as webmasters, administrators, and managers—accused of posting or allowing the dissemination of content considered harmful to national security or public order.[44] The executive authorities are left to decide what amounts to a violation under these vaguely defined terms, and criminal courts make the final judgments. In practice, several individuals have indeed been charged under section 15 of the CCA for content posted by other users on websites or bulletin boards they hosted.[45]

Under the emergency declaration in effect from April to December 2010, top security officials held the power to shut down any website unilaterally. Thousands of websites were reportedly blocked under this extrajudicial mechanism.[46] Although this procedure was abolished with the end of the state of emergency, the censorship system in Thailand continues to lack transparency and accountability.[47] Reports emerged in 2011 of two other government bodies tasked with monitoring and curbing the circulation of lèse-majesté

[42] "Thailand tries to censor site devoted to flood news," Committee to Protect Journalists, October 25, 2011, http://cpj.org/2011/10/thailand-tries-to-censor-site-devoted-to-flood-new.php.
[43] Sarinee Achavanuntakul, "Danger! Computer Crimes Act," Fringer Blog, July 18, 2007, http://www.fringer.org/?p=259 [in Thai].
[44] Sections 14(1), 14(3), and 14(5) and Article 15 of the 2007 Computer Crimes Act pertain to crimes that "involve import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to a third party or the public; that involve import to a computer system of any computer data related to an offense against the kingdom's security under the criminal code; that involve the dissemination or forwarding of computer data already known to be computer data [which are illegal]." The act states that "any service provider intentionally supporting or consenting to an offense…within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offense." For an unofficial translation of the Act in English, see http://www.prachatai.com/english/node/117.
[45] iLaw Project Report pg. 13.
[46] CJ Hinke, "Thailand Now Blocking 277,610 Websites," Global Voices Advocacy, November 8, 2010, http://advocacy.globalvoicesonline.org/2010/11/08/thailand-now-blocking-256110-websites/; iLaw Project Report pg. 17.
[47] For example, in seeking to collect details of blocked websites, iLaw researchers found government agency response inconsistent with several entities being unable or unwilling to provide the requested data on the number and content of censored sites.

content. The first entity belongs to the Technology Crime Suppression Division that operates under the Royal Thai Police.[48] Media reports describe an entity with several dozen computer technicians scouring thousands of websites, manually and with automated crawlers, for potential insults of the royal family.[49] The second is the Cyber-Security Operation Center (CSOC) inaugurated by the MICT in December 2011.[50] The CSOC is an upgrade of a previously existing entity called the Internet Security Operation Center (ISOC) that was created in 2010. Its precise mandate and activities remain unclear.[51] Once an offending site or post is identified, a court order for blocking is requested and almost always granted. Such court decisions are usually made quickly and with minimal deliberation. In addition, the judicial reasoning is typically vague, with little indication of what the problematic content was or why it was deemed to violate the law.

Because those providing hosting services are held responsible for comments posted by third parties, they have an interest in censoring their own sites. Self-censorship is encouraged through the work of volunteers who monitor suspicious websites and report their findings to the MICT. In October 2009, the ministry opened a call center to receive reports of offensive websites. These reporting hotlines remained in effect as of May 2012 and were joined by a Facebook group called the "Reporting Association of Thailand."[52] In 2010, the MICT and Ministry of Justice introduced a controversial "cyber scout" project that aims to train students as volunteer web monitors.[53] By mid-2011, several dozen such "cyber scouts" had been recruited and were patrolling online forums and social networks without clearly identifying themselves as working with the government.[54] According to one such scout, their task was to alert users who may have posted lèse-majesté content, urge them to change their views, and if they refused, report them to the authorities.[55]

[48] Also called Office of Prevention and Suppression of Information Technology Crimes and referred to as a 'war room' for stopping lèse-majesté content. See, Thomas Fuller, "A High-Tech War Against Slights to a Centuries-Old Monarchy," New York Times, October 2, 2011, http://www.nytimes.com/2011/10/03/world/asia/03iht-thailand03.html?pagewanted=all.

[49] Martin Petty and Natnicha Chuwiruch, "Thais test taboos as war on royal slurs heats up," Reuters, December 6, 2011, http://www.reuters.com/article/2011/12/07/us-thailand-monarchy-idUSTRE7B605920111207.

[50] "MICT: More cyber offenders to be arrested soon," Prachatai, December 3, 2011, http://www.prachatai.com/english/node/2930.

[51] "Centre starts monitoring lese majeste," Bangkok Post, December 24, 2011, http://www.bangkokpost.com/lite/topstories/272260/centre-starts-monitoring-lese-majeste.

[52] Reporting Association of Thailand's Facebook page, https://www.facebook.com/reportthailand. As of August 2012, the page had over 22,000 "likes."

[53] "Prime Minister Inaugurates 'Cyber Scout' Project; Support the MICT in building the Cyber Scout Program to Protect the Online World," Ministry of Information and Communication Technology (MICT), accessed December 13, 2010, http://www.mict.go.th/ewt_news.php?nid=3430&filename=index [in Thai]; Mong Palatino, "Cyber Scout: Thailand's Internet Police?" Global Voices, December 24, 2010, http://globalvoicesonline.org/2010/12/24/cyber-scout-thailand%E2%80%99s-internet-police/.

[54] Cyber Scout webpage: http://www.justice-cyberscout.org/General/home.aspx.

[55] Daniel Rook, "Thai 'cyber scouts' patrol web for royal insults," AFP, May 10, 2011, http://www.google.com/hostednews/afp/article/ALeqM5iMwhnHSt36x-Hm-Wm_Y3thBV_t9w?docId=CNG.66922326b86c84d2b0f3ebc395ad2035.1c1.

The creation of programs employing citizens informants, along with prosecutions initiated against internet users in recent years, has generated a chilling effect among some members of the online community. In November 2011, the ICT Minister warned users that "liking" lèse-majesté content on Facebook could be a violation of the CCA and suggested they delete their reactions to avoid prosecution for "indirectly distributing inappropriate content."[56] Many internet users thus engage in self-censorship when communicating online, even when the exchange is among friends within a closed network.

Despite this constraining environment, outside of comments perceived as critical of the monarchy, most other areas of discussion on political, social, and human rights issues are freely and passionately debated in Thailand. Thus, in the run-up to the July 2011 elections, there was a rather free atmosphere for public debate and for political parties to mobilize supporters, contributing to the opposition's victory in an election deemed free and fair. Even with regards to lèse-majesté, observers noted more open public discussion on the possibility of amending the relevant provisions since July 2011.

Political propagandizing and proactive state manipulation of online discussions happen occasionally but have not had a significant impact on online discourse. The military has special units tasked with creating media content to counter criticism of the monarchy, such as the navy's Network for Promoting and Protecting the Monarchy over the Internet.[57]

In terms of the financial sustainability of online news outlets, there appeared to be a fairer distribution of advertisements across the political spectrum under the new government. In addition, red-shirt supporters have created their own advertising market to sustain news websites that share their political perspective, even if other businesses shy away.

As internet usage expands, online communication tools and resources are growing in importance for Thai citizens, particularly youth. While many blogs and discussion sites are blocked, users can access them with readily available circumvention software, and content producers often republish information on alternate sites. These techniques have undermined the MICT's censorship efforts.

Meanwhile, social media applications have grown in popularity. Advanced web applications such as YouTube, Facebook, Twitter, and international blog-hosting services like Blogger are freely available in Thailand, though individual pages or videos may be blocked. According to one study, at the end of 2011, 85 percent of Thai internet users visited a social

[56] Hana Stewart-Smith, "Thai Facebook users warned over anti-monarchy 'Likes'," ZDNet, November 26, 2011, http://www.zdnet.com/blog/asia/thai-facebook-users-warned-over-anti-monarchy-likes/286.
[57] Website: http://www.navyfamilylovetheking.com/.

media website at least once a week.[58] Such sites have become important spaces for political expression, including messages that implicitly challenge the existing sociopolitical power structures and prevalence of elite politics. They have also become a key channel for citizen journalists to disseminate updates on breaking news. Social media played a particularly important role during the flooding crisis in late 2011.[59] For example, Twitter usage jumped by 20 percent to 600,000 accounts within the first two months of the flooding.[60] The microblogging application was widely used to share photos, provide updates on conditions in specific locations, and inform donors of what relief materials were needed where. Alongside YouTube and Facebook, it was among the top 20 most visited websites in Thailand as of mid-2012.[61] The number of Facebook users has also increased exponentially, growing from approximately 250,000 in January 2009 to over 14 million—approximately one in five Thais—by May 2012.[62]

Although the scale of mobilization was not as intense as in previous years, when the red-shirt and yellow-shirt movements used social media to organize offline actions like flash mobs and protests, these tools remained important to Thai politics. In advance of the July 2011 elections, the main candidates and political parties used Twitter and Facebook to communicate with supporters. Nonetheless, with under one-third of Thais having internet access, traditional media—especially television—remained the most important source of information for many voters, particularly in rural areas.[63]

As internet freedom has come under growing pressure, online activists have organized to push back. The Political Prisoners in Thailand blog provides information on lèse-majesté prosecutions.[64] The Thai Netizen Network (TNN) was founded in early 2009 to uphold users' right to access, free expression, and privacy via public statements and other advocacy initiatives.[65] In January 2012, a coalition of academics and civil society groups calling itself the Campaign Committee for the Amendment of Article 112 launched an initiative to collect signatures urging the government to change the lèse-majesté provision of the criminal code.[66] Under the constitution, lawmakers must consider citizen-initiated legislative changes if they receive at least 10,000 signatures. The campaign sparked public

[58] Simon Kemp, "Social Digital and Mobile in Thailand," we are social (blog), January 3, 2012, http://wearesocial.net/blog/2012/01/social-digital-mobile-thailand/.
[59] Thai Netizen Network, *Thailand Internet Freedom and Online Culture Report 2011* (Bangkok: Thai Netizen Network, 2011): 112-129, https://thainetizen.org/docs/netizen-report-2011/.
[60] http://www.nationmultimedia.com/technology/SOCIAL-NETWORKING-A-GROWING-PHENOMENON-30172722.html
[61] "Top Sites in Thailand," Alexa, accessed May 1, 2012, http://www.alexa.com/topsites/countries/TH.
[62] "Thailand Facebook Statistics," Social Bakers, accessed September 18, 2012, http://www.socialbakers.com/facebook-statistics/thailand#chart-intervals.
[63] Jon Russell, "How influential is social media in Thailand's election?" Asian Correspondent, June 10, 2011, http://asiancorrespondent.com/56997/how-influential-is-social-media-in-thailands-election/.
[64] The blog is located at http://thaipoliticalprisoners.wordpress.com.
[65] The Thai Netizen Network website is located at https://thainetizen.org.
[66] Campaign Committee for the Amendment of Article 112's website: http://www.ccaa112.org/.

discussions both online and offline about the role of the monarchy. At end of April 2012, the campaign was still gathering signatures, but planned to soon submit the petition to parliament. The proposed legislative revisions were prepared by legal scholars and included changes such as reducing punishments for violations and enabling only the king's private secretary to initiate charges.[67] Despite such efforts, most observers were skeptical about the chances of the changes being adopted given the political environment and government fears that supporting such an amendment might spark another military coup.

VIOLATIONS OF USER RIGHTS

Since January 2011, legal harassment to lèse-majesté provisions and the CCA have continued, and in some respects worsened. Notably, these provisions have not only been used by political opponents against each other, but have also led to the imprisonment of citizens with little or no political connections, often following questionable legal proceedings.

The 2007 constitution, which replaced an interim charter imposed by the military government after the 2006 coup, guarantees freedom of expression. However, other laws have been used to curtail free expression. These include the Internal Security Act of 2007 and the CCA. Legal experts have criticized the CCA for its vague language, reliance on the "intent" of the accused, and lack of specificity regarding how an intermediary should receive a take down notice or know within what time frame to implement it.[68] In addition, harsh defamation and lèse-majesté provisions in the penal code, particularly Article 112, assign penalties of up to 15 years in prison for criticism of the king, the royal family, or Buddhism.[69] These provisions have generally been applied to online expression in much the same way as for traditional media.

Since 2007, hundreds of people have been charged under Article 112 or the CCA for communications sent via ICTs, reflecting a dramatic increase compared to previous years. Statistics from the Office of the Judiciary indicate 478 lèse-majesté cases were filed in 2010 under Article 112.[70] Between July 2007 and July 2010, a reported 185 legal cases were initiated against internet users under the CCA. Of these, 31 involved lèse-majesté charges, 54 involved defamation, and six involved actions considered by the authorities to threaten

[67] "Article 112 amendment bill to House," Bangkok Post, May 29, 2012, http://www.bangkokpost.com/breakingnews/295588/article-112-amendment-draft-to-house.
[68] "Freedom of Expression (Still) Under Attack," Political Prisoners of Thailand (blog), June 12, 2012, https://politicalprisonersofthailand.wordpress.com/2012/06/12/freedom-of-expression-still-under-attack/.
[69] Karin Deutsch Karlekar, ed., "Thailand," in *Freedom of the Press 2010* (New York: Freedom House, 2010), http://www.freedomhouse.org/template.cfm?page=251&year=2010.
[70] "Freedom of Expression (Still) Under Attack," Political Prisoners of Thailand (blog).

national security. The remainder related to fraud, pornography, and other commonly recognized computer crimes.[71] As of May 2012, the government had published neither official figures on new prosecutions for 2011 or early 2012, nor updates on the number of convictions from earlier cases.

From incomplete records compiled by lawyers and free expression groups, it appears that most of the defendants in CCA and Article 112 cases have been ordinary Thais, rather than well-known activists or government opponents. For example, in February 2012, Abhinya Sawatvarakorn (nicknamed Kantoop), a 19-year-old university student, became the youngest person to appear before a judge on lèse-majesté charges for a comment she had posted to Facebook in 2009.[72] As of May 2012, her case was still pending.[73]

Throughout 2011 and early 2012, guilty verdicts were returned in several lèse-majesté cases. They drew international condemnation because of the disproportionately harsh punishments imposed and the judges' reliance on questionable evidence. In November 2011, 61-year-old Ampol Tangnopakul was sentenced to twenty years in prison for violating Article 14 of the CCA and Article 112 of the penal code when he allegedly sent a high-ranking government official four mobile phone text messages deemed to have insulted the monarchy.[74] Human rights groups criticized that the burden was placed on the defendant to prove he had not sent the messages, although the prosecutor failed to definitively prove that he had and Ampol claimed he did not even know how to send a text message. Exacerbating his situation, Ampol was suffering from cancer and not receiving adequate medical attention in custody. Relative to other lèse-majesté prosecutions, the case received attention from traditional media, who referred to Ampol as "Uncle SMS."[75]

Shortcomings in judicial knowledge and the extensive use of pretrial detention have also been pronounced in the prosecution of internet-related cases. Specifically, judges hearing the cases often display a limited understanding of the technical dimensions of digital communications, causing them to convict users even when the evidence of their supposed guilt is inconclusive. For example, in March 2011, website designer Thanthawut Thaweewarodomkul was sentenced to 13 years in prison despite discrepancies in the

[71] iLaw Project Report.
[72] Nirmil Ghosh, "Thai Divide Growing Over Lese Majeste Law," Jakarta Globe, January 25, 2012, http://www.thejakartaglobe.com/international/thai-divide-growing-over-lese-majeste-law/493508; Pavin Chachavalpongpun, "Kantoop and lese-majeste," New Mandala (blog), February 3, 2012, http://asiapacific.anu.edu.au/newmandala/2012/02/03/kantoop-and-lese-majeste/.
[73] "Case #236: Kanthoop," iLaw Freedom, accessed September 18, 2012, http://freedom.ilaw.or.th/case/236.
[74] "THAILAND: Twenty years in prison for four SMS messages," Asian Human Rights Commission, November 24, 2011, http://www.humanrights.asia/news/ahrc-news/AHRC-STM-180-2011.
[75] Ampol later died in prison from his illness on May 8, 2012. See, "An inconvenient death," The Economist, May 12, 2012, http://www.economist.com/node/21554585; "Case #21: Uncle SMS," iLaw Freedom, accessed September 18, 2012, http://freedom.ilaw.or.th/case/21.

electronic evidence tying him to the offending content.[76] In February 2012, Human Rights Watch also voiced concerns over the repeated denial of bail to lèse-majesté defendants, particularly those affiliated with the red-shirt movement, and referred to the phenomenon as politically motivated.[77] A typical example was the case of Joe Gordon (also known as Lerpong Wichaikhammat), a dual Thai-U.S. citizen.[78] Gordon was sentenced in December 2011 to two and a half years in prison for posting on his blog excerpts from the banned book *The King Never Smiles* while living in the United States.[79] He was denied bail eight times and kept in pretrial detention for 84 days until he pleaded guilty in an apparent effort to reduce his sentence and expedite his release.[80]

Some prosecutions have not only targeted those who posted critical comments, but also sought punishment for content hosts who failed to remove comments posted by other users quickly enough. In one high-profile case, police raided Prachatai's offices and arrested Chiranuch Premchaiporn, the outlet's director and discussion-board moderator, in March 2009. She was accused of supporting a comment critical of the royal family by allowing it to remain posted for 20 days. Chiranuch was released, then arrested again in September 2010 on a second charge of "defaming the royal family," and of violating Articles 14 and 15 of the CCA, and Article 112 of the penal code. She was released after posting a 200,000 baht (US$6,500) bail.[81] Multiple hearings were subsequently held, but as of May 1, 2012, no verdict had been reached. Given the potential liability a guilty verdict would impose on intermediaries—including social media applications and other content providers—the case has far-reaching implications for internet freedom and the IT sector in Thailand.[82]

Besides the state's use of the CCA and penal code provisions to suppress dissent, a June 2011 report by Thai civil society groups and legal experts pointed to a "growing trend of companies, interest groups, and individuals using these laws to stop legal reform campaigns, social movements, and trade unions."[83] For example, in April 2011, activist Preeyanan

[76] "Nor Por Chor USA web designer sentenced to 13 years in jail," Prachatai, March 16, 2011, http://www.prachatai.com/english/node/2366.
[77] "Thailand: Courts Denying Bail in Lese Majeste Cases," Human Rights Watch, February 23, 2012, http://www.hrw.org/news/2012/02/24/thailand-courts-denying-bail-lese-majeste-cases.
[78] Ibid.
[79] "U.S. citizen jailed for insulting Thai monarchy," Reuters, December 8, 2011, http://af.reuters.com/article/worldNews/idAFTRE7B709A20111208.
[80] Gordon subsequently applied for a royal pardon, which was granted, leading to his release in July 2012. See, Kocha Olarm and Jethro Mullen, "Thai-American jailed for insulting monarchy receives royal pardon," CNN, July 11, 2012, http://edition.cnn.com/2012/07/11/world/asia/thailand-american-pardon/index.html.
[81] "Prachatai Editor Released on Bail," Reporters Without Borders, September 24, 2010, http://en.rsf.org/thailand-news-website-editor-arrested-on-24-09-2010,38440.html.
[82] At the end of May 2012, a Thai court found Chiranuch guilty and handed down an eight-month suspended sentence and 20,000 Baht (US$630) fine. See, James Hookway, "Conviction in Thailand Worries Web Users," Wall Street Journal, May 30, 2012, http://online.wsj.com/article/SB10001424052702303674004577435373324265632.html.
[83] "Thailand: Cybercrime Acts vs. the Right to Freedom of Expression," Thai Netizen Network, June 2, 2011, https://thainetizen.org/docs/thailand-cybercrime-acts-vs-the-right-to-freedom-of-expression/.

Lorsermvattana of the Medical Error Network, was accused by a doctor of "forging computer data" under the CCA after she posted online figures of patient fatalities as part of a campaign to support victims of medical malpractice.[84] In May 2011, prosecutors launched a case against Songkram Chimcherd, a labor union activist at Thai Industrial Gases, on charges of defamation and importing "false computer data." The charges were based on a series of emails Songkram had sent to various organizations regarding a dispute with the company over unpaid worker compensation.[85]

New prosecutions were also documented after the Yingluck Shinawattra administration took office. For example, in September 2011, a computer programmer, Surapak Phuchaisaeng, was arrested in Bangkok for allegedly creating a Facebook page with messages deemed insulting to the monarchy; he was indicted in November 2011 and his requests for bail were rejected.[86] In December 2011, two people—a 45-year-old store owner and a 30-year-old graduate student and blogger—were detained, interrogated, and had their computer equipment confiscated by police after someone reported they might be collecting or disseminating information detrimental to the monarchy.[87]

The scale of ICT surveillance in Thailand is unclear, but recent directives and public announcements indicate the government is trying to increase its capacity to intercept private communications. The CCA requires ISPs and webmasters to retain data logs for up to 90 days and turn data over to investigators upon request. In December 2011, the cabinet approved a directive placing ten types of cases, including violations of the CCA, under the jurisdiction of the Department of Special Investigation (DSI).[88] Under the rules regulating DSI operations, this means that intercepting internet communications and collecting personal data in CCA cases will no longer require a court order. The regulations came into effect in May 2012 upon publication in the Royal Gazette.[89] There have also been initial reports of the government delegating substantial resources to create a system that allows law enforcement agencies to directly access user data held by ISPs rather than having to request it from telecom employees. In December 2011, the government announced the proposed procurement of 400 million Baht (US$13 million) for a "lawful interception" system, but provided few additional details.[90] In most instances, obtaining user information would still require a court order, though as with censorship decisions, Thai judges typically approve

[84] Ibid.
[85] Ibid.
[86] "Surapak Puchaisaeng," Political Prisoners in Thailand (blog), accessed September 18, 2012, http://thaipoliticalprisoners.wordpress.com/pendingcases/surapak-puchaisaeng/.
[87] "Recent crackdown on cyber dissidents," Prachatai, March 10, 2012, http://www.prachatai.com/english/node/3096.
[88] "Cabinet approves draft directive for setting guidelines of DSI cases," The Nation, December 19, 2011, http://www.nationmultimedia.com/breakingnews/Cabinet-approves-draft-directive-for-setting-guide-30172173.html.
[89] "DSI added special case for 9 offenses" [in Thai], VoiceTV, May 25, 2011, http://news.voicetv.co.th/thailand/40014.html.
[90] "Web censor system hits protest firewall," Bangkok Post, December 15, 2011, http://www.bangkokpost.com/news/local/270812/web-censor-system-hits-protest-firewall.

such requests without serious deliberation. In addition, the above-mentioned changes regarding the role of the DSI mean that no court order would be needed in some cases. In practice, police reportedly need up to three days to trace the source of offensive online comments.[91]

Concerns about surveillance have led some political activists to use caution when communicating online and to employ additional security and privacy tools. Customers at cybercafes must present identification cards, though smaller businesses do not always comply with this rule. Mobile phone users are required to register their real names and national ID with their carrier upon purchasing a SIM card, whether prepaid or for a long-term subscription. Although the rule is less strictly enforced for prepaid SIM cards, those who do not register are unable to receive certain services, including roaming or mobile phone reception in the southern provinces of Pattani, Yala, and Narathiwat.[92]

Besides legal repercussions, internet users who post controversial content can face societal harassment and at times, physical attacks. Abhinya Sawatvarakorn, the 19-year-old mentioned above, was refused a place at Silpakorn University because of the lèse-majesté charges against her for Facebook postings.[93] In February 2012, professor Worachet Pakeerut, one of several academics leading the petition campaign to amend lèse-majesté provisions, was assaulted by two unidentified men who then fled on motorbikes. The Asian Human Rights Commission advocacy group said the attack represented an "ominous escalation of the dangers" faced by those promoting critical discussion of Article 112.[94] In December 2011, police raided the office of an editor of Thai E-News, the second most popular alternative source of online news after Prachatai; the catalyst for the search was unclear and no one was detained as the editor was not present at the time.[95]

A network of users calling themselves the "Social Sanction" group has launched online campaigns to vilify individuals who express views deemed disrespectful of the monarchy, sometimes sparking official investigations of the targeted user.[96] Other internet users have launched their own countermeasures again groups like "Social Sanction," posting online the personal information of individuals they believe belong to such communities.[97]

[91] Personal conversation with a senior police officer specializing in ICT crimes, March 27, 2009.
[92] "Register SIM Card," Happy, accessed September 18, 2012, http://www.happy.co.th/index.php?option=com_content&view=article&id=159&Itemid=169&lang=en.
[93] Nirmal Ghosh, "Thai Divide Growing Over Lese Majeste Law," Jakarta Globe, January 25, 2012, http://www.thejakartaglobe.com/international/thai-divide-growing-over-lese-majeste-law/493508.
[94] "Thailand's struggle to face its future," Asia Sentinel, April 27, 2012, http://www.asiasentinel.com/index.php?option=com_content&task=view&id=4459&Itemid=189.
[95] Interview with online journalist who requested to remain anonymous, December 2011.
[96] iLaw Project Report pg 14.
[97] Thai Netizen network, *Thailand Internet Freedom and Online Culture Report 2011* (Bangkok: Thai Netizen Network 2012): 54-76.

There have been sporadic reports of hacking attacks on online news outlets. Prachatai repeatedly faced denial-of-service (DoS) attacks during periods of political turmoil in 2009 and 2010 before being blocked by the authorities. The attacks forced the outlet to change servers and set aside large sums to pay for extra bandwidth. A web administrator for the news outlet reported in February 2012 that the site continued to face attacks, but was able to stay online thanks to the bandwidth upgrade.

TUNISIA

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Partly Free**
Obstacles to Access (0-25)	21	14
Limits on Content (0-35)	28	12
Violations of User Rights (0-40)	32	20
Total (0-100)	**81**	**46**

* 0=most free, 100=least free

POPULATION: 11 million
INTERNET PENETRATION 2011: 39 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

The internet was first launched for public use in Tunisia in 1996, and the first broadband connections were made available by the end of 2003. Since the traditional media under the Ben Ali regime was censored and tightly controlled by the government, the internet was used as a comparatively open forum for airing political and social opinions and an alternative platform for public debates on serious political issues. As internet penetration continued to grow, however, the regime responded by creating an extensive online censorship and filtering system. In 2009 and especially in 2010, censorship expanded and became increasingly arbitrary. Even websites with no political or pornographic content were censored, and hundreds of blogs as well as several online applications such as the photo-sharing site Flickr and video-sharing site YouTube were blocked.

The Tunisian internet landscape changed dramatically in 2011 after the extraordinary series of events that began with the self-immolation of the unemployed fruit vendor Mohamed Bouazizi on December 17, 2010. Widespread protests against the autocratic rule of President Zine el-Abidine Ben Ali ensued, fueled in no small part by online citizen journalism on social media sites such as Twitter, YouTube, and Facebook, as well as various blogs. This in turn led the government to increase its efforts to dismantle networks of online activists, hack into their social networking and blogging accounts, conduct extensive online surveillance, and disable activists' online profiles and blogs. Remarkably, the repressive censorship apparatus largely dissipated with Ben Ali's fall on January 14, 2011.

Since the end of Ben Ali's 23-year rule, Tunisia has been in the midst of a democratic transition. The country held its first democratic election in October 2011, leading to the appointment of 217 members of the Constituent Assembly of Tunisia in charge of writing a new constitution. In the meantime, however, a number of laws from the Ben Ali era remain on the books that restrict freedom of expression online, including those under the Telecommunications Decree and the Internet Regulations that hold internet service providers (ISPs) liable for third-party content, require ISPs to proactively monitor internet activity, and ban encryption technologies, among other restrictive provisions. While these laws have not been enforced in the post-Ben Ali era, their continuing existence remains a threat to the country's precarious internet freedom. Concerns have also emerged over the return of censorship with the initiative to block online pornography launched in 2011, which was ultimately overturned by the courts. Finally, the conviction of two Tunisians in March 2012 for publishing online content perceived as offensive to Islam and public morality prompted serious concerns among free expression advocates.

OBSTACLES TO ACCESS

Internet usage in Tunisia has grown rapidly in recent years, even as access remained restrictive under the Ben Ali regime. According to the International Telecommunication Union (ITU), internet penetration in Tunisia stood at 39.1 percent in 2011, up from 13 percent in 2006.[1] Although the government has actively sought to improve the country's information and communication technologies (ICTs), access is still hindered by high prices and underdeveloped infrastructure.

The popularity of mobile phones is also on the rise, with over 12.3 million mobile phone subscriptions and a penetration rate of 117 percent in 2011.[2] Nonetheless, mobile internet connections are rarely used, since mobile phone companies purchase internet access from existing ISPs and the cost remains beyond the reach of many Tunisians.

State-controlled Tunisie Telecom and the country's third mobile phone company Orange Tunisie, which launched in May 2010, provides 3G internet service through a plug-in USB key that enables laptops to connect to the mobile network. The device costs 69 dinars

[1] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#. Official statistics by the Tunisian Internet Agency (ATI) indicate an internet penetration rate of nearly 40 percent and 547,598 broadband subscriptions in Tunisia as of March 2012. See: AIT, "Statistiques du mois de mars 2012 sur l'Internet en Tunusie," Agence Tunisienne d'Internet (ATI), http://www.ati.tn/fr/index.php?id=90&rub=27 (in French); "Indicators – Number of subscriptions to Internet," Ministry of Information and Communication Technologies, http://www.mincom.tn/index.php?id=305, accessed March 2012.

[2] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

(approximately US$43), while the service costs 30 dinars (US$18.50) per month. Tunicell launched a second 3G mobile service in August 2011, offering up to 42 Mbps.[3] In early 2012, the government issued a tender for a new 3G and landline license won by the telecom operator Tunisiana—a development that will likely increase competition in the broadband market, deploy the 3G network to rural regions of the country,[4] and create a more open internet ecosystem.

Under Tunisie Telecom, which manages a national backbone bandwidth capacity of 60 Gbps, every internet subscriber must buy a landline package before choosing an ISP. Internet subscription prices range from 10 dinars (approximately US$6) a month for a connection speed of 1 Mbps, to 50 dinars (US$31) for a connection speed of 20 Mbps. On top of this cost, the subscriber must also pay the ISP for the same speeds, ranging from 10 to 25 dinars (US$6-15). Although there are no legal limits on the data capacity that ISPs can supply, the bandwidth remains very low, and connectivity is highly dependent on physical proximity to the existing infrastructure.

Tunisia has one of the most developed telecommunications markets in the region, with 11 ISPs supported by a nationwide fiber-optic backbone network, over which the state-controlled Tunisie Telecom has a de facto monopoly.[5] Previously, there were five privately-owned ISPs—Planet Tunisie, 3S Globalnet, Hexabyte, Topnet and Tunet; however, Topnet was acquired by Tunisie Telecom in June 2010,[6] and the telecom operator Tunisiana took over Tunet in September 2011.[7] In addition, since the country's regime change in January 2011, 25 percent of the formerly-private Tunisiana has reverted to state ownership through the confiscation of shares held by Ben Ali's son-in-law, Sakher El Materi.[8] Tunisia's interim authorities also seized a 51 percent share of Orange Tunisie that was formerly held by another son-in-law of Ben Ali, Marwan Ben Mabrouk.[9]

The Ben Ali regime attempted to increase access to ICTs by investing in infrastructure to improve connectivity and by promoting competition among ISPs to lower prices. In 2004, the government set up an initiative to encourage widespread computer use by removing

3 "Tunisia – Telecoms, Mobile and Broadband. Executive Summary," BuddeComm, http://www.budde.com.au/Research/Tunisia-Telecoms-Mobile-and-Broadband.html, accessed June 12, 2012.

4 "Tunisiana wins 3G and fixed licence," Global Telecoms Business, March 29, 2012, http://www.globaltelecomsbusiness.com/Article/3003562/Tunisiana-wins-3G-and-fixed-licence.html.

5 Mohamed Guesmi, "Tunisie Telecom's Monology Over Internet Infrastructure Blamed for High Bandwidth Costs," Tunisia-live.net, June 19, 2012, http://www.tunisia-live.net/2012/06/19/tunisie-telecoms-monopoly-over-internet-infrastructure-blamed-for-high-bandwidth-costs/.

6 Imen, "Tunisia: 'Tunisia Telecom' Acquires 'Topnet,'" AllAfrica.com, June 15, 2010, http://allafrica.com/stories/201006170303.html.

7 "Tunisiana takes over Tunet," TMTFinance, September 15, 2011, http://tmtfinance.com/news/tunisiana-takes-over-tunet.

8 Ibid.

9 "Tunisia seized Ben Ali family Orange Tunisie stake," Reuters, March 31, 2011, http://in.reuters.com/article/2011/03/31/idINIndia-56028120110331?feedType=RSS&feedName=technologyNews.

customs fees and creating the Family PC concept, which promoted ownership of a personal computer for each family. Authorities set a price ceiling for computer hardware and arranged loans at low interest rates for families to purchase the necessary equipment. The program also provided an internet subscription with every computer sold. Unfortunately, the project did not achieve the intended results, and computer prices remained relatively high—about 700 dinars (US$432)—even with the government incentives. Still, the number of computers per 100 inhabitants rose from approximately 12 in 2009 to 15 as of December 2011, and more banks are granting Tunisians special loans to buy computers.[10]

Although many people are unable to connect at home, the previous government claimed that universities, research centers, laboratories, and high schools have a 100 percent connectivity rate and that 70 percent of primary schools are connected.[11] Most Tunisian users access the internet at their work or at privately-owned cybercafes known as "publinets," where one hour of connection may cost up to 1 dinar (US$0.62). Before 2011, wireless access in cafes and restaurants was not permitted by law, which allowed only licensed ISPs to offer access to the network (free or paid). After the revolution, free access without any identification or registration requirements has become very common in cafes and restaurants in urban cities, attracting youth who use wireless internet on their laptops to connect to social networks. Nevertheless, the law restricting wireless internet provision remains on the books as of early 2012, putting those businesses that provide wireless access at risk of violating the law if the regulator decides to apply it.

Today, Tunisian users enjoy access to various internet services and applications, including free blog-hosting websites. Under the Ben Ali regime, however, many social media applications such as Dailymotion, YouTube, Flickr, and Wat TV were systematically blocked by the government.[12] Software that allows voice calls over the internet were also prohibited, but web-based applications like Skype and Google Talk that provide Voice over IP (VoIP) and other such services were nevertheless accessible under Ben Ali. The social-networking site Facebook was temporarily blocked in 2008, and some groups, profiles, and video links within the application were inaccessible thereafter. Furthermore, the private internet connections of some journalists, activists, and political bloggers were often cut ostensibly due to "technical problems," or speeds were reduced to hamper their ability to view sites and post information. Certain accounts on the Twitter micro-blogging service were also

10 Mincom, "Indicateurs et données statistiques TIC—Accés et infrastructure TIC: Le nombre d'ordinateurs pour 100 habitants" [ICT Indicators and Statistical Data—ICT Access and Infrastructure: Number of Computers per 100 Inhabitants], http://www.mincom.tn/index.php?id=315, accessed March 12, 2012.
11 ATI, "Statistiques du mois de Mars 2010 sur l'Internet en Tunisie."
12 Sami Ben Gharbia, "Tunisia: Flickr, Video-Sharing Websites, Blog Aggregators and Critical Blogs Are Not Welcome," Global Voices Advocacy, April 28, 2010, http://advocacy.globalvoicesonline.org/2010/04/28/tunisia-flickr-video-sharing-websites-blogs-aggregators-and-critial-blogs-are-not-welcome/.

blocked.[13] When protests broke out in December 2010, online articles covering the events of the unrest in foreign media outlets, including *Al-Jazeera*, the *BBC* and *France24*, were heavily censored. After the revolution, applications that had been systematically forbidden were unblocked, and social-networking sites such as Facebook became immensely popular, with the number Tunisian accounts reaching nearly three million users as of May 2012.[14]

The Ministry of Communication Technologies is the main government body responsible for ICTs and became a major shareholder of the three telecom operators after the revolution and subsequent expropriation of the shares connected to the Ben Ali regime. Under Article 7 of the Telecommunications Decree (carried over from Ben Ali), ISPs must obtain a license from the Ministry of Communications in order to deliver internet services.[15]

The National Instance of Telecommunication (INT) is the regulator for all telecom and internet-related activities and has the responsibility of resolving technical issues and disputes between actors. The INT governance body and president are nominated by the ICT minister and come mainly from government ministries and agencies, which activists argue is unfair and has led to a lack of independence. Nevertheless, the INT has initiated some positive change in internet policy, namely through the introduction of a new more liberal domain name chart and by inviting independent arbitrators from technical and civil society to develop a new Alternative Domain Name Dispute Resolution Process.[16]

Internet policy is decided by the INT and executed by the Tunisian Internet Agency (ATI), a state agency governed by a board of trustees comprised of representatives from the main shareholder, Tunisie Telecom, and other government-owned banks. The ATI manages the internet exchange point (IXP) between national ISPs that buy connectivity from Tunisie Telecom; it also manages the Domain Name Server (DNS) of the national country code top level domain ".TN" and the allocation of internet protocol (IP) addresses. Formally an integral part of Ben Ali's power structure responsible for implementing the regime's internet censorship and filtering system, the current ATI under the leadership of Moez Chakchouk has taken steps to become a more transparent and accountable body, although some issues of censorship still remain (see "Limits on Content").[17]

13 Jillian York, "Tunisia and Bahrain Block Individual Twitter Pages," Global Voices Advocacy, January 4, 2010, http://advocacy.globalvoicesonline.org/2010/01/04/tunisia-and-bahrain-block-individual-twitter-pages/.
14 "Tunisia Facebook Statistics," Socialbakers, accessed March 12, 2012, http://www.socialbakers.com/facebook-statistics/tunisia.
15 "Tunisia: Background paper on Internet regulation," Article 19, legal analysis, March 2011, http://www.article19.org/data/files/medialibrary/3014/12-04-03-ANAL-ICT-tunisia.pdf.
16 "Appel a manifestation d'interet pour la selection d'arbitres pour la resolution des litiges relatifs aux noms de domaines," Instance Nationale des Telecommunications, Republique Tunisienne, May 24, 2012, http://www.intt.tn/fr/index.php?actu=392&typeactu=89 [in French].
17 Yasmine Ryan, "Transforming Tunisia's internet agency," AlJazeera, October 5, 2011, http://www.aljazeera.com/indepth/features/2011/10/201110512451675190 0.html.

LIMITS ON CONTENT

Under the Ben Ali regime, Tunisia had one of most repressive internet censorship apparatuses in the world that employed three main techniques as part of its internet control strategy: technical filtering, post-publication censorship, and proactive content manipulation. When the country rose up in mass protest following the self-immolation of the fruit stand vendor Mohamed Bouazizi on December 17, 2010, the government increased its online censorship efforts, blocking more than 100 Facebook pages related to protest events along with online articles covering the unrest in media outlets such as *Al-Jazeera* and the *BBC*.[18] While video and photo-sharing websites such as Flikr, YouTube, and Vimeo were already permanently blocked in the country, photos and videos on Facebook became inaccessible.

In the immediate aftermath of Ben Ali's fall on January 14, 2011, the interim government stopped censoring the internet, and all web content became freely available with a few exceptions. On January 21, the Ministry of Technology and Communications stated that there would be partial censorship on sites that "offended public decency, through violence or incitement to hatred."[19] In an apparent effort to promote openness, the Ministry's statement also provided an email address (contact@web-liberte.tn) to which citizens and civil society could send claims concerning issues of freedom of expression online.[20] Nevertheless, there was still a lack of transparency over the process by which censorship decisions would be made and which sites would be blocked.[21]

While the technical filtering strategy employed by the ATI was also officially abandoned after January 2011, concerns arose over the return of filtering in May 2011 when the Tunis Permanent Military Tribunal ordered the removal of five Facebook pages based on charges of defamation against the military and its leaders.[22] According to the Ministry of Defense, the Facebook pages of "Jalel Brick," "Youssef patriote," "Takriz," "Ouajih Badreddine," and "Tunisie Toujours" had published video clips and circulated comments and articles that aimed to destabilize the trust of citizens in the national army and spread disorder in the country.[23] Two

18 "Tunisia – Countries Under Surveillance," Reporters without Borders, March 11, 2011, http://en.rsf.org/tunisia-11-03-2011,39747.html.

19 Astrubal de Nawaat, "Censure, manipulation et violation de la deontologie… Nous y sommes encore!" [Censorship, manipulation, and breaches of ethics … Here we are again!], Nawaat.org, January 25, 2011, http://nawaat.org/portail/2011/01/25/censure-manipulation-et-violation-de-la-deontologie-nous-y-sommes-encore/.

20 Ibid.

21 Ibid.

22 "Tunisie – Le tribunal militaire ordonne la censure de quatre pages sur Facebook" [Tunisia – The military court ordered the censorship of four pages on Facebook], Business News, May 11, 2011, http://www.businessnews.com.tn/Tunisie---Le-tribunal-militaire-ordonne-la-censure-de-quatre-pages-surFacebook,520,24752,1.

23 Afed Abrougui, "Tunisia: Internet Censorship Makes a Comeback," Global Voices Online, May 17, 2011, http://globalvoicesonline.org/2011/05/17/tunisia-internet-censorship-makes-a-comeback/.

of the Facebook pages were ostensibly known to have promoted violence against security forces on several occasions.[24] In a departure from its non-transparent past, the ATI published a list of the pages affected and the reasons for being filtered.[25] Many in the Tunisian internet community were outraged by the censorship, fearing the return of "Ammar 404," the codename Tunisian bloggers gave to the ATI's censorship apparatus under Ben Ali.[26] Some netizens, however, defended the military's actions as a legitimate effort to condemn violence.[27]

During the Ben Ali regime, the protection of children and society against pornography was the first argument used by the government to justify the necessity of internet filtering and censorship, with the ATI employing SmartFilter software to limit access to specified content. This argument surfaced again on May 26, 2011 when the Tunis Court of First Instance ordered the ATI to block pornographic websites in response to a complaint from lawyers that the sites were a threat to minors and the country's Muslim values.[28] The ATI pledged to oppose the blocking order, but its appeal was rejected in August 2011, prompting the agency to take the case to the highest appeal court. In a positive step forward, the Court of Cassation overturned the Court of Appeal decision on February 22, 2012 on the grounds that the ATI lacked the technical capacity to implement the filtering system mandated by the blocking order.[29] However, the justification in support of the appeal was not based on rights to freedom of expression or the principles of open internet, thus leaving open the possibility of future censorship as technologies for filtering internet content continue to develop.

Furthermore, while the Tunisian government no longer employs systematic online censorship, many internet users have expressed concern over the continued existence of the former censorship apparatus and its risk of being reinstated. Moreover, two laws remain on the books that govern the liability of ISPs over ICT activities: Decree no. 97-501 of 14 March 1997 (the Telecommunications Decree) and the Regulations of 22 March 1997 (the Internet Regulations). For example, ISPs are held liable for third-party content under Article 1 of the Telecommunications Decree. Article 9 of the Internet Regulations further requires ISPs to actively monitor and take down objectionable online content, retain archives of

24 Facebook note by "Tunisia: Against the rumors post-revolution," posted May 11, 2011, https://www.facebook.com/notes/tunisie-contre-les-rumeurs-post-r%C3%A9volution/message-%C3%A0-ceux-qui-sont-contre-la-censure-des-pages-web-par-le-tribunal-militair/128665313878396.
25 List of filtered sites: http://filtrage.ati.tn/
26 Afed Abrougui, "Tunisia: Internet Censorship Makes a Comeback," Global Voices Online.
27 Tweet by "@AymenOuerghi," Twitter.com, May 11, 2011, http://twitter.com/aymenouerghi/status/68296881092038656.
28 "Tunis court upholds order requiring filtering of porn sites," Reporters without Borders, August 16, 2011, http://en.rsf.org/tunisia-court-to-take-crucial-decision-for-01-07-2011,40566.html.
29 "National Internet Governance Forum," Tunisian Internet Agency (ATI), accessed September 18, 2012, http://www.ati.tn/en/index.php?id=97.

content for up to one year, and turn over all archived content to the ATI "without delay" if an ISP closes down.[30]

Self-censorship among online users dissipated rapidly with the fall of Ben Ali and the opening up of the internet in Tunisia. Citizen journalism on blogs and Facebook pages have proliferated and become a powerful source of critical reporting on any single event. "Facebook Admin" and "Blogger" have even become full-time paid jobs, especially during the election period in October 2011 when political parties counted on online mobilization to build their support base. Nevertheless, as the country continues to transform politically, self-censorship may be occurring on sensitive topics such as religion or among those associated with the former regime and ruling party.

Since the December 2010 revolution, numerous online sources of information have been launched alongside new newspapers, radio stations, and television channels, all of which are enriching the information landscape and diversity of viewpoints in Tunisia. By May 2011, the Ministry of Interior had granted 51 licenses for new newspapers,[31] and the High Independent Instance for Audiovisual had approved 12 new radio stations and six new TV channels.[32]

The abundance of information online has led to some cases of information manipulation by partisan interests, although the practice is far from as pervasive as under the Ben Ali regime, which proactively worked to shape public opinion online. For example, there is strong suspicion that the ruling Islamist Ennadha party in Tunisia has employed a digital army of young activists and bloggers tasked with managing Facebook communities and propagating an "info war" to disseminate partisan content.[33] Nevertheless, the unprecedented openness of the Tunisian internet sphere in the post-Ben Ali era has greatly diluted the influence of such content, and there is at present a more positive trend of politicians using social media tools to engage the internet populace rather than manipulate.[34]

Following the tremendous success of social media in launching the revolution and ousting

30 "Tunisia: Background paper on Internet regulation," Article 19, legal analysis, March 2011.
31 Ahmed Sahraoui, "Le ministere de l"interieur deliver 51 recepisses pour de nouveaux journaux" [The Ministry of Interior issues receipts for 51 new newspapers], Tunisie Numerique, May 3, 2011, http://www.tunisienumerique.com/le-ministere-de-linterieur-delivre-51-recepisses-pour-les-journaux/29499.
32 "12 nouvelles radios et 5 chaines TV privees: est-ce la saturation?" [12 new radio stations and five private TV channels: is saturation?], Leaders.com, November 27, 211, http://www.leaders.com.tn/article/12-nouvelles-radios-et-5-chaines-tv-privees-est-ce-la-saturation?id=7042.
33 "Manipulation de masse sur Internet: la Tunisie comme laboratoire?" [Mass manipulation on the Internet: Tunisia as lab?], FHIMT.com, May 26, 2011, http://www.fhimt.com/2011/05/26/manipulation-de-masse-sur-internet-la-tunisie-comme-laboratoire/.
34 Ahmed Medien, "Tunisia: Politicians and Deputies Opt for Open Governance Through Social Media," Global Voices Online, February 6, 2012, http://globalvoicesonline.org/2012/02/06/tunisia-politicians-and-deputies-opt-for-open-governance-through-social-media/.

Ben Ali, individuals and organizations have continued to use online tools for initiatives relating to political and social issues. For example, the Internet Society in Tunisia (ISOC)[35] has partnered with other youth associations to launch a successful online crowd-sourcing platform, which allows citizens to participate in election monitoring using SMS and online tools to report incidents related to the elections process.[36] Another platform, Mejlis.tn (meaning "assembly"), was launched to post recorded videos of the Constituent Assembly sessions as well as information on law projects and members of the assembly work. Social media continued to mobilize activists and protests throughout the year, including the major protests on March 20, 2011 for Independence Day[37] and on April 9, 2011 for Martyrs Day.[38]

VIOLATIONS OF USER RIGHTS

Article 8 of the old Tunisian constitution under the Ben Ali regime guaranteed "freedom of opinion, expression, the press, publication, assembly and association… according to the terms defined by the law."[39] Nevertheless, such constitutional protections did little to prevent Ben Ali from limiting freedom of expression and censoring the internet. After the 2010 revolution, the old constitution was annulled and in October 2011, the Constituent Assembly of Tunisia was elected to develop a new constitution within 12 to 18 months. In December 2011, the assembly adopted a provisional constitution (known as the "Small Constitution")[40] to guide the country's executive, legislative, and judiciary bodies until a final constitution is written.[41] The process of drafting the new constitution began in February 2012. Many civil society activists and human rights advocates have called on the Constituent Assembly to enshrine freedom of information and the right to access the internet in the country's future constitution.[42]

While the internet opened up dramatically after Ben Ali's fall from power, the repressive laws that enabled the government's censorship apparatus still remain, leaving open the possibility that freedom of expression online could be restricted again. For example, Tunisian law still allows the government to censor internet content that is deemed obscene or

35 Website of the Internet Society in Tunisia (ISOC): www.isoc.org.tn.
36 Such as Nchoof (Tunisian Dialect): translated to English as "I see," at www.nchoof.org.
37 Tarek Amara, "Tunisian protesters reject calls for Islamic state," Reuters, March 20, 2012, http://uk.reuters.com/article/2012/03/20/uk-tunisia-protest-idUKBRE82J0LJ20120320.
38 Salah Almhamdi, "Tunisia: Martyr's Day Clashes :eave Many Wounded," Global Voices, April 10, 2012, http://globalvoicesonline.org/2012/04/10/tunisia-martyrs-day-clashes-leave-many-wounded/.
39 "The Constitution of Tunisia," http://confinder.richmond.edu/admin/docs/Tunisiaconstitution.pdf, accessed March 2012.
40 Samia Fitouri, "Constituent Assembly Discusses Provisional Legislation: Live Updates," Tunisia Live, December 8, 2011, http://www.tunisia-live.net/2011/12/08/constituent-assembly-discusses-provisional-legislation-live-updates/.
41 "Tunisian assembly adopts provisional constitution," AlJazeera, December 11, 2011, http://www.aljazeera.com/news/africa/2011/12/201112115101550490.html.
42 "Report on IFEX-TMG Strategy Workshop: Campaign for Free Expression (September 2011)," IFEX, October 18, 2011, http://www.ifex.org/tunisia/2011/10/18/workshop_report/fr/.

threatening to public order, or is defined as "incitement to hate, violence, terrorism, and all forms of discrimination and bigoted behavior that violate the integrity and dignity of the human person, or are prejudicial to children and adolescents." Furthermore, the Tunisian Press Code (Act No. 1975-32) states that charges of defamation can be punished by imprisonment from one to three years with a fine of 120 to 1,200 dinars (US$74 to $740).[43] Articles 245 to 249 of the penal code also punish slander with two to five years of prison.[44]

During the revolutionary events of December 2010 and early January 2011, several bloggers and online activists were arrested or disappeared for their online activities but were released after Ben Ali's fall. Despite vast improvements in internet freedom that followed, there have been several instances of prosecution against bloggers and online users. In early 2012, for example, blogger Riadh Sahli was charged with defamation for posting on his Facebook page a press release sent by demonstrators rallying against the nomination of a lawyer to the position of advisor to the governor. The lawyer, Mabrouk Korchide, also accused another Facebook user of defamation for commenting on Sahli's post.[45] These cases remain unresolved as of May 2012.

In a more disconcerting case, two Tunisians were given seven-year prison sentences on March 28, 2012 for publishing online content that was perceived as offensive to Islam and "liable to cause harm to public order or public morals," a crime that is punishable under the repressive penal code still in place from the Ben Ali era. One of the individuals, Ghazi Ben Mohamed Beji, was convicted for an essay he published on Scribd.com (a free social publishing website) in July 2011 that satirized the Prophet Muhammad's biography. The other individual, Jaber Ben Abdallah Majri, was accused of posting photos and satirical writings about Islam and the Prophet on his Facebook page. Beji was sentenced in absentia, while Majri has been in prison since his arrest on March 5, 2012.[46]

Laws that limit online anonymity also remain a concern in the post-Ben Ali era. In particular, Article 11 of the Telecommunications Decree prohibits ISPs from transmitting encrypted information without prior approval from the Minister of Communications. Furthermore, Article 8 of the Internet Regulations requires ISPs to submit a list of all subscribers to the ATI.[47] While there have been no reports of the various Telecommunications Decree and Internet Regulations laws being enforced by the interim government in 2011 and early

43 "Code de la Presse: Loi n. 1975-32," Juriste Tunisie, April 28, 1975, http://www.jurisitetunisie.com/tunisie/codes/cpresse/cpresse1045.html.
44 "Code Penal," Juriste Tunisie, 2009, http://www.jurisitetunisie.com/tunisie/codes/cp/cp1225.htm.
45 "Tunisia – 2012 Surveillance," Reporters without Borders, March 12, 2012, http://en.rsf.org/tunisia-tunisia-12-03-2012,42072.html.
46 "Tunisia: Seven Years in Jail for Mocking Islam," Human Rights Watch, April 6, 2012, http://www.hrw.org/news/2012/04/06/tunisia-seven-years-jail-mocking-islam.
47 Ibid.

2012, their continuing existence underscore the precarious nature of Tunisia's newfound and relatively open internet environment. In a positive step, the ATI has begun to actively support online privacy, officially launching a mirror of the TOR website (Tor.mirror.tn) that features popular circumvention and anonymizing software previously used by cyber-dissidents against the ATI's censorship apparatus.[48] Mobile phone subscribers are required to register their SIM cards.

In addition, there were no reports of extralegal government surveillance of online activity in the post-Ben Ali period. However, the deep-packet inspection technology employed by the former authorities to monitor the internet and intercept communications is still in place, sparking worries that the technology can be reinstated if desired. According to the current leader of the ATI, Maoz Chakchouk, the internet authority is trying "to understand the equipment… [and] we're waiting for the new government to decide what to do with it."[49]

Under the Ben Ali regime, online journalists and bloggers were commonly targeted with extralegal intimidation and physical violence. In 2011, no instances of targeted violence and beatings were reported, though some online journalists and bloggers present at recent demonstrations were reportedly harassed by the police for their protest activities.

Technical attacks were a popular tool used under the Ben Ali regime to intimidate and silence ICT users. During the December 2010-January 2011 protests, police hacked into numerous email and Facebook accounts of cyber-activists, stealing passwords to infiltrate the networks of citizen-journalists that were fueling the anti-government uproar. Since Ben Ali's fall, there have been no reported incidents of cyberattacks perpetrated by the government. However, in April 2012 the hacktivist group Anonymous leaked emails stolen from members of the ruling Ennahda party. The Anonymous attack was reportedly a response to the rise of the conservative Salafi Muslim faction in Tunisia and the Ennahda party's perceived lack of action against the Salafi's violent efforts to implement Sharia law in the country.[50]

48 Ibid.

[49] Vernon Silver, "Post-Revolt Tunisia Can Alter E-Mail With 'Big Brother' Software," Bloomberg.com, December 12, 2011, http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html.

50 Zach Walton, "Anonymous Leaks Tunisia Prime Minister's Emails," WebProNews, April 9, 2012, http://www.webpronews.com/anonymous-leaks-tunisia-prime-ministers-emails-2012-04.

TURKEY

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	12	12
Limits on Content (0-35)	16	17
Violations of User Rights (0-40)	17	17
Total (0-100)	**45**	**46**

* 0=most free, 100=least free

POPULATION: 75 million
INTERNET PENETRATION 2011: 42 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Internet and mobile telephone use in Turkey has grown significantly in recent years, though access remains a challenge in some parts of the country, particularly in the southeast. Until 2001, the government had a hands-off approach to internet regulation but has since taken considerable legal steps to limit access to certain information, including some political content. According to Engelliweb,[1] there were over 15,000 blocked websites as of February 2012, and certain online services, particularly file-sharing sites such as Last.fm and Metacafe, have experienced repeated blocking. Over the last two years, citizens have filed five separate applications to the European Court of Human Rights to challenge the government's blocking of YouTube,[2] Last.fm, and Google sites from Turkey after applicant appeals before the local courts were rejected.

In February 2011, the Information Technologies and Communication Board (BTK)[3] decided to establish a countrywide mandatory filtering system with the aim of protecting citizens from so-called "harmful content," which includes but is not limited to sexually explicit content and terrorist propaganda. Subsequent to strong opposition from the public and street demonstrations in May 2011,[4] a legal challenge against the BTK policy was launched at the Council of State level, leading the Turkish authorities to modify the policy in August

[1] Engelliweb.com is a website that documents information about blocked websites from Turkey.
[2] The YouTube block was lifted in November 2010 only after disputed videos were made unavailable from the country.
[3] Decision No. 2011/DK-10/91 of Bilgi Teknolojileri ve İletişim Kurumu, dated February 22, 2011.
[4] Yesim Comert, "Marchers protest new Turkish Web filtering rule," CNN, May 15, 2011, http://edition.cnn.com/2011/WORLD/meast/05/15/turkey.internet.protest/index.html.

2011. The modified filtering system is now voluntary for subscribers and became operational in November 2011.

OBSTACLES TO ACCESS

Despite an increasing penetration rate in the last few years, obstacles to internet access remain. According to the International Telecommunication Union (ITU), internet penetration in Turkey stood at 42.1 percent in 2011, up from 18.2 percent in 2006.[5] The number of mobile telephone subscriptions in 2011 was over 65 million for a penetration rate of 88.7 percent in 2011,[6] and all mobile phone operators offer third-generation (3G) data connections.

Although many people access the internet from workplaces, universities, and internet cafes, poor infrastructure and the lack of electricity in certain areas, especially in the eastern and southeastern regions, have had a detrimental effect on citizens' ability to connect, particularly from home. High though decreasing prices, bandwidth caps, and a lack of technical literacy, particularly among older Turks, also inhibit wider internet use. Bandwidth capping has become standard practice and a part of the broadband services offered by major providers throughout 2011.

The population generally enjoys widespread access to internet technology, and diverse news sources are available to users. Popular social networks such as Facebook and MySpace, and applications like Skype are available in Turkish. However, the government routinely blocks advanced web content and applications including video- and music-sharing sites such as YouTube, MySpace, Last.fm, Metacafe, and Dailymotion; blog-hosting sites like WordPress and Blogspot; Google groups; the photo-sharing website Slide; and file-sharing websites such as Rapidshare. In 2011, several websites addressing Turkey-related issues were subjected to blocking orders. This particularly affected news websites such as Özgür Gündem, Azadiya Welat, Keditör, Firat News, and Günlük Gazete that report news on southeastern Turkey and Kurdish issues. Google-owned Blogspot was also inaccessible for approximately three months as a result of a blocking order in 2011.

In most instances, these large-scale shutdowns have been blunt efforts to halt the circulation of specific content that is deemed undesirable or illegal by the government. Nevertheless,

[5] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[6] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

circumvention tools are widely used to access blocked websites, and the government has not restricted their use to date.

There are 150 internet service providers (ISPs) in Turkey, but the majority act as resellers for the dominant, partly state-owned Turk Telekom, which provides more than 95 percent of the broadband access in the country. Liberalization of local telephony is still pending, and the delay undermines competition in the fixed-line and broadband markets. ISPs are required by law to submit an application for an "activity certificate" from the Telecommunications Communication Presidency (TIB), a regulatory body, before they can offer services. Internet cafes are also subject to regulation and registration. Those operating without an activity certificate from a local authority representing the central administration may face fines of 3,000 to 15,000 lira (US$1,900 to $9,600). Mobile phone service providers are subject to licensing through the regulatory authority and a licensing fee.

The Computer Center of Middle East Technical University has been responsible for managing domain names since 1991. Unlike in many other countries, individuals in Turkey are not permitted to register and own ".com.tr" and ".org.tr" domain names unless they own a company or civil society organization with the same name as the requested domain. A new set of rules on Domain Names Registration through an official Government Regulation was published in the Official Gazette on November 7, 2010. The Information and Communication Technologies Authority oversees and establishes the policy and its bylaws.

The Information and Communication Technologies Authority and the TIB, which it oversees, act as the regulators for all of these technologies and are well staffed and self-financed.[7] However, the fact that board members are government appointees is a potential threat to the authority's independence, and its decision-making process is not transparent. Nonetheless, there have been no reported instances of activity certificates being denied. The TIB also oversees the application of the country's website blocking law and is often criticized by pressure groups for a lack of transparency.

LIMITS ON CONTENT

Government censorship of the internet is relatively common and has increased in recent years. In May 2007, the government enacted Law No. 5651 titled, "Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication," which delineates the responsibilities of content providers, hosting companies, mass-use providers, and ISPs.[8] The law's most important provision calls for the blocking of

[7] Information and Communication Technologies Authority, http://www.tk.gov.tr/Eng/english.htm.
[8] Law No 5651 was published on the Turkish Official Gazette on 23.05.2007, No. 26030.

websites that contain certain types of content, including material that shows or promotes sexual exploitation and abuse of children, obscenity, prostitution, or gambling. Also targeted for blocking are websites deemed to insult Mustafa Kemal Ataturk, the founding father of modern Turkey. Domestically-hosted websites with proscribed content can be taken down, while websites based abroad can be blocked and filtered through ISPs. According to Engelliweb.com,[9] there were over 15,000 blocked websites as of February 2012.

The procedures surrounding decisions to block websites, whether by the courts or the TIB, are nontransparent, creating significant challenges for those seeking to appeal. Judges can issue blocking orders during preliminary investigations as well as during trials. The reasoning behind court decisions is not provided in blocking notices, and the relevant rulings are not easily accessible. As a result, it is often difficult for site owners to determine why their site has been blocked and which court issued the order. The TIB's mandate includes executing judicial blocking orders, but it can also issue such orders under its own authority for certain content. Moreover, it has in some cases successfully asked content and hosting providers to remove offending items from their servers, allowing it to avoid issuing a blocking order that would affect an entire website. According to TIB statistics as of May 2009, the courts are responsible for 21 percent of blocked websites, while 79 percent are blocked administratively by the TIB. The regulator has refused to publish blocking statistics since May 2009.[10] In December 2011, an administrative court in Ankara rejected an appeal to obtain the official blocking statistics under Turkey's freedom of information law. A subsequent appeal to the Council of State, the highest administrative court in Turkey, was lodged in January 2012 to obtain the statistics.

Although Law No. 5651 was designed to protect children from illegal and harmful internet content, its broad application to date has effectively restricted adults' access to some legal content. In various instances, the courts have blocked websites for political content using other laws. For example, the courts have indefinitely blocked access to the websites of several alternative news sources such as Atilim, Özgür Gündem, Keditör, Günlük Gazetesi, and Firat News Agency. Access to the website of Richard Dawkins, a British etiologist, evolutionary biologist and popular science writer, was blocked in September 2008 after a pro-creationist Islamist claimed that the website contents had insulted him, his work, and his religion, though in July 2011, an Istanbul Court lifted the blocking ban and rejected the defamation claims. As of mid-2012, the case is on appeal at the Court of Appeal, but the website is accessible from Turkey.[11]

[9] Engelliweb.com is a website that documents information about blocked websites from Turkey.
[10] Reporters Without Borders, "Telecom Authority Accused of Concealing Blocked Website Figures," news release, May 19, 2010, http://en.rsf.org/turkey-telecom-authority-accused-of-19-05-2010,37511.html.
[11] "RD.net no longer banned in Turkey!" The Richard Dawkins Foundation, July 8, 2011,

On September 28, 2010, the Ankara 3rd Criminal Court of Peace ordered the blocking of BugunKilicdaroglu.com, a website that assesses the policies and strategies of the CHP (Republican People's Party, the main Turkish opposition party) leader, Mr. Kemal Kılıçdaroğlu. The injunction to block access to the website was requested by Mr. Kılıçdaroğlu's lawyers. The Ankara 11th Criminal Court of First Instance overturned the blocking decision in January 2011.[12]

Certain leftist and pro-Kurdish news websites are blocked consistently,[13] especially those dealing with southeastern Turkey, home to most of the country's Kurdish population. In 2011, two different Court injunctions were issued to block access to LiveStream for allegedly distributing content involving terrorist propaganda. In addition, a Turkish blogger currently residing in Sweden is being prosecuted for the crime of publishing "obscene" content on the 5Posta.org website. The author writes about sexual politics and freedom, as well about sexuality, the sex industry, pornography, and internet censorship among other topics. Access to the 5Posta.org website is blocked by two different decisions, and court cases are pending. Similarly, an appeal is ongoing at the Council of State level with regards to the blocked Playboy.com website in Turkey. The user-based appeal was lodged by two university professors and is currently ongoing as of mid-2012.

Blocking orders related to intellectual property infringement continued in 2011 with access being blocked to the Google-owned Blogspot for nearly three months beginning in January 2011.[14] In the case of Blogspot, five different appeals were lodged with three different criminal courts in Diyarbakir on behalf of a Turkish blogger in early March 2011. On March 14, the Diyarbakir Public Prosecutor's Office revoked the blocking decision.[15]

In April 2011, the TIB sent a letter to hosting companies based in Turkey with a list of 138 potentially provocative words that may not be used in domain names and websites.[16] This raised strong national and international criticism, to which the TIB responded that the list of

http://richarddawkins.net/articles/642074-rd-net-no-longer-banned-in-turkey.

[12] Yaman Akdeniz, "Fighting Political Internet Censorship in Turkey: One Site Won back, 10,000 To Go," Index on Censorship, March 4, 2011, http://www.indexoncensorship.org/2011/03/fighting-political-internet-censorship-in-turkey-one-site-won-back-10000-to-go/.

[13] Yaman Akdeniz, *Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship*, January 2012, http://www.osce.org/fom/41091.

[14] "Blogspot banned in football row," BBC News, March 4, 2011, http://www.bbc.com/news/technology-12639279.

[15] Yaman Akdeniz, "Turkish Blogspot Blocking Order Has Been Revoked," CyberLaw Blog, March 14, 2011, http://cyberlaw.org.uk/2011/03/14/turkish-blogspot-blocking-order-has-been-revoked/.

[16] Several "controversial words" appeared on the list of "banned words" including: *Adrianne* (no one knows who she is), *Haydar* (no one knows who he is), *aayvan* (animal), *baldiz* (sister-in-law), b*uyutucu* (enlarger), c*iplak* (nude), c*itir* (crispy), e*tek* (skirt), free, girl, *ateşli* (passionate), *frikik* (freekick), gay, *gizli* (confidential), *gogus* (breast), *hikaye* (story), homemade, hot, *İtiraf* (confession), *liseli* (high school student), *nefes* (breath), partner, *sarisin* (blond), *sicak* (hot), *sisman* (overweight), *yasak* (forbidden), y*erli* (local), *yetiskin* (adult), etc.

words was intended to help hosting companies identify and remove allegedly illegal web content.[17]

According to Thomas Hammarberg, the Commissioner for Human Rights of the Council of Europe, it is essential that the Turkish authorities review Law No. 5651 to align the grounds for restriction with those accepted in the case law of the European Court of Human Rights.[18] Similarly, the European Commission stated in its "Turkey 2011 Progress Report" that frequent website bans are cause for serious concern and called for the revision of Law No. 5651, which limits freedom of expression and restricts citizens' right to access to information.[19]

Five separate applications have been made between April 2010 and January 2011 to the European Court of Human Rights regarding the blocking of YouTube,[20] Last.fm, and Google sites from Turkey after the applicants' appeals before the local courts were rejected. In February 2011, the Strasbourg Court published the statement of facts for the appeals applications involving Google and Last.fm and asked the government of Turkey to respond to a number of questions by June 2011.[21] The government responded in July 2011, and the written submissions by the parties, which are confidential, were completed in September 2011. A decision is expected by the end of 2012.

In a step towards increasing control over the internet in Turkey, the Information Technologies and Communication Board (BTK) announced in February 2011 a decision to implement a mandatory countrywide filtering system that claims to protect families, particularly children, from harmful online content such as pornography.[22] In response, the IPS Communication Foundation, which owns the alternative media website Bianet, initiated in April 2011 a legal challenge against the BTK decision at the Council of State, the highest administrative court in Turkey.[23] The pressure of legal action against the proposal eventually

[17] Ekin Karaca, "138 Words Banned from the Internet," Bianet, April 29, 2011, http://www.bianet.org/english/freedom-of-expression/129626-138-words-banned-from-the-internet; See also, Erisa Dautaj Senerdem, "TIB's 'forbidden words list' inconsistent with law, say Turkish web providers," Hurriet Daily News, April 29, 2011, http://www.hurriyetdailynews.com/n.php?n=tibs-forbidden-words-list-inconsistent-with-law-2011-04-29.

[18] Thomas Hammarberg, "Freedom of Expression and Media Freedom in Turkey," Council of Europe, July 12, 2011, https://wcd.coe.int/ViewDoc.jsp?id=1814085.

[19] European Commission, "Turkey 2011 Progress Report," Commission Staff Working Paper, October 2011, http://ec.europa.eu/enlargement/pdf/key_documents/2011/package/tr_rapport_2011_en.pdf.

[20] The YouTube block was lifted in November 2010 only after disputed videos were removed or made unavailable from the country.

[21] Application No. 3111/10 by Ahmet YILDIRIM against Turkey (Google Sites) introduced January 12, 2010 and Application No. 20877/10 by Yaman Akdeniz against Turkey (Last.fm) introduced April 6, 2010. Assessment of these two cases is currently ongoing as of early 2012.

[22] Decision No. 2011/DK-10/91 of Bilgi Teknolojileri ve İletişim Kurumu, dated February 22, 2011.

[23] On September 27, 2011, the Council of State rejected the "stay of execution" request by Bianet referring to the annulment of the February 22, 2011. The case between Bianet and BTK is currently on-going as of early 2012.

led the BTK to modify the policy in August 2011, annulling the original decision and making the adoption of the filtering system optional instead of compulsory.

Before the decision was annulled, the BTK's original "safe use of the internet" filtering system required ISPs to offer four separate user profiles—standard, children, family, and domestic internet—with different access authorizations and obligated all home subscribers to choose one of the four filtering profiles upon purchase. ISPs would then be given filtering lists for each profile from the BTK that included domain names, IP addresses, port numbers, and web proxy addresses. Further, the BTK would have had broad discretionary powers to include on the black list any website that it believed to be harmful. No criteria or rules were established for deciding what sort of content could be subject to filtering, and ISPs would have been compelled to provide the service free of charge to their customers.

The modified filtering system is not compulsory for users, and the new version includes only the family and child profiles. However, ISPs are still compelled to offer the filtering service to their customers, and the filtering criteria have been considered somewhat arbitrary yet discriminatory and eclectic.[24] For example, the "child fliter" blocks access to several websites advocating the theory of evolution as well as the website of Richard Dawkins,[25] while some anti-evolution websites remain accessible through the same filter.[26] The "child filter" also blocks access to Facebook and the online video-sharing website YouTube, in addition to *Yasam Radyo* (Radio Life) and the Armenian minorities' newspaper, *AGOS*.[27] The BTK claims "technical errors" before removing websites from its filter, and a lack of transparency behind the filtering process has been the subject of criticism.

The filtering database and profiles are controlled and maintained by the government. The Child and Family Profiles Criteria Working Committee was introduced in January 2012—almost three months after the new filtering system become operational—to address concerns about the establishment of filtering criteria. However, the formation of the committee itself raised concerns about its independence and impartiality. Seven of the 11 members of the committee are either from the BTK, Family and Social Policies Ministry, or Internet Board, and three experts are selected and appointed by the BTK. Moreover, the principles on which the committee will work remains unclear.

[24] "New Internet Filtering System Condemned as Backdoor Censorship," Reporters Without Borders, December 2, 2011, http://en.rsf.org/turquie-new-internet-filtering-system-02-12-2011,41498.html.
[25] Dorian Jones, "Turkey Blocks Web Pages Touting Darwin's Evolution Theory," Voice of America, December 23, 2011, http://www.voanews.com/english/news/europe/Turkey-Blocks-Web-Pages-Touting-Darwins-Evolution-Theory-136162663.html.
[26] Sara Reardon, "Controversial Turkish Internet Censorship Program Targets Evolution Sites," Science Magazine, December 9, 2011, http://news.sciencemag.org/scienceinsider/2011/12/controversial-turkish-internet-c.html?ref=hp.
[27] "Agos'u Biz Değil Sistem Engelledi" [AGOS was filtered through the Ministry of Education filter. See Haber Merkezi], Bianet, January 23, 2012, http://www.bianet.org/bianet/ifade-ozgurlugu/135645-agosu-biz-degil-sistem-engelledi.

On November 4, 2011, a second legal challenge was launched by Alternatif Bilişim Derneği (the Alternative Information Technologies Association), which asked the Council of State to annul the modified August 2011 BTK filtering policy on the grounds that the policy lacks legal basis. The Association further argues that the BTK system discourages diversity by imposing a single type of family and moral values.

Despite the large number of sites blocked, circumvention techniques and technologies are widely available, enabling even inexperienced users to avoid filters and blocking mechanisms. Each time a new order is issued and a popular website is blocked, a large number of articles are published to instruct users on how to access the banned websites. As a demonstration of the extent of this phenomenon, during the two and a half year block of YouTube, the video-sharing website remained the eighth most-accessed site in Turkey.[28]

Turkish users increasingly rely on internet-based publications as a primary source of news, and despite the country's restrictive legal environment, the Turkish blogosphere is surprisingly vibrant and diverse. There is a wide range of blogs and websites through which citizens question and criticize Turkish politics and leaders, including issues that are generally viewed as politically sensitive. The majority of civil society groups maintain an online presence, and social-networking sites such as Facebook, FriendFeed, and especially the microblogging platform Twitter are used for a variety of functions, including political campaigns.

In May 2011, internet users organized a major protest against the introduction of the country-wide filtering system. The protest gathered approximately 50,000 people in Istanbul who demanded freedom from filters as well as the abolishment of Law No. 5651.[29] Arguably, the protest and its associated media coverage had a huge impact on the modification of the mandatory filtering system. Thus far, however, mobile phones and SMS technology do not seem to play a large role in social or political mobilization.

VIOLATIONS OF USER RIGHTS

The constitution includes broad protections for freedom of expression, stating that "everyone has the right to express and disseminate his thought and opinion by speech, in writing or in pictures or through other media, individually or collectively." Turkish law and court judgments are also subject to the European Convention on Human Rights and bound by the decisions of the European Court of Human Rights. While thousands of websites have

[28] According to Alexa, a web information company, as of August 26, 2010, http://www.alexa.com/topsites/countries/TR.
[29] "Turks marched against government censorship of the Internet in Istanbul," CyberLaw Blog, July 19, 2010, http://cyberlaw.org.uk/2010/07/19/17-temmuz-2010-internette-sansuru-protesto-etmek-icin-2000-kisi-yuruduk.

been blocked under Law No. 5651, there have been no prosecutions of individuals for publication of the proscribed content. There are also no laws that specifically criminalize online expression or activities like posting or downloading information, sending email, or transmitting text messages.

However, many provisions of the criminal code and other laws, such as the Anti-Terrorism Law, are applicable to both online and offline activity. In October 2011, the Anti-Terrorism law was used to prosecute journalist Recep Okuyucu for allegedly advocating terrorist propaganda by downloading Kurdish music files and accessing the blocked Kurdish *Firat News Agency* website.[30] He was found not guilty by a Diyarbakir court.

Article 301 of the Criminal Code has been used against journalists who assert that genocide was committed against the Armenians in 1915, discuss the division of Cyprus, or write critically about the security forces. Book publishers, translators, and intellectuals have also faced prosecution for insulting Turkish identity. Thus far, there have been no prosecutions under Article 301 for online material, but the possibility of such charges significantly contributes to self-censorship.

Nevertheless, a number of citizens have been penalized for their online activities. In February 2012, a student named Mikail Boz was subjected to a disciplinary investigation for criticizing the dean of the communications studies department at Marmara University on the popular Turkish social media platform, Sour Times. He was punished with a one-semester suspension, which was reduced to one week after his case was widely covered by the media.[31] In March 2012, Erol Ceylan, a public servant, shared a song on Facebook that prompted the publication of a number of anti-government comments on his profile. Subsequent to an administrative disciplinary investigation, he lost his job.[32]

The constitution states that "secrecy of communication is fundamental," and users are allowed to post anonymously online. The constitution also specifies that only the judiciary can authorize interference with the freedom of communication and the right to privacy. For example, judicial permission is required for technical surveillance under the Penal Procedural Law. However, the anonymous purchase of mobile phones is not allowed, and would-be buyers need to provide official identification. Turkey has yet to adopt a data

[30] "Court Acquits Journalist Who Interviewed Kurdish Separatist," Reporters Without Borders, December 29, 2011, http://en.rsf.org/turkey-journalists-under-pressure-as-26-10-2011,41282.html.

[31] Isil Cinmen, "Ekşi Sözlük'e Yazdı, Okuldan Uzaklaştırıldı," Bianet, February 1, 2012, http://bianet.org/bianet/genclik/135862-eksi-sozluke-yazdi-okuldan-uzaklastirildi#.Tyk6VzET46o.facebook [in Turkish]; See also, Isil Cinmen, "Üniversiteden Geri Adım, Mikail Haftaya Okulda," Bianet, February 3, 2012, http://bianet.org/bianet/genclik/135939-universiteden-geri-adim-mikail-haftaya-okulda [in Turkish].

[32] Erol Ceylan took legal action at an administrative court to annul the decision. See, "Facebook bir hayat daha karartti!" CNN Turk, March 2, 2012, http://www.cnnturk.com/2012/guncel/02/03/facebook.bir.hayat.daha.karartti/647658.0/index.html [in Turkish].

protection law even though the September 2010 amendments to the Turkish Constitution included data protection provisions. In 2011, the use of encryption (hardware or software) became subjected to regulations introduced by the Information Technologies and Communication Board. Suppliers of encryption products are now required to provide private keys before they can offer their products or services within Turkey.

Despite the constitutional guarantees, most forms of telecommunication have been tapped and intercepted in practice.[33] Between 2008 and 2009, several surveillance scandals received widespread media attention, and it is suspected that all communications are subject to interception by various law enforcement and security agencies, including the Gendarmerie (military police). Some reports indicate that up to 50,000 phones—both mobile and land-line—are legally tapped daily in Turkey, and 150,000 to 200,000 interception requests are made each year. During 2009, it was alleged that phone conversations involving members of the parliament, journalists, Supreme Court and other judges, and prosecutors including the chief public prosecutor were tapped.[34]

Such actions have been challenged in court on at least one occasion. In 2008, responding to complaints lodged by the TIB, the Supreme Court of Appeals overruled a lower court's decision to grant both the Gendarmerie and the National Intelligence Agency (MIT) the authority to view countrywide data traffic retained by service providers.[35] Nonetheless, similar powers to access and monitor data traffic have been granted to the MIT and the National Police Department. Faced with criticism on the issue, the parliament in 2008 launched a major inquiry into illegal surveillance and interception of communications, though the inquiry concluded in January 2009 without finding any "legal deficiencies" in the interception regime.

ISPs are not required to monitor the information that goes through their networks, nor do they have a general obligation to seek out illegal activity. However, all access providers, including internet cafe operators, are required to retain all communications (traffic) data for one year. Administrative fines of 10,000 to 50,000 lira (US$6,400 to US$32,200) can be imposed on access providers if they fail to comply, but no ISP or other provider has been prosecuted to date.

[33] For a history of interception of communications, see: Faruk Bildirici, *Gizli Kulaklar Ulkesi* [The Country of Hidden Ears] (Istanbul: Iletisim, 1999); Enis Coskun, *Kuresel Gozalti: Elektronik Gizli Dinleme ve Goruntuleme* [Global Custody: Electronic Interception of Communications and Surveillance] (Ankara: Umit Yayincilik, 2000).

[34] "Başsavcı Engin dinlenmiş ve takip edilmiş" [The Chief Public Prosecutor's Calls Are Tapped], *Radikal*, November 12, 2009.

[35] The court stated that "no institution can be granted such authority across the entire country, viewing all people living in the Republic of Turkey as suspects, regardless of what the purpose of such access might be." See, "Supreme Court of Appeals Overrules Gendarmerie Call Detail Access," Today's Zaman, June 6, 2008, http://www.todayszaman.com/tz-web/news-144038-supreme-court-of-appeals-overrules-gendarmerie-call-detail-access.html.

All mass-use providers are required to use one of the filtering programs approved by the TIB, which are published on the TIB's website. However, criteria for the approval of these programs are not publicly available, and it remains unclear whether the approved programs filter websites other than the ones formally blocked by the courts and the TIB. As a result, the system could lead to systematic censorship of websites without the necessary judicial or TIB orders.

There were no reports of extralegal intimidation or harassment of bloggers or others for their online activities in 2011 and early 2012, though some internet content was believed to have contributed to the 2007 murder of Hrant Dink, the editor-in-chief of the bilingual Turkish-Armenian newspaper *Agos*. He had received several death threats via email, and it was reported that his teenage killer was influenced by the writings on certain ultra-nationalist websites and online forums. Such sites are not covered by Law No. 5651 and have not been subject to blocking or regulation.

Unlike physical attacks, technical attacks are becoming increasingly common. During 2011 and in early 2012, the international internet hacktivist collective known as Anonymous launched a successful distributed denial-of-service (DDoS) attack against the Turkish government, taking down several official government websites, including the Telecommunications Communication Presidency (TIB) website (www.tib.gov.tr) and Turkish Social Security Institution (SGK, www.sgk.gov.tr). Furthermore, Anonymous hacked a consumer complaints website run by the BTK in February 2012, and data relating to a considerable number of users was circulated through numerous websites.[36]

[36] "Anonymous Hacked BTK Database," Bianet, February 15, 2012, http://www.bianet.org/english/world/136178-anonymous-hacked-btk-database.

UGANDA

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Partly Free**
Obstacles to Access (0-25)	n/a	11
Limits on Content (0-35)	n/a	8
Violations of User Rights (0-40)	n/a	15
Total (0-100)	**n/a**	**34**

* 0=most free, 100=least free

POPULATION: 36 million
INTERNET PENETRATION 2011: 13 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

Internet penetration in Uganda has grown steadily following the deregulation and liberalization of the information and communication technology (ICT) sector in 1997, which ushered in reductions in mobile telephone tariffs and bandwidth prices, as well as greater availability of fiber optics bandwidth, increased ICT literacy, and supportive government-led ICT policies. As a result of these initiatives, the number of internet users has increased dramatically. However, in a country with a population of 34.5 million,[1] internet penetration and accessibility for the majority of Ugandans is still low, hampered primarily by high costs and poor infrastructure. Nearly 30 million people, the majority of whom live in rural areas, do not have access to the internet. Furthermore, for most internet users, the cost of access remains high and the quality of service inconsistent.

Perhaps the most dramatic development in telecommunications in the last decade has been the growth of mobile phone subscribers from less than one million in 2001 to more than 14 million in 2011.[2] Uganda is ranked among the ten African countries with the highest number of mobile phone subscribers,[3] and a small but growing number of Ugandans own a smart

[1] Raymond Baguma, "Uganda's population now at 34.5 million," New Vision, October 30, 2011, http://www.newvision.co.ug/news/18769-Uganda-s-population-now-at-34-5-million.html.
[2] Paul Tentena, "Uganda: Mobile phone subscribers hit 14 million," East African Business Week, June 20, 2011, http://www.busiweek.com/11/news/uganda/1207-mobile-phone-subscribers-hit-14-million-in-uganda.
[3] Mark Page, Laurent Viviez, and Maria Molina, "African Mobile Observatory 2011: Driving Economic and Social Development through Mobile Services," GSMA, January 2011, http://www.mobileactive.org/files/file_uploads/African_Mobile_Observatory_Full_Report_2011.pdf.

phone that helps them access the internet at a considerable fee. Overall, freedom to access the internet via computer-based applications and internet-enabled phone devices is generally unfettered. Rather, internet access is restricted mainly by economic and infrastructural constraints.

In early 2011, as demonstrations inspired by the Arab Spring erupted in North Africa, there were rumors that the government had ordered telecoms to block keywords such as "bullet," "Mubarak," and "Ben Ali" in SMS services, but the allegations were never confirmed. In April 2011, political and activist groups initiated a "walk-to-work" campaign to protest the government's apparent inaction in the face of spiraling food and fuel prices. The movement relied heavily on social media for mobilizing and publicizing the brutal response of security agencies to the campaign. In defense, the Uganda Communications Commission (UCC) directed internet service providers to temporarily block access to Facebook and Twitter; however, the directive was never carried out.

OBSTACLES TO ACCESS

The liberalization of the Uganda's telecommunications sector in 1997 created a very competitive environment that has nurtured dramatic growth in the expansion and usage of ICTs over the past 15 years. In 2007, a mere one million Ugandans were reported to be using the internet. As of the end of 2011, the Uganda Communications Commission (UCC) and the International Telecommunication Union (ITU) reported 4.6 million internet users (individuals using the internet at least once a month) in Uganda, amounting to 13 percent of the country's population of 34.5 million.[4] The growth in internet users coincided with an increase in subscriptions, with fixed-line internet subscriptions numbered at 88,000 and mobile broadband connections (through wireless modems) estimated at 850,000 in 2011.[5] In contrast, market penetration for voice technologies, both fixed-line and mobile, stands at 48.4 percent with nearly 75 million mobile telephone subscribers in 2011.[6] Mobile users account for more than 95 percent of voice connections. However, multiple SIM card ownership is common and estimated at 45 percent of total subscribers.[7]

[4] Uganda Communications Commission (UCC), "2010/11 Annual Post and Telecommunications Market Review," http://www.ucc.co.ug/endOfFYReview2011.pdf; International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[5] Ibid.

[6] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[7] UCC, "2010/11 Annual Post and Telecommunications Market Review."

There are currently 48 licensed telecommunications service providers, a good number of which offer both voice and data services.[8] More than 30 internet service providers (ISPs) offer both broadband and dial-up internet services.[9] The state-owned Uganda Electricity Transmission Company Ltd (UETCL), a licensed public infrastructure provider, has part ownership of Uganda Telecom (UTL). The rest of the licensed telecommunications service providers are privately-owned entities. There are no restrictions on licensing, and the entry of new providers in the market is by and large determined by market forces. There are no known obstacles placed by the government on entry into the sector.

The infrastructure of most internet operators currently consists of CDMA, GSM, VSAT satellite technology, and copper or optical fiber cables. In 2009, the country connected its national fiber backbone to the EASSy international submarine fiber optic cable system that was constructed along the east and southern coasts of Africa.[10] Ugandan telecommunications providers are also hooked to the TEAMs (The East African Marine System) and SEACOM marine fibers through Kenya, which sells bandwidth to ISPs in Uganda at a much cheaper cost than the previous satellite connections. Connection to these networks has not only led to exponential growth in Uganda's international bandwidth,[11] but also to decreasing costs of internet access alongside an increasing demand for data services and high speed internet. The highest growth rate has been registered in wireless broadband solutions, which accounted for more than 90 percent of internet subscriptions by the end of 2010.[12]

Many Ugandans access the internet through cybercafes, where it costs about 1,000 Ugandan shillings (US$0.40) for up to 30 minutes. Access to internet at workplaces, schools and libraries is also common. With mobile internet access becoming cheaper,[13] a growing number of Ugandans are able to use phones and other internet-enabled devices to access social networks, news sites, and other websites at a reasonable cost. For example, a mobile internet package through MTN Uganda, the country's leading telecom company, can cost Shs500 (US$0.20) for 10MB of data and Shs15,000 (US$6) for 300MB of data.[14] Free access to Facebook is also available to MTN and Orange mobile network subscribers.

However, even with the growing availability of cheap mobile internet bundles, internet-enabled devices are still costly in Uganda. In particular, excise duties and the value added tax

[8] Uganda Communications Commission (UCC), "Telecommunications Service Providers," http://www.ucc.co.ug/index.php?option=com_k2&view=item&layout=item&id=66&Itemid=66.
[9] Ibid.
[10] "Welcome to EASSy," accessed June 29, 2012, http://www.eassy.org/index-2.html.
[11] "Uganda - Broadband and Internet Market, Convergence," BuddeComm, September 2011, https://www.budde.com.au/Research/Uganda-Broadband-and-Internet-Market-Convergence.html?r=51.
[12] Ibid.
[13] "Ugandan telcos lower mobile Internet tariffs," IT News Africa, April 17, 2010, http://www.itnewsafrica.com/2010/04/ugandan-telcos-lower-mobile-internet-tariffs/.
[14] "MTN Mobile Internet," accessed June 29, 2012, http://mtn.co.ug/MTN-Internet/MTN-Mobile-Internet.aspx.

(VAT) levy have curtailed sales of both internet and non-internet-enabled phone devices.[15] Mobile phone vendors such as Huawei Technologies, a Chinese firm, reported selling only 30,000 Android-powered handsets that enable mobile phone internet access in 2011, compared to 200,000 phones sold in neighboring Kenya where the VAT on mobile handsets was scrapped two years ago.[16] Furthermore, many Ugandans cannot afford personal computers with regular internet connections, and only about one million Ugandans have access to computers.[17] The repeal of import taxes on computers some years ago facilitated increased computer usage and ownership; however, further growth has been hindered by a 2009 government ban on the importation of used computers which are cheaper alternatives to new computer sets.[18]

Other impediments to increased internet usage include the high cost of modems, which range between US$24 and US$41. A monthly limited internet package of 1GB costs US$18 and could not last a whole month for users who would like to experience the full range of internet capabilities,[19] while an unlimited broadband internet connection from Orange Uganda costs US$124 for one month and up to US$673 for six months. Across the five main firms in the industry, the average monthly cost of a 1GB subscription is US$20, and speeds are coverage-dependent, ranging from 236KB per second to 7.2MB per second. With an average per capita monthly income of US$110 in 2011,[20] the high cost effectively prices all but the wealthiest Ugandans out of regular internet access.[21] Furthermore, only 6 percent of Ugandans are connected to the national electricity grid (2 percent for rural areas). A much smaller number use fuel-powered generators and solar energy, while the rest of the population has no access to electricity.

While Ugandans residing in urban areas are able to access the internet through cafes, workplaces and schools, those in the rural areas—where more than 80 percent of the population lives—remain disproportionately underserved by ICTs. According to a 2008 survey by Audience Scapes, an online research program, only 3 percent of Uganda's rural population has access to the internet compared to 16 percent in urban areas.[22] In addition to internet access being prohibitively expensive, ICT infrastructure is particularly inadequate in

[15] David Mugabe, "Taxes hindering Uganda Internet penetration," New Vision Newspaper, September 27, 2011, http://www.africa-uganda-business-travel-guide.com/taxes-hindering-uganda-internet-penetration.html.
[16] Ibid.
[17] Isaac Imaka, "Uganda's journey to a computerised era," Daily Monitor, March 13, 2010, http://www.monitor.co.ug/News/National/-/688334/877862/-/wj8wrm/-/index.htm.
[18] Ibid.
[19] "MTN Mobile Internet."
[20] World Bank, "Gross national income per capital 2011, Atlas method and PPP," World Bank Databank, 2011, accessed July 18, 2012, http://databank.worldbank.org/databank/download/GNIPC.pdf.
[21] "Internet users in Uganda," Trading Economics, accessed June 29, 2012, http://www.tradingeconomics.com/uganda/internet-users-wb-data.html.
[22] "Internet Access in Uganda," Audience Scapes, accessed June 29, 2012, http://www.audiencescapes.org/country-profiles/uganda/country-overview/internet/internet-285.

rural areas, with private sector companies primarily investing in infrastructure projects in commercially-viable regions of the country. This disparity is exacerbated by low literacy rates in the same areas, which stands at 67 percent for rural Ugandans aged 10 and above,[23] and only 10 percent of Ugandans are estimated to be computer literate.[24]

In 2011, the Google Uganda domain became available in five local languages, making the popular browser more available to about five million Ugandans.[25] Nevertheless, Ugandans can only access news websites in three local languages (out of 40 languages and 56 native dialects) provided by the Vision Group, a media company partly owned by the government. The web versions of the newspapers include Bukedde.co.ug, Etop.co.ug and Orumuri.co.ug. Other news sites of major privately-owned newspapers are only accessible in English, which is not widely spoken in Uganda. The full extent of the internet's utility can only be enjoyed by all Ugandans with more widespread availability of content in local languages.

Over the past few years, the government has embarked on initiatives to improve rural connectivity, and a national ICT policy was finalized in 2010 to facilitate the proliferation of ICTs across the country. One of the policy's guiding principles is to "ensure access to IT services to men and women in both rural and urban areas."[26] Since 2007, Uganda's ICT ministry has been developing the National Data Transmission Backbone Infrastructure, which aims to ensure the availability of high bandwidth data connection in all major towns at reasonable prices.[27] The project, now under the provision of the National Information Technology Authority (NITA-U), involves the installation of over 1,500km of fiber optic cable and related equipment, including switches, optical transmission, data communication, fixed network, and video equipment, as well as computers and servers.[28] In addition, the UCC's Rural Communications Development Fund (RCDF) policy, established in 2001, aims to provide access to basic communications services within a reasonable distance to all Ugandans, leverage investment into rural communications, and promote ICT usage.[29] The

[23] Uganda Bureau of Statistics, "Statistical Abstract, 2011," accessed June 29, 2012, http://www.ubos.org/index.php?st=pagerelations2&id=31&p=related%20pages%202:Abstracts.
[24] Uganda Bureau of Statistics, "Statistical Abstract, 2011."
[25] Tabitha Wambui, "Google Uganda launches two new local language domains," Daily Monitor, August 4, 2010, http://www.monitor.co.ug/Business/Technology/-/688612/970404/-/uithj9/-/index.html.
[26] Ministry of Information and Communications Technology, "Information Technology Policy for Uganda," Republic of Uganda, February 2010, http://ict.go.ug/index.php?option=com_docman&task=doc_details&gid=48&Itemid=61.
[27] Ministry of Information and Communications Technology, "National Data Transmission Backbone and e-Government Infrastructure Project," Republic of Uganda, accessed June 29, 2012, http://www.ict.go.ug/index.php?option=com_content&view=article&id=69:national-data-transmission-backbone-and-e-government-infrastructure-project&catid=25:the-project&Itemid=93.
[28] "NBI/EGI Project," National Information Technology Authority – Uganda, accessed June 29, 2012, http://www.nita.go.ug/index.php/projects/nbiegi-project.
[29] "Rural Communications Development Policy for Uganda," UCC, January 2009, http://www.ucc.co.ug/index.php?option=com_k2&view=item&layout=item&id=56&Itemid=59.

RDCF also oversees the setup of internet cafes, internet Points of Presence (rural wireless connectivity networks with a 5-10km radius at costs, speeds and types of services comparable to those in the capital city, Kampala), ICT training centers, and web portals for districts (local government units).

The ICT sector is divided into three levels: policy, regulatory, and operational. The policy and regulatory levels are overseen by the UCC and NITA-U, while the operational level is composed of telecommunications, postal, information technology (IT), and broadcasting operators. Uganda's policy and regulatory environment was established through the Telecommunications Sector Policy Framework of 1996 and the Uganda Communications Act of 1997. The Ministry of Information and Communication Technology was set up in June 2006 with the mandate of providing strategic and technical leadership, overall coordination, support, and advocacy on all matters of policy, laws, regulations, and strategy for the ICT sector.[30]

The Uganda Communications Commission (UCC) is the statutory body charged with the regulation of telecoms and ISPs in the country, and its policy goals focus on expanding telecommunications infrastructure and services. The body has taken steps to avail information about the regulatory process on its website and through publications and press releases. However, the general perception is that accessible, complete and understandable information is not available, and that the UCC is not entirely independent from the executive arm of government.

The UCC also promotes developments in Uganda's communications industry and issues licenses for ICT infrastructure and service providers. There are no restrictions on licensing, and the UCC issues two types of service licenses: Public Service Provider (PSP) and Public Infrastructure Provider (PIP).[31] The application fee for both license types is US$2,500 dollars (a PIP license requires a one-off initial fee of US$100,000), and annual fees range from US$3,000-$10,000.[32] These licenses allow holders to either set up telecommunications infrastructure or provide telecommunications services. The UCC levies a 1 percent charge on providers' annual revenue.

[30] Ministry of Information and Communications Technology, "About MOICT," Republic of Uganda, accessed June 29, 2012, http://ict.go.ug/index.php?option=com_content&view=article&id=55.
[31] "UCC Licensing Regime," UCC, accessed June 29, 2012, http://www.ucc.co.ug/index.php?option=com_k2&view=item&layout=item&id=52&Itemid=55.
[32] "Uganda Communications Fees Structure," UCC, 2008, accessed June 29, 2012, http://www.ucc.co.ug/images/stories/fees/Fees_Structure.pdf.

LIMITS ON CONTENT

To date, there are no known restrictions on internet applications. Both local and international online news, media and political blogs, various social media platforms such as Facebook and Twitter, as well as human rights websites are widely accessible. However, the first reported case of internet censorship in Uganda occurred in 2006 when the government allegedly blocked access to the news website, RadioKatwe.com, in advance of the presidential and parliamentary elections. The website published content submitted by internet users from all over the world that was critical of the government. Following orders by the UCC, local ISPs reportedly filtered the site by blocking its internet protocol (IP) address and nearly 700 other sites hosted by the same server, which was based in the United States.[33] Access to the website was later restored, but its administrators have since shut it down.

A second government attempt to interfere with citizens' online activity was reported in early 2011, as demonstrations inspired by the Arab Spring erupted in North Africa. There were rumors that the government had ordered telecoms to block and regulate the use of some keywords such as "bullet," "Mubarak," and "Ben Ali" in SMS services; however, these allegations were never confirmed. In April 2011, political and activist groups initiated a "walk-to-work" campaign to protest the government's apparent inaction in the face of spiraling food and fuel prices. The movement relied heavily on social media for mobilizing and publicizing the brutal response of security agencies to the campaign. In defense, the UCC directed ISPs to temporarily block access to Facebook and Twitter.[34] The regulator reasoned that the move was intended "to eliminate the connection and sharing of information that incites the public"; however, the directive was never carried out.[35] Later in 2011, a government minister accused the opposition of using social media to incite the youth to revolt the government.[36]

Although Uganda's media remains open and vibrant, the practice of self-censorship has been growing following the harassment and arrest of journalists as well as shut downs of media houses believed to be anti-government.[37] Reports of the persecution or prosecution of

[33] Reporters Without Borders, "Net Censorship Reaches Sub-Saharan Africa," February 24, 2006, http://en.rsf.org/uganda-net-censorship-reaches-sub-saharan-24-02-2006,16569.html.
[34] Karen Allen, "African jitters over blogs and social media," BBC News Africa, June 15, 2011, http://www.bbc.co.uk/news/world-africa-13786143.
[35] Rebekeh Heacock, "Uganda: Government Attempts to Block Facebook, Twitter as Protests Continue," Global Voices, April 19, 2011, http://globalvoicesonline.org/2011/04/19/uganda-government-attempts-to-block-facebook-twitter-as-protests-continue/.
[36] "Uganda anger at opposition's Twitter 'insurrection'," BBC News Africa, August 22, 2011, http://www.bbc.co.uk/news/world-africa-14491135.
[37] See, "Freedom House Condemns Crackdown on Journalists, Social Media in Uganda," Freedom House, Press Release, April 22, 2011, http://freedomhouse.org/article/freedom-house-condemns-crackdown-journalists-social-media-uganda.

journalists or citizens for online expression have been rare; nevertheless, the self-censorship practiced by those in the mainstream media may well extend online.

In recent years, regime critics and opposition political parties have taken to the internet as a platform for political debate and an informal means of disseminating information to the masses. During the February 2011 elections period, crowdsourcing and crowd-mapping technology offered citizens a way to monitor various stages of the election process. Two websites, Uchaguzi and Uganda Watch 2011,[38] were created to monitor the elections, allowing citizens to report information and events via SMS texts as they happened. Integrating SMS, online forums, email and Twitter, the platforms attempted to support fair and transparent elections in real time. In addition, social media has been widely used as a platform for protest in Uganda, mainly by activist groups. For example, the continuing campaign against the government's proposed give-away of Mabira, Uganda's largest rainforest, to an investor has been sustained partly through SMS, Facebook, and email alerts. The president's proposal to clear parts of the forest to pave way for a sugar plantation is opposed by environmentalists, citizen groups, and some politicians who have used social media to disseminate alerts with key facts about Mabira and the environment in Uganda, and to occasionally call for action and demonstrations.

Despite growing internet usage in Uganda, the government, opposition groups, and civil society in Uganda have not fully taken advantage of the opportunities for mobilization offered by the internet. Most local websites carry very little up-to-date information, have few dynamic links, and contain little or no interactive features.

VIOLATIONS OF USER RIGHTS

Uganda's Constitution provides for freedom of expression, speech and association, as well as the right to access information. Uganda was among the first countries in Africa, and among only nine on the continent, to enact freedom of information legislation.[39] However, several laws—including the Press and Journalists Act, the Electronic Media Act, the Anti-Terrorism Act,[40] and sections of the Penal Code—appear to negate these constitutional guarantees for the freedom of expression. For instance, both the Press and Journalists Act and the Electronic Media Act introduce statutory licensing of journalists and create statutory regulatory authorities, such as the Media Council and Broadcasting Council, whose

[38] Website links: Uchaguzi, http://www.uchaguzi.co.ug/; Uganda Watch 2011, http://www.ugandawatch.org/.

[39] The Access to Information Act provides for the right to access information pursuant to Article 41 of the Constitution, the right to prescribe the classes of information referred to in that article, the procedure for obtaining access to that information, and for related matters.

[40] "The Anti-Terrorism Act, 2002," International Commission of Jurists, accessed June 29, 2012, http://www.icj.org/IMG/ATA.pdf.

independence is believed to be compromised because of the government's major hand in their composition. The Penal Code still contains provisions on criminal libel and the promotion of sectarianism, for which penalties include lengthy jail terms. None of these laws contain specific provisions on online modes of expression, but they could arguably be invoked in relation to online communication. In any case, they create a "chilling effect" on freedom of expression generally.

In 2010, the government passed three cyber laws—the Electronic Signatures Act, Electronic Transactions Act, and Computer Misuse Act—which focus mainly on cybercrimes and terrorism. [41] The Computer Misuse Act seeks to prevent unlawful access, abuse or misuse of information systems through computers and electronic devices such as mobile phones. These laws are seen among local stakeholders as necessary to enhance safety and security on the internet.

Following the Al-Shabab terrorist attacks during the World Cup on July 11, 2010 in Kampala, Parliament hurriedly passed the Regulation of Interception of Communications Act, which requires telecommunication companies to install equipment that enables the electronic surveillance of people suspected of terrorism without the need of a court order. The Act also gives the government permission to tap into personal communications deemed to be a threat to national security.[42] This action can be requested by the Minister for Security and granted after an order by a High Court judge. In effect, the Act provides undue powers to state organs to intercept private communications and potentially threatens free expression through the restriction of content and access to information. Some media observers worry that the Act "will likely embolden the government to go after online work more aggressively. It will snoop around more, hacking into people's emails in the name of ensuring national security."[43]

In 2010, Timothy Kalyegira, editor for the now defunct online publication, Uganda Record, became the first journalist to be arrested for online content. He was charged with criminal libel over a story accusing the government of having a hand in the July 11th Kampala bomb blasts that killed 78 people.[44] Since then, Kalyegira has appeared before police 18 times with critics arguing that the government has deliberately delayed his case. After the incident,

[41] "Laws: Cyber Laws," National Information Technology Authority - Uganda, accessed June 29, 2012, http://www.nita.go.ug/index.php/policies-and-laws/cyber-laws.
[42] Amnesty International, "Uganda: Amnesty International Memorandum on the Regulation of Interception of Communications Act, 2010," December 14, 2010, http://www.amnesty.org/en/library/asset/AFR59/016/2010/en/4144d548-bd2a-4fed-b5c6-993138c7e496/afr590162010en.pdf.
[43] Ibid.
[44] Anthony Wesaka, "Journalist remanded over bomb blasts story," Daily Monitor, June 1, 2011, http://www.monitor.co.ug/News/National/-/688334/1172874/-/c0wtytz/-/index.html.

Ugandan journalists predicted that there would be more online monitoring by the government.

Beyond the new Regulation of Interception of Communications Act, there is no direct evidence of government surveillance of telecommunications, although it is widely believed that security agencies, sometimes with the complicity of telecommunication companies, quietly monitor and sometimes interfere with the communications of government opponents.[45] Another potentially worrying trend is SIM card registration for mobile phone users, which started in March 2012. The exercise involves the recording of personal data, including photographic and biometric data.[46] According to the UCC, the registration requirement aims to curb crime conducted through mobile phones.[47] By contrast, internet subscription requires minimal personal information, and there are no identification or registration requirements needed to access the internet from cybercafes.

[45] "Uganda's Opposition Calls for MTN Boycott," Telecom Africa (blog), March 29, 2011, http://telecomafrica.blogspot.com/2011/03/ugandas-opposition-calls-for-mtn.html.
[46] "Sim Card Registration," UCC, accessed June 29, 2012, http://www.ucc.co.ug/index.php?option=com_k2&view=item&layout=item&id=93&Itemid=77.
[47] Flavia Nalubega, "SIM card registration to curb crime – UCC," Daily Monitor, March 7, 2012, http://www.monitor.co.ug/Business/-/688322/1360918/-/4xpbt1/-/index.html.

UKRAINE

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Free**
Obstacles to Access (0-25)	n/a	7
Limits on Content (0-35)	n/a	8
Violations of User Rights (0-40)	n/a	12
Total (0-100)	**n/a**	**27**

* 0=most free, 100=least free

POPULATION: 46 million
INTERNET PENETRATION 2011: 31 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Partly Free

INTRODUCTION

The citizens of Ukraine enjoy largely unhindered access to the internet. The country's internet infrastructure has been rapidly developing since the early 1990s, and today information and communication technologies (ICTs) are beginning to have a more notable influence over the political process, with diverse and generally independent online media and social networks playing a key role. This comes in part as a result of the 2005 Orange Revolution in which communication technologies played a significant role.[1]

Ukraine has relatively liberal legislation governing the internet and access to information. In 2011, a number of state initiatives were introduced that aim to control electronic media and exercise surveillance over internet content in order to "protect public morality" and limit other forms of "undesirable" content. Although the initiatives are still up for discussion as of April 2012, the regulations embody the potential for indirect formal and informal controls over political and social content online.

Social media networks are also gaining ground, with activists increasingly using the platforms for organizing and promoting ideas. Political parties and the government have also started using the internet as another tool of political competition, engaging in both legitimate forms of communication such as social media profiles and blogging, and manipulative techniques such as trolling.

[1] Joshua Goldstein, "The Role of Digital Networked Technologies in the Ukrainian Orange Revolution," Berkman Center Research Publication No. 2007-14, December 2007, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf.

OBSTACLES TO ACCESS

Internet penetration in Ukraine has been growing steadily, due in part to diminishing costs and the increasing ease of access, including to mobile internet. According to the International Telecommunication Union (ITU), Ukraine had an internet penetration of 30.6 percent in 2011,[2] a major increase from 4.5 percent in 2006.[3] For fixed-broadband subscriptions, the penetration rate was approximately 7 percent in 2011.[4] Meanwhile, Ukraine ranks eighth in the world for download speeds, with an average download speed of 1190 Kbps,[5] and access to broadband internet in Ukraine is fairly affordable. A monthly unlimited data plan with a 1 Mb broadband channel costs 80-120 UAH (US$10-15), while the average monthly wage in the country was 2,942 UAH (US$368) in April 2012.[6]

Of current internet users, 56 percent live in urban areas, while internet penetration in smaller towns and rural areas is currently below 20 percent.[7] The level of infrastructure differs between urban and rural areas, contributing to the gap in number of users. Most people access the internet from home and/or work, though internet cafes are present in most major cities, and many middle- and higher-end cafes and restaurants often provide free WiFi access. Access is also common in public libraries and schools.

Mobile phone penetration has also continued to grow, reaching 123 percent in 2011.[8] Use of mobile internet is gaining in popularity, and an estimated 16 percent of Ukrainian urban dwellers have access to mobile internet.[9] Cost continues to be the main barrier to higher mobile internet use. Third-generation (3G) mobile phone frequencies are still owned by the Ministry of Defense, but the ministry has stated plans to convert the networks for use by

[2] Differing from ITU statistics, the research company, InMind, found that there were 14.3 million Ukrainians ages 15 and up who used the internet at least once a month in September 2011,[2] comprising 36 percent of the total population. InMind, "Рост уровня проникновения интернета в Украине существенно замедлился" [Growth of Internet Penetration Level In Ukraine Has Slowed Significantly], AIN.UA, October 19, 2011, http://ain.ua/2011/10/19/62100 (In Russian).

[3] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[4] "ШПД в Украине продолжает расти" [Broadband Internet Access in Ukraine Continues to Grow], iKS-Consulting, December 16, 2011, http://www.iksconsulting.ru/news/4071555.html.

[5] Pando Networks, "Report: U.S. Broadband Speeds Remain Slow, 26th in the World," SiliconFilter, September 20, 2011, http://siliconfilter.com/report-u-s-broadband-still-slow-ranks-26th-in-the-world/.

[6] State Statistics Service of Ukraine, "Average monthly wage by region in 2012," accessed on June 15, 2012, http://www.ukrstat.gov.ua/operativ/operativ2012/gdn/reg_zp_m/reg_zpm12_u.htm.

[7] InMind, "Рост уровня проникновения интернета в Украине существенно замедлился" [Growth of Internet Penetration Level In Ukraine Has Slowed Significantly], AIN.UA, October 19, 2011, http://ain.ua/2011/10/19/62100.

[8] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[9] Erik Johannisson, "Ericsson 2011 Ukraine Country Study: ConsumerLab Research Results," MaxKutik on SlideShare, December 22, 2011, http://www.slideshare.net/MaxKutik/erik-johannisson-consumerlab-research-results-10663813.

mobile operators in 2012.[10] The only commercial 3G license was previously owned by state-run Ukrtelecom. Now that Ukrtelecom has been privatized and its 3G division is a separate company, the chances for frequency conversion are said to be much higher.[11]

YouTube, Facebook, Twitter, and international blog-hosting services such as Wordpress and LiveJournal are freely available. There are no known instances of the authorities demanding internet service providers (ISPs) to block any Web 2.0 applications, protocols, or instant communication tools. The backbone connection of UA-IX (Ukrainian internet exchange, a mechanism of traffic exchange and connection to the wider internet for Ukrainian ISPs) to the international internet is not centralized, and major ISPs each have their own channels, managed independently.

The Ukrainian telecommunications market is fairly liberal and in the process of slow development. The largest telecom company and top-tier ISP, Ukrtelecom, previously had 92.7 percent state ownership but was privatized in March 2011.[12] Though no longer state-owned, Ukrtelecom is the largest ISP in the country and possesses Ukraine's primary network, trunk, and zone telecom lines,[13] but it does not decisively control the other major ISPs. Other telecommunications providers are dependent on leased lines, since Ukrtelecom owns the majority of the infrastructure, and many alternative providers do not have sufficient resources to build their own networks. Among the major private ISPs are Volia, Triolan, Vega and Datagroup; however major mobile service providers, like Kyivstar and MTS, are also starting to provide broadband internet access.[14] There are about 400 ISPs in Ukraine according to the State Commission on Communications and Informatization.[15] Regional ISPs are usually smaller local businesses, and regional dominance largely depends on business and power connections in a specific region, making the market prone to corruption.

Ukrchastotnagliad, the Ukrainian frequencies supervisory center, reports that 86 operators have licenses to provide satellite communications services in Ukraine, and companies providing internet access using satellite technologies in Ukraine include Ukrsat, Infocom-

[10] Ihor Burdyga, "Операторов свяжут с третьим поколением" [Operators To Be Connected To Third Generation], Kommersant Ukraine, December 12, 2011, http://www.kommersant.ua/doc/1833438.

[11] "Частоты для 3G-связи освободят в следующем году" [Frequencies for 3G Communications to be Freed Next Year], AIN.UA, December 8, 2011, http://ain.ua/2011/12/08/67725.

[12] 92.8 percent of shares sold to ESU, a Ukrainian subsidiary of the Austrian company EPIC. Source: "Укртелеком продан" [Ukrtelecom Sold], Dengi.Ua, March 11, 2011, http://dengi.ua/news/77761_Ukrtelekom_prodan_.html.

[13] "Ukraine: Country Profile 2010," OpenNet Initiative, December 21, 2010, http://opennet.net/research/profiles/ukraine.

[14] "Количество пользователей широкополосного доступа в Украине достигло 5,6 млн" [Number Of Broadband Internet Users in Ukraine Reaches 5.6 Million], AIN.UA, December 16, 2011, http://ain.ua/2011/12/16/68574.

[15] "Во 2 квартале количество абонентов провайдеров Интернет увеличилось на 6,4%" [In Second Quarter Number Of Subscribers Of Internet Providers Grew By 6.4%], Delo.Ua, July 26, 2007, http://delo.ua/tech/vo-2-kvartale-abonentov-provaj-44242/.

SK, Spacegate, Adamant, LuckyNet, Ukrnet, and Itelsat. With the exception of Infocom-SK,[16] all these companies are private.[17] The three major players in the mobile communications market are Kyivstar (owned by Dutch VimpelCom Ltd.), MTS Ukraine (owned by Russian AFK Sistema), and life:) (owned by Astelit, whose main shareholders are Turkish Turkcell and Ukrainian System Capital Management). Together these players hold over 93 percent of the mobile communications market.[18]

There are no obvious restrictions or barriers to entry into the ICT market, but any new business venture, be it an ISP or an internet cafe, faces the usual bureaucracy, corruption, and legal/tax hurdles common to the Ukrainian business environment. In particular, the Ukrainian ICT market has been criticized for its difficult licensing procedures for operators. Under the 2003 Law on Communications, operators are required to have a license before starting activity.

The ICT sector is regulated by the National Commission on Communications and Informatization (NCCIR), which was reformed from the previous National Commission on Communications (NCCR) in November 2011. Members of NCCIR are appointed by the President of Ukraine.[19] Because of widespread corruption in the political system and the lucrative nature of business in the ICT sector, appointments to the Commission are often not transparent. The 2003 Law on Communications does not guarantee the independence of the NCCIR. Instead, industry experts point to a number of inconsistencies between sector laws, and the NCCIR's work has often been obstructed by claims of non-transparent decisions and operations. For instance, in July 2011 the NCCIR (then NCCR) refused to prolong the operating license of mobile provider Kyivstar for GSM 900/1800 frequencies.[20]

---

[16] Infocom-SK was founded in 1991 jointly by state-owned Ukrtelecom and Controlware, a German telecommunications company. "History," Infocom, accessed on June 15, 2012, http://infocom.ua/catalogue.jsp?catalogueId=3000&cataloguerId=6070&lang=3.

[17] "Ukraine: Country Profile 2010," OpenNet Initiative.

[18] iKS-Consulting, "«Киевстар» потерял более 80 тысяч абонентов" [Kyivstar Has Lost Over 80 Thousand Subscribers], AIN.UA, November 1, 2011, http://ain.ua/2011/11/01/63452.

[19] National Commission on Regulation of Communications and Informatization, accessed on January 10, 2012, http://en.nkrz.gov.ua/.

[20] "НКРС отказалась продлевать «Киевстар» лицензию на мобильную связь" [NCCR Refused to Prolong Kyivstar's mobile communications license], ITC.ua, July 8, 2011, http://itc.ua/news/nkrs_otkazalas_prodlevat_kievstar_licenziyu_na_mobilnuyu_svyaz_54417/. The NCCR said Kyivstar first acquired their license in 1996 for 15 years under the acting Law on Telecommunications, while in 2004 a new Law on Telecommunications came into power, thus making the old Law (and any agreements under it) void. NCCR believed Kyivstar was not entitled to simply pay 30 percent of the license price to prolong said license, but ought instead to pay 200 percent of the license price to acquire two new licenses for GSM 900 and GSM 1800 each. This would cost Kyivstar around 19 million UAH. As a result, in September 2011 Kyivstar had to pay the full price for two new licenses in order to continue their activities in the market. See also, "Киевстару выдали новые лицензии на мобильную связь" [Kyivstar Given New Mobile Communications Licenses], LigaNet, September 8, 2011, http://biz.liga.net/all/it/novosti/2048038-kievstaru-vydali-novye-litsenzii-na-mobilnuyu-svyaz.htm.

LIMITS ON CONTENT

There is no practice of institutionalized blocking or filtering, or a regulatory framework for censorship of content online, although indirect attempts at creating legislation which could help censor or limit content are occurring. For example, a new set of amendments to the law "On Protection of Public Morals"[21] (#7132) was adopted at its first reading on October 18, 2011 by the Ukrainian Parliament and has caused widespread concern from the Ukrainian media and international media rights groups. The law deals with pornography, eroticism, hate speech, violence, and explicit language; however, it has been criticized for being written in such a way where the definitions of these terms are so vague that anything could be considered erotic, hate speech, or explicit and vulgar language, especially on the internet. The proposed amendments would obligate ISPs to remove or block the offensive content for 24 hours or, if such content is found to be hosted outside of Ukraine, ISPs would have to limit Ukrainian users' access to such content, effectively introducing a practice of filtering content. This, some experts believe, opens a potential area for manipulation and indirect censoring of unwanted online political/social content or websites.[22]

Critics of the amendments include Reporters Without Borders, who said the amended law would be in violation of Article 10 of the European Convention of Human Rights and the Declaration of Human Rights, both ratified by Ukraine.[23] Aside from the vague definitions, experts are worried that the law gives extraordinary powers to the National Expert Commission on the Protection of Public Morals (NECPPM), allowing it to issue orders to block websites and access to content within 24 hours without a court order or any provisions for website owners/content authors to appeal. At the moment, access providers and content hosts are not responsible for the content transmitted or hosted, and may block or require a user to remove content only when provided with a court order.

A bill attempting to regulate copyright issues online was introduced in parliament by Minister of Parliament (MP) Maksym Lutsky and passed the first reading in February 2011.[24]

---

21 "Проект Закону про внесення змін до Закону України "Про захист суспільної моралі"" [Draft Bill on Introducing Changes to the Law of Ukraine "On Protection of Public Morals"], #7132, Official Website of Ukrainian Parliament, September 15, 2010, http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_1?id=&pf3511=38551.

22 Natalka Zubar, Olexander Severyn, Viktor Garbar, "New Ukrainian Law Could Block Any Site Including Facebook or Youtube," Maidan, October 20, 2011, http://world.maidan.org.ua/2011/new-ukrainian-law-could-block-any-site-including-facebook-or-youtube.

23 "Генсек "Репортерів без кордонів" стурбований наміром депутатів обмежити ЗМІ" [Reporters Without Borders General Secretary Concerned With MP's Intention To Limit Mass Media], Ukrainska Pravda, October 28, 2011, http://www.pravda.com.ua/news/2011/10/28/6711923/.

24 Проект Закону про внесення змін до деяких законодавчих актів України щодо врегулювання питань авторського права і суміжних прав [Draft Bill on Introducing Changes to Some Legislative Acts of Ukraine on Regulation of Copyright And Adjacent Rights Issues], Ukrainian Parliament Website, accessed on June 15, 2012, http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_1?pf3511=37985.

Opposition MPs believe the bill is aimed at censoring unwanted content rather than fighting piracy and copyright theft and are especially worried about creating a precedent that would allow authorities to close down websites that violate the bill for seven days without a court order. Other changes the bill proposes include introducing civil and criminal responsibility for illegal content for users, ISPs, and hosting providers. Opposition MPs believe a bill like this to be an attempt at controlling the online information sphere in anticipation of the next parliamentary election in the fall of 2012.[25] The second reading of the bill was scheduled to take place on May 16, 2012, however, due to protests by activists of the Internet Party of Ukraine and critical comments from other MPs and the public, the bill was removed from the agenda, and the second reading was postponed indefinitely.[26]

There have been periodic instances of state pressure to remove online content. Most recently in February 2012, the activist website Road Control, which collected crowd-sourced information about the corrupt behavior of road police officers, was taken offline after the website hosting company was approached by officials with a court order saying the website was involved in a civil lawsuit and therefore had to be temporarily taken down. The website soon resumed its work on a different host, but founders said they believed the civil lawsuit against Road Control was initiated by a road police officer who was featured in one of the videos on the website and filmed saying to the driver, "Stop reading Road Control, we'll close it down soon, I promise you."[27]

The internet often serves as a last reserve outlet for news and content that is prevented from being aired or published in traditional media. Such was the case with the now ubiquitous video from May 2010 of a wreath blown over by the wind that fell onto the head of President Victor Yanukovich during a joint honor ceremony with the Russian president in Kyiv. Although filmed by all, the video did not run in the evening news of most national channels due to calls from the authorities or self-censorship by the editorial staff,[28] which is often exercised on certain topics that relate to the business/political interests of media owners. However, the video leaked onto YouTube and quickly became an internet sensation, gaining 700,000 views during the first 18 hours online.[29]

---

[25] "Нардеп ПР хочет добиться закрытия сайтов без суда в течение 7 дней" [Party of Regions MP Wants To Take Down Websites Without Court Order In 7 Days], AIN.ua, April 20, 2012, http://ain.ua/2012/04/20/81836.

[26] "Законопроект об интернет-цензуре стал большой проблемой для его инициатора" [Internet Censorship Bill Becomes a Big Problem For Its Author], InternetUA, May 22,2012, http://internetua.com/zakonoproekt-ob-internet-cenzure-stal-bolshoi-problemoi-dlya-ego-iniciatora.

[27] "Сайт «Дорожного контроля», на котором собирались жалобы на сотрудников ГАИ, заблокирован по решению суда (обновлено)" [Website of Road Control, which collected complaints about road police officers, blocked by court order (updated)], AIN.ua, February 14, 2012, http://ain.ua/2012/02/14/73581.

[28] "Журналісти "1+1" розповіли, як їм "зарізали" відео про вінок" ["1+1" Journalists Told of How Their "Wreath" Video Was Cut], Ukrainska Pravda, May 21, 2010, http://www.pravda.com.ua/news/2010/05/21/5064773/.

[29] Maksym Savanevsky, "Янукович з вінком б'є всі рекорди українського інтернету" [Yanukovych With Wreath Beats All RecordsOf Ukrainian Internet], Watcher, May 18, 2010, http://watcher.com.ua/2010/05/18/yanukovych-z-vinkom-bye-vsi-

Attempts to manipulate the online news landscape are not numerous, but there are some pro-government news websites, as well as online media which support certain political figures or political ideas. Some online news websites belong to media holdings owned by oligarchs close to the ruling Party of Regions and other political forces. By and large, though, online media are varied and represent many opinions on the political spectrum, with a key cluster of independent media playing the role of watchdogs and conducting investigative journalism. Discussion of political and social issues is free on internet forums and in comments on news sites like *Ukrainska Pravda* and *Korrespondent*. Access to international media websites is also unfettered.

A more common method of manipulation is the use of paid commentators or "trolls" on news websites and on social networks.[30] This phenomenon becomes especially active around election time, when various political supporters engage in defamatory and offensive comments on issues of politics, nationality, language, etc. on media websites. Most political analysts, however, do not see this as an effective political strategy, as users quickly recognize the trolls and do not take the commenters seriously. Increasingly, Ukrainian politicians are realizing the value of social media, and many have started accounts on Facebook and Twitter, LiveJournal, or YouTube in the hopes of engaging their voters.[31]

The Ukrainian blogosphere is fairly active, although less so than the Russian LiveJournal community, which houses many more politically-active citizens. According to Yandex, in 2011 there were 1.1 million Ukrainian blogs, up from 700,000 in 2010, and blogs are increasingly appearing as a genre of online news websites.[32] In addition, there are about 500,000 Ukrainian Twitter accounts, with a large majority of them in Kyiv.[33] The Ukrainian segment on Facebook continues to grow, with nearly two million users as of April 2012.[34]

Ukrainian bloggers, online personas, NGOs, and citizen movements are joining forces and creating online projects aimed at scrutinizing government policies, monitoring elections, and

rekordy-ukrayinskoho-internetu/.

[30] Viktor Bishchuk, "Є вакансія: інтернет-українофоб на півставки" [Job Opening: Part-Time Ukrainophobe], ZIK, August 17, 2011, http://zik.ua/ua/news/2011/08/17/304029.

[31] Yelena Gladskih, "Как используют блоги украинские политики" [How Ukrainian Politicians Use Blogs], Delo.Ua, February 12, 2011, http://delo.ua/ukraine/kak-ispolzujut-blogi-ukrainski-152081/.

[32] Yandex, "Антон Волнухін, Яндекс «Дослідження української блогосфери 2011»" [Anton Volnukhin, Yandex "Research on Ukrainian Blogosphere 2011"], presented at Microsoft BlogFest 2011, shared by Microsoft Ukraine, November 19, 2011, http://docs.com/G65I.

[33] "Яндекс дружит с Твиттером" [Yandex Gets Friendly With Twitter], Yandex Company Blog, February 21, 2012, http://clubs.ya.ru/company/43938.

[34] "Кількість українських користувачів Facebook опустилась нижче 2 млн" [Number Of Ukrainian Users On Facebook Fell Below 2 Million], Watcher, April 20, 2012, http://watcher.com.ua/2012/04/20/kilkist-ukrayinskyh-korystuvachiv-facebook-opustylas-nyzhche-2-mln/ [In Ukrainian].

uncovering corruption in the higher ranks of power.[35] Among successful examples is the Save Old Kyiv movement[36] against illegal construction in the city, which originated on LiveJournal. Another example involved the use of Twitter to engage users in citizen journalism in the Elect_Ua project during the 2010 local elections, when a group of activists and journalists popularized the hashtag "#elect_ua" and called on Twitter users to report violations from their polling stations in every region. Out of 19,450 tweets with the hashtag, over 1,700 were confirmed as possible violations of electoral process.[37] The "#elect_ua" hashtag remains active and is still used by Twitter users today.

VIOLATIONS OF USER RIGHTS

The right to free speech is granted to all citizens of Ukraine in Article 34 of its Constitution, although in practice this right is frequently violated. Part three of Article 15 of the Constitution also forbids censorship, though this norm is also routinely violated, with especially grave violations observed during the time of President Leonid Kuchma (before the 2004-2005 Orange Revolution). In addition, Article 171 of the Criminal Code of Ukraine provides fines and detention sentences for obstructing journalists' activity. The Ukrainian judiciary, however, is prone to the same level of corruption evident in other branches of power, and for many businesses, including media companies, bribes remain the main guarantee of successful consideration of their affairs in courts.[38]

The law "On Protection of Public Morals" (discussed above) in its 2003 primary incarnation, along with the National Expert Commission for the Protection of Public Morals, was instrumental in the case of one of the most popular Ukrainian file-exchange networks, Infostore.org. In December 2008, the Ministry of Internal Affairs searched the premises of the website and confiscated servers and other equipment, accusing the service of hosting pornographic materials. While there were such materials among files hosted on the website, the owners and their supporters believe the ministry had ulterior motives for taking down

[35] Examples include the New Citizen partnership's initiative ЧЕСНО[35] (Honestly, a movement for transparent and fair parliamentary elections), and PRYAMA DIYA[35] (Direct Action, a movement of student unions organizing street protests on relevant issues).

[36] Save Old Kyiv movement, http://saveoldkyiv.org/. During its activity, Save Old Kyiv activists were able to stop several instances of construction in historical areas of Kyiv, such as Peyzazhna Alley[36] or the corner of Prorizna in the heart of the city. "Прорізна, 3-5 (сквер)" [Prorizna, 3-5 (Corner Park)], Save Old Kyiv, accessed on January 10, 2012, http://saveoldkyiv.org/hotspot/prorizna-skver.

[37] "(прес-реліз) 1700 повідомлень про можливі порушення – результат Twitter-трансляції місцевих виборів" [(press-release) 1700 Tweets About Possible Violations – Result of Local Elections Twittercast], Blog of Elections Twittercast Project, November 3, 2010, http://electua.blogspot.com/2010/11/1700-twitter.html.

38 "Судова реформа не розвіяла сутінків у бізнес-настроях" [Judiciary reform does not banish twilight in business mood], Deutsche Welle, June 1, 2012, http://www.dw.de/dw/article/0,,15992775,00.html.

Infostore.org and have accused the ministry of limiting freedom of speech. Since this incident, Infostore.org has been unavailable.[39]

Criminal responsibility for libel/defamation has been abolished in Ukraine since 2001, and despite several attempts by various MPs to reintroduce it, libel is currently considered a civil offense, punishable by fines.[40]

In 2011, online journalists achieved similar status and privileges as traditional journalists, such as being able to get accreditation for parliament sessions and other official meetings frequented by the press. Nevertheless, there has been an ongoing discussion about the need for online media to register, with some suggesting that registration would provide additional mechanisms for protecting journalists, while others refute the idea, considering any form of registration to be an inhibition to press and internet freedom.[41]

While there have been no instances of journalists arrested for posting content online, there have been several cases of law enforcement action against ordinary users. The most notorious case is that of Oleg Shinkarenko, a LiveJournal blogger and journalist, who in July 2010 was visited by representatives of the Ukrainian Security Service claiming they had allegedly found threats aimed at President Yanukovich on Shinkarenko's blog.[42] The blogger was asked to attend a meeting at the Kyiv Prosecutor's office, where he was told his posts constituted a crime according to Article 346 of the Criminal Code. The blog posts had contained sharp criticism of the current government and ruling party, as well as comments used to question the authority of President Yanukovich and "curse" him. While Shinkarenko himself saw no crime or threats in his words, he was released after providing a written promise to never again threaten the authorities in such a form online. The offensive posts were also removed from his blog but not by him, prompting suspicions that the Security Service had broken into

[39] Alexey Mas, "Сервис Infostore и МВД!" [Service Infostore and MIA!], Alexey Mas on the Internet, Business and Infostore Blog, December 31, 2009, http://alexeymas.livejournal.com/ (entry later deleted).

[40] Due to generally lax libel case attitudes in Ukraine, rich and powerful Ukrainians use libel tourism as a mechanism of punishing the media. Britain, where the burden of truth is on the defendant, has seen two such cases. In the most recent case, Ukrainian businessman Dmytro Firtash sued the *Kyiv Post* newspaper and website at the end of 2010 for libel in Britain over an article on RosUkrEnergo, a company owned jointly by Firtash, a Ukrainian partner, and Russian Gazprom. The lawsuit prompted the *Kyiv Post* to block access to its website from the United Kingdom. The British judge eventually dismissed the case for its weak link to English jurisdiction. Source: "Ukraine: free speech vs. Firtash," Beyondbrics blog, *Financial Times*, February 24, 2011, http://blogs.ft.com/beyond-brics/2011/02/24/ukraine-free-speech-vs-firtash/#axzz1y8aSZXqA.

[41] Ukrainian Internet Association, "Підсумки прес-конференції: "Саморегулювання вітчизняних електронних медіа як альтернатива державному регулюванню в Українському сегменті Інтернет" [Summary of Press-Conference: "Selfregulation of Ukrainian Electronic Media As An Alternative To State Regulation In The Ukrainian Internet Segment"], InAU (Ukrainian Internet Association), July 19, 2011, http://www.inau.org.ua/170.3675.0.0.1.0.phtml.

[42] "СБУ: блоггер угрожал Януковичу" [SBU (Ukrainian Security Service): Blogger Threatened Yanukovich], TSN.ua, July 30, 2010, http://ru.tsn.ua/ukrayina/sbu-blogger-ugrozhal-yanukovichu.html.

his site. Commentators saw this as a precedent for political censorship and a sign that it would now be harder to criticize government officials online.[43]

In another case in December 2011, the news website *Levy Bereg* (*Left Bank*) was contacted by the Kyiv Cybercrime and Trafficking Administration with a demand to disclose all information about the website's owner and the identity of the website's registrar. The administration claimed they were investigating complaints from a user about vulgar and obscene comments on the website. However, the website's editors believed they were being pressured for their controversial reporting, including investigations on key politicians abusing their powers.[44] With support from media NGOs and activists, the publication asked the Ministry of Interior and prosecutor general to explain the legal grounds for disclosing the requested information, after which the demands were dropped.

There is no obligatory user registration that supplies data to the authorities for either internet users or mobile phone subscribers. Nevertheless, it is unclear how pervasive or widespread extralegal surveillance of Ukrainians users' activities online really is at present. From 2002 to 2006, mechanisms for internet monitoring were in place under the State Committee on Communications' Order No. 122, which required ISPs to install so-called "black-box" monitoring systems that would provide access to state institutions. This was mainly done to monitor the unsanctioned transmission of state secrets. Caving to the pressure of public protests and complaints raised by the Internet Association of Ukraine and the Ukrainian Helsinki Human Rights Union, the Ministry of Justice abolished this order in August 2006. Since then, the Security Service has seemingly acted within the limits of the Law on Operative Investigative Activity and must obtain a court order to carry out surveillance.[45] Nevertheless, some human rights groups believe that the Security Service is still keeping intercepted messages and carrying out internet surveillance on a large scale.[46]

Physical attacks against online journalists and activists have not been recorded, but there have been periodic instances of intimidation against users for their online activities. For example, internet entrepreneur Denis Oleynyk had his online printing business closed down and equipment confiscated by law enforcement in September 2011 over allegations of copyright violations.[47] Oleynyk denied the copyright infringement claims and believes he

[43] "Януковича проклял сам блог" [Yanukovich Cursed by The Blog], Glavred, August 2, 2010, http://glavred.info/archive/2010/08/02/102221-4.html.

[44] "Готовится "наезд" милиции на LB.ua (документ)" [Law Enforcement Prepares Attack On LB.ua (document)], Levy Bereg, December 1, 2011, http://lb.ua/news/2011/12/01/126411_gotovitsya_naezd_militsii_na_lbua.html.

[45] "Ukraine: Country Profile 2010," OpenNet Initiative.

[46] Kharkiv Human Rights Group, "Права людини в Україні - 2006. V. Право на приватність" [Human Rights in Ukraine in 2006. V. Privacy Rights], Human Rights in Ukraine, March 5, 2010, http://www.khpg.org/index.php?id=1186147137.

[47] Maksym Savanevsky, "Офіс компаній Prostoprint та futbolka.ua захопив УБОЗ (оновлено 23:15)" [Offices Of Prostoprint And futbolka.ua Taken Hostage By UBOZ (Unit on Figthing Organized Crime) (updated at 23:15)], Watcher,

and his business were being persecuted for using a controversial slogan that made fun of the president on their t-shirts. The slogan itself earlier became a YouTube hit after being recorded at a football match, and the video was repeatedly taken down from YouTube, only to reappear again and again.[48] Oleynyk eventually left the country out of fear for his and his family's wellbeing. He continues to run his company from Croatia and has reportedly applied for political asylum in Latvia.[49]

In another example on May 17, 2011, blogger Nikolay Sukhomlyn published a story on his Facebook page about the corrupt practices of then Donetsk governor Anatoly Blyznyuk, including a video of the governor riding in an S-class Mercedes said to be worth up to 700,000 UAH (over US$87,000). The news and video went viral, and the next day Sukhomlyn began receiving private messages telling him to take down the content and stop criticizing Ukrainian politicians. The next week he received an anonymous phone call telling him he would be "dealt with."[50] Then on June 1, 2011, Sukhomyln's Facebook profile was deleted by website administrators.[51]

Cyberattacks are not very common in Ukraine, and most of the few recent cases relate to users' discontent with the actions of authorities. On February 5, 2012, there were reports of the independent investigative journalism website *Ukrainska Pravda* being inaccessible due a distributed denial-of-service (DDoS) attack,[52] but the website itself did not confirm these reports and denied that the access issues were connected with hacker attacks.[53]

September 6, 2011, http://watcher.com.ua/2011/09/06/ofis-kompaniy-prostoprint-ta-futbolka-ua-zahopyv-uboz/.

[48] Maksym Savanevsky, "«Спасибо жителям Донбасса» став найпопулярнішим запитом в Google" ['Spasibo zhitelyam Donbassa' ('Thank You, Citizens of Donbass') Becomes Most Popular Search Request in Google], Watcher, August 16, 2011, http://watcher.com.ua/2011/08/16/spasybo-zhytelyam-donbassa-stav-naypopulyarnishym-zapytom-v-google/.

[49] "Создатель Prostoprint будет просить политического убежища в Латвии" [Prostoprint Founder To Apply For Political Asylum In Latvia], Internet.UA, September 27, 2011, http://www.internetua.com/sozdatel-Prostoprint-budet-prosit-politicseskogo-ubejisxa-v-latvii.

[50] "Профиль журналиста в Facebook заблокировали из-за машины Близнюка" [Journalist's Facebook profile blocked because of Blyznyuk's car], Focus, June 2, 2011, http://focus.ua/politics/187290/.

[51] When approached for explanations, the Russian Facebook office representative said that "…upon receipt of legitimate claims of violations of intellectual property rights, we will immediately remove or disable access to the risk of unauthorized materials."Open Letter To Mark Zuckerberg, UAINFO, June 8, 2011, http://uainfo.censor.net.ua/news/2917-otkrytoe-pismo-k-marku-cukerbergu.html.

[52] "Українську правду атакували хакери?" [Ukrainska Pravda attacked by hackers?], Реально, February 5, 2012, http://realno.te.ua/novyny/hot/українську-правду-атакували-хакери/; "В Україні хакери атакують опозиційні сайти" [In Ukraine hackers attack opposition sites], Prometey Information Agency, February 5, 2012, http://ia-prometei.org.ua/?p=9628.

[53] Ukrainska Pravda on Facebook, February 5, 2012, https://www.facebook.com/ukrpravda/posts/377158162298850.

UNITED KINGDOM

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	1	1
Limits on Content (0-35)	8	8
Violations of User Rights (0-40)	16	16
Total (0-100)	**25**	**25**

* 0=most free, 100=least free

POPULATION: 63 million
INTERNET PENETRATION 2011: 82 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

The United Kingdom was an early adopter of new information and communication technologies (ICTs). The University of London was one of the first international nodes of the ARPAnet, the world's introductory operational packet switching network that later came to compose the global internet, and the Queen sent her first ceremonial email in 1976. Academic institutions began connecting to the network in the mid-1980s. Internet service providers (ISPs) began appearing in the late 1980s, and more general commercial access was available by the early 1990s.

The United Kingdom has high levels of internet penetration, and online freedom of expression is generally respected. In the past year, however, substantial debate emerged about placing limits on social media sites such as Twitter and Facebook following the London riots in 2011, which prompted Prime Minister David Cameron and other officials to suggest that there should be a way of disabling these services when they are being used to promote violence. After an immediate public outcry, the government backed away from making any concrete proposals to this effect. The government has also taken proactive measures to combat copyright violations through the blocking of websites and penalties for alleged offenders. Moreover, public concern over surveillance has continued to grow, particularly after the Communications Capabilities Development Programme was reintroduced in May 2012, which if implemented would require ICT service providers to retain data on phone calls, emails, text messages and communications on social-networking

sites, in addition to expanding the real time surveillance capabilities of the security services in order to combat terrorism and organized crime.[1]

In a positive development, the government introduced a bill to revise the Defamation Act,[2] which would provide greater protections for ISPs, limit their liability for user-generated content, and place limits on "libel tourism." Additionally, new Protection of Freedoms Act of 2012 sets forth a requirement for local authorities to obtain a magistrate's approval for access to communications data, thereby placing limits on their surveillance powers.

OBSTACLES TO ACCESS

Access to internet in the United Kingdom is widespread, and there are few practical barriers, even in rural and disadvantaged areas. The share of homes with computers has increased from 52 percent in 2001 to 78 percent in 2011,[3] and internet penetration stood at 82 percent in 2011.[4] Broadband is almost universally available, with nearly 100 percent of all households capable of obtaining ADSL connections and 48 percent able to connect via cable. The government in December 2010 committed to ensuring "superfast" broadband of at least 24 Mbps for 90 percent of households by 2015.[5] The Broadband Delivery Programme is providing £830 million (US$1.32 billion) in funding for the project.

Those in the lowest income groups are significantly less likely to have home internet subscriptions, and the gap has remained the same for the past several years. The share of people over 65 with an internet subscription is significantly lower than that of all other age groups, but the gap has been narrowing rapidly.

Mobile telephone penetration is also universal, with a penetration rate of over 130 percent in 2011.[6] Second-generation (2G) networks are available in 99.9 percent of households while third-generation (3G) services are available in 98.9 percent. Mobile broadband is also increasing and is now used by 17 percent of all households, while 11 percent of households

[1] David Barrett, "Phone and email records to be stored in new spy plan," The Telegraph, February 18, 2012, http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html.
[2] See, Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), http://services.parliament.uk/bills/2012-13/defamation.html.
[3] Ofcom, *The Consumer Experience 2011: Research Report* (London: Ofcom, December 2011), http://stakeholders.ofcom.org.uk/binaries/research/consumer-experience/tce-11/research_report_of511a.pdf.
[4] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[5] Department for Innovation, Business and Skills (BIS), *Britain's Superfast Broadband Future*, December 2010. http://www.culture.gov.uk/images/publications/britainsSuperfastBroadbandFuture.pdf.
[6] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

use mobile broadband as their main internet connection. Prices for telecommunications access, including mobile telephony and broadband, have continued to decline. Between 2008 and 2011, the average cost of all mobile service packages declined 27 percent to under £9 pounds (US$14) per month for a basic package and £33 for (US$52) for an advanced package that includes internet.[7] The price of broadband declined 33 percent in the past five years to about 14 pounds (US$22) per month while increasing in speed from 1.6 Mbps to an average of 15.5 Mbps.[8]

The government does not place limits on the amount of bandwidth ISPs can supply, and the use of internet infrastructure is not subject to government control. ISPs regularly engage in traffic shaping or slowdowns of certain services, such as peer-to-peer (P2P) file sharing and television streaming, while mobile providers have cut back previously unlimited access packages for smart phones, reportedly because of concerns about network congestion. The Office of Communications (Ofcom), the country's telecommunications regulator, adopted a voluntary code of practice on broadband speeds in 2008, which it updated in 2010.[9] It held a consultation on the subject in 2010[10] and released a report in 2011 that called for a self-regulatory approach to network neutrality focusing on information disclosure rather than enforceable rules.[11] It described blocking of services and sites by ISPs as "highly undesirable" but said that market forces will address possible problems. In March 2011, the major ISPs pledged to a "Voluntary industry code of practice on traffic management transparency for broadband services,"[12] which will make the traffic management practices of various ISPs more transparent and accessible to consumers.

There was significant controversy about placing limits on social media sites such as Twitter and Facebook following the London riots in 2011. It was alleged that the sites were used to organize the disorder, prompting Prime Minister David Cameron and other public officials to suggest that there should be a way of preventing people from using these sites in similar situations.[13] The government, however, backed away from the statement after public and industry protests, and no specific steps were ever taken that would restrict use of social media.

---

[7] Ofcom, *The Consumer Experience 2011: Research Report*.
[8] Ibid.
[9] Ofcom, "2010 Voluntary Code of Practice: Broadband Speeds," July 27, 2010, http://stakeholders.ofcom.org.uk/telecoms/codes-of-practice/broadband-speeds-cop-2010/code-of-practice/.
[10] Ofcom, "Traffic Management and 'net neutrality,' A Discussion Document," June 24, 2010, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/.
[11] Ofcom, "Ofcom's approach to net neutrality," November 11, 2011, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/statement/.
[12] Broadband Stakeholder Group, "Broadband providers launch new traffic management transparency code," March 15, 2012, http://www.broadbanduk.org/content/view/479/7/.
[13] "PM statement on disorder in England," The official site of the British Prime Minister's Office, August 11, 2011, http://www.number10.gov.uk/news/pm-statement-on-disorder-in-england/; "England riots: Government mulls social media controls," BBC News, August 11, 2011. http://www.bbc.co.uk/news/technology-14493497.

Nominet, the main domain registrar in the United Kingdom, is currently consulting on a new policy regarding the suspension of web domains at the request of law enforcement bodies.[14] The registrar has already suspended thousands of domains without a court order after receiving complaints from the police and other bodies for alleged criminal violations.[15] Nominet is also being told that failure to remove the domains may result in them being found criminally liable. Under an appeals process, 12 orders have been appealed with three overturned. Civil rights groups and ISPs are demanding that court orders should be required under the new policy.[16]

The United Kingdom provides a competitive market for internet access, with approximately 700 ISPs in operation; however, 95 percent of users are served by five major companies. ISPs are not subject to licensing but must comply with the general conditions set by Ofcom, such as having a recognized code of practice and being a member of an alternative dispute-resolution scheme.[17] Ofcom's duties include regulating competition among communications industries, including telecommunications and wireless communications services. It is generally viewed as fair and independent in its oversight.

LIMITS ON CONTENT

There is no general law authorizing filtering or blocking of internet content. Nevertheless, there have been increasing demands in recent years to expand the blocking and filtering of content related to violations of intellectual property and sites that promote extremism and terrorism, as well as measures to strengthen parental controls and prevent children from viewing adult-oriented sites.

The Internet Watch Foundation (IWF), a British charity funded by ISPs and the European Union (EU), operates hotlines and investigates allegedly unlawful content related to child sexual abuse and criminally obscene materials.[18] Previously, it had also received reports on materials inciting racial hatred, but that has been moved to TrueVision, a new police-run

[14] "UK police may be given domain name-suspension powers," Out-Law.com, September 5, 2011. http://www.out-law.com/en/articles/2011/september/uk-police-may-be-given-domain-name-suspension-powers/; Nominet, "Dealing with domain names used in connection with criminal activity," accessed August 20, 2012, http://www.nominet.org.uk/policy/issuegroups/current/domainsassociatedwithcrime/.

[15] According to Open Rights Group, Nominet has said that the takedowns are for "counterfeit goods sites (83%), phishing (9.6%), drugs (6.3%) and fraud (0.8%)"; Jim Killock, "Domain seizures: it's good to talk," Open Rights Group (blog), May 20, 2011, http://www.theoneclickgroup.co.uk/news.php?id=6261.

[16] Jim Killock, "ISPA, LINX and ORG insist on Court Orders for domain suspensions," Open Rights Group (blog), November 23, 2011, http://www.openrightsgroup.org/blog/2011/ispa,-linx-and-org-insist-on-court-orders-for-domain-suspensions.

[17] Ofcom, "The General Authorisation Regime," accessed March 31, 2011, http://www.ofcom.org.uk/telecoms/ioi/g_a_regime/.

[18] The Internet Watch Foundation (IWF) website is located at http://www.iwf.org.uk/.

website.[19] The Internet Services Providers' Association (ISPA) adopted a code of practice in January 1999 under which ISPs voluntarily agree to follow the watch list provided by the IWF on which content to remove and block.[20] Additionally, laws such as the Protection of Children Act are used to prosecute individuals suspected of accessing or circulating child pornography.

The CleanFeed filtering system, developed by British Telecom and the IWF, blocks access to any images or websites listed in the IWF database. It is estimated that 98.9 percent of all UK traffic is filtered using CleanFeed or other, less-sophisticated filtering systems.[21] In 2009, the Home Office shelved plans to require all ISPs to implement the IWF blocking list,[22] but in 2010 it adopted rules that prohibit government bodies from procuring services from ISPs that do not use the list.[23] On several occasions, due to technical difficulties on the ISP level, blocking decisions designated to prevent access to harmful content also disabled users from temporarily accessing popular sites such Wikipedia.[24] Most recently, in 2011, the IWF identified for blocking a single URL at the popular cloud server site Fileserve, but due to technical problems, British Telecom and Virgin subscribers were prevented from using the entire service for several days.[25]

There has also been increased public debate about imposing measures that would more effectively prevent children from accessing adult-oriented material on the internet. In June 2011, the Department of Education sponsored a review, which recommended that ISPs provide an "active choice" to parents to limit children's access to adult materials.[26] The four largest ISPs announced in October 2011 that they were offering systems allowing users to filter "adult" materials at the ISP level and they issued a code of practice aimed at educating consumers about parental controls.[27] There has been considerable public discussion, including parliamentary meetings, over whether the system should be turned on by default, requiring users to request the ability to access adult materials, but the government has declined to endorse that policy. Instead, the government launched the ParentPort website in

[19] Homepage: http://www.report-it.org.uk/home. See, IWF, "Incitement to racial hatred removed from IWF's remit," April 11, 2011, http://www.iwf.org.uk/about-iwf/news/post/302-incitement-to-racial-hatred-removed-from-iwfs-remit.
[20] Internet Services Providers' Association, "ISPA Code of Practice," accessed August 20, 2012, http://www.ispa.org.uk/about-us/ispa-code-of-practice/.
[21] Chris Williams, "Home Office Backs Down on Net Censorship Laws," The Register, October 16, 2009, http://www.theregister.co.uk/2009/10/16/home_office_iwf_legislation/.
[22] Ibid.
[23] Ben Leach, "Ban for internet providers failing to block child sex sites," The Daily Telegraph, March 10, 2010. http://www.telegraph.co.uk/technology/facebook/7411020/Ban-for-internet-providers-failing-to-block-child-sex-sites.html.
[24] "Wikipedia Child Image Censored," BBC News, December 8, 2008, http://news.bbc.co.uk/2/hi/uk_news/7770456.stm.
[25] "UK ISP Block of Fileserve Site Blamed on Internet Watch Foundation Filter," ISPreview, November 19, 2011.
[26] "Update on the implementation of 'Letting Children be Children,'" Department for Education, April 26, 2012, http://www.education.gov.uk/childrenandyoungpeople/healthandwellbeing/b0074315/bailey-review.
[27] "Code of Practice on Parental Controls—BT, TalkTalk, Virgin Media and Sky," Virgin Media, October 28, 2011, http://mediacentre.virginmedia.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=1245.

October 2011 to receive complaints about materials "unsuitable for children" across all forms of media.[28]

The government has also taken a proactive approach in limiting access to websites that have been found in violation of copyright protections. There have been a number of cases where courts have ordered websites, such as Newzbin and the Pirate Bay, to be blocked for copyright infringement[29] and to have their domain names seized[30] based on the Copyright Act and other laws. The High Court has ordered the ISPs to use the CleanFeed system to block the URLs to the sites. The Department for Culture, Media and Sport (DCMS) has also been meeting with ISPs and rights holders to develop a code of practice for a "rapid judicial procedure" to block "substantially infringing websites."[31]

In addition, the government has increased its efforts to limit access to "extremist" materials on the internet.[32] The Terrorism Act of 2006 allows for the takedown of terrorist material hosted in the United Kingdom if it "glorifies or praises" terrorism, is information that could be useful to terrorism, or urges people to commit or help with terrorism.[33] ISPs reportedly take down material voluntarily when contacted by the authorities, though there are no statistics available on the practice and it appears to be unregulated and informal.[34] A new Counter Terrorism Internet Referral Unit (CTIRU) was set up in 2010 to investigate internet materials, and as of 2011, the unit reported that it had successfully taken down material in 156 cases.[35] The government released a revised Prevent Anti-Terrorism Strategy in 2011, which calls for blocking access to "extremist" materials in schools and public libraries and more efforts to remove "harmful content" from the internet.[36] The report also states that commercial filtering companies have agreed to include terrorist-related materials in their filtering systems.

[28] Homepage: http://www.parentport.org.uk/.
[29] Twentieth Century Fox Film Corporation and others v. British Telecommunications plc [2011] EWHC 2714 Ch (October 26, 2011).
[30] Matt Warman, "Serious Organised Crime Agency closes down rnbxclusive.com filesharing website," The Telegraph, February 15, 2012, http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html.
[31] "FOI request reveals plans for 'rapid procedure' on web blocking," Out-Law.com, November 17, 2011, http://www.out-law.com/en/articles/2011/november/foi-request-reveals-plans-for-rapid-procedure-on-web-blocking/.
[32] See, Home Affairs Committee, "MPs urge internet providers to tackle on-line extremism," February 6, 2012. http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/news/120206-rvr-rpt-publication/.
[33] Terrorism Act 2006 (c. 11), §3, available at Office of Public Sector Information, http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en_1; See, "Reporting extremism and terrorism online," DirectGov, http://www.direct.gov.uk/en/CrimeJusticeandtheLaw/CounterTerrorism/DG_183993.
[34] Chris Williams, "Terrorism Chiefs Don't Know What They've Censored Online," The Register, November 12, 2009, http://www.theregister.co.uk/2009/11/12/west_terror/.
[35] Home Office, "Prevent Strategy," June 2011, http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy/prevent-strategy-review?view=Binary.
[36] Ibid

Users in the United Kingdom continue to enjoy wide access to free or low-cost blogging services, allowing them to express their views on the internet. Users and nongovernmental organizations also employ various forms of online communication to organize political activities, protests, and campaigns. Civil society organizations maintain a significant presence online and have used internet platforms to promote various causes. For example, the group, 38 Degrees, has over one million members who use social media to campaign successfully on issues, such as saving national forests from being sold off.[37] However, as noted above, there have been discussions about whether it is appropriate to limit access to social media if necessary to prevent violence. The Attorney General also said in June 2011 that social media users who violate court injunctions, such as those that aim to prevent the publication of information about pending court cases in which one of the parties is not named, could face criminal charges for contempt of court.[38]

VIOLATIONS OF USER RIGHTS

The United Kingdom has no written constitution or comprehensive bill of rights. The European Convention on Human Rights is incorporated into UK law through the Human Rights Act of 1998, and British courts have increasingly recognized freedom of expression and other human rights.

The intersection of intellectual property and freedom of expression is currently one of the most hotly debated issues. After much controversy, the Digital Economy Act (DEA) was adopted in April 2010,[39] giving the government the power to impose rules requiring ISPs to monitor their users and take "technical measures" against users who are reported (but not proven in a court or independent hearing) to be infringing copyright. These measures include limiting access speeds and cutting off access altogether. The ISPs, British Telecom and TalkTalk, together with free expression and consumer groups filed a legal challenge of the law in 2010.[40] However, the High Court rejected most of the challenge in April 2011 with only a cursory regard to freedom of expression,[41] and the decision was upheld by the

[37] See, "Victory! Government to scrap plans to sell our forests," 38 Degrees (blog), February 17, 2011, http://blog.38degrees.org.uk/2011/02/17/victory-government-to-scrap-plans-to-sell-our-forests/.
[38] Tara Conlan, "Twitter users who breach injunctions risk legal action, warns attorney general," Guardian, June 7, 2011, http://www.guardian.co.uk/media/2011/jun/07/twitter-users-injunctions-legal-action.
[39] The Digital Economy Act 2010 (c. 24), available at Office of Public Sector Information, accessed August 20, 2012, http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1.
[40] "ISPs Take Digital Economy Act to the Courts," Out-Law.com, July 8, 2010, http://www.out-law.com/default.aspx?page=11211; "Skeleton Argument on Behalf of Consumer Focus and ARTICLE 19," ARTICLE 19, March 10, 2011. http://www.article19.org/data/files/pdfs/submissions/skeleton-argument-on-behalf-of-consumer-focus-and-article-19.pdf.
[41] British Telecommunications Plc & Anor, R (on the application of) v. The Secretary of State for Business, Innovation and Skills [2011] EWHC 1021 (Admin) (April 20, 2011); Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012]

Court of Appeal in March 2012.[42] The DEA also stipulates that websites found to have or likely to have "substantial" violations of copyright can be blocked by a court order.

Ofcom is currently working on an Obligations Code—which will specify when and how ISPs will issue warning notices to their customers who are thought to be illegally accessing copyright-protected material—to implement the law. The present draft allows customers to challenge any such allegation, but they will have to pay a £20 ($US 32) fee for each appeal. In an interesting development, the High Court in March 2012 ruled that the use of internet protocol (IP) addresses was an unreliable way of identifying violators. The ruling also described as "objectionable" the letters that the company was planning to send to people accused of intellectual property violations, which had included threats to cut off service and demands for excessive payments.[43]

A new initiative to revise the Communications Act of 2003 is expected to be announced in late 2012, which will likely result in substantial changes to the provisions that were adopted through the DEA. The government also initiated a review of intellectual property law in 2011, releasing a report which recommended significant changes to the law, including an explicit exemption for parody, which only partially exists in case law now.[44] The government is currently holding a consultation to implement some of the recommendations of the review.

The threat of libel suits continues to have a significant chilling effect on both content producers and ISPs. English libel law is expansive in its restrictions on allegedly libelous material and places a heavy financial and evidentiary burden on defendants.[45] The United Kingdom has implemented the EU 2002 E-Commerce Directive, which states that hosts can be held liable if they are found to have had knowledge of illicit material, including defamatory content, but failed to remove it.[46] This often results in hosting companies

EWHC 268 (Ch) (20 February 2012); Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012] EWHC 1152 (Ch) (02 May 2012).

[42] British Telecommunications Plc, R (on the application of) v. BPI (British Recorded Music Industry) Ltd & Ors [2012] EWCA Civ 232 (March 06, 2012).

[43] Golden Eye (International) Ltd & Anor v Telefonica UK Ltd [2012] EWHC 723 (Ch) (March 26, 2012); "O2 disclosure ruling could impact on workings of imminent new anti-piracy code, campaigners say," Out-Law.com, March 29, 2012, http://www.out-law.com/en/articles/2012/march1/o2-disclosure-ruling-could-impact-on-workings-of-imminent-new-anti-piracy-code-campaigners-say/.

[44] Intellectual Property Office, "Digital Opportunity: A review of Intellectual Property and Growth," May 2011, http://www.ipo.gov.uk/ipreview; See also, "Parody, pastiche & caricature Enabling social and commercial innovation in UK copyright law," Consumer Focus, July 2011, http://www.consumerfocus.org.uk/files/2011/07/Consumer-Focus-Parody-briefing.pdf.

[45] Section 1, Defamation Act 1996; see Jo Glanville and Jonathan Heawood, eds., *Free Speech Is Not for Sale: The Impact of English Libel Law on Freedom of Expression* (London: Index on Censorship/English PEN, 2009), http://libelreform.org/our-report#.

[46] Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013). See, *Metropolitan International Schools Ltd v. (1) Designtechnica Corporation (2) Google UK Ltd &(3) Google Inc* [2009] EWHC 1765 (QB) (search engine not liable for excerpts); *Bunt v. Tilly* [2006] EWHC 407 (QB) (ISP not liable if just provides connection); *Twentieth Century Fox Film Corporation v. Newzbin*

quickly taking down material when asked, with little inquiry as to the legality of the demand. There is also concern over "libel tourism," a practice in which foreign litigants with little or no connection to the country exploit the ubiquity of online content to invoke plaintiff-friendly English libel laws against their critics.[47] Recently, the High Court has narrowed the application of the law, in one case ruling that Google does not qualify as a publisher for its blog-hosting service, even though it has received notification of allegedly infringing materials.[48] Moreover, there has been an increased use of libel law for offending Twitter posts, some resulting in substantial damages.[49]

In 2011, the government introduced a bill to revise the Defamation Act,[50] which will provide greater protections for ISPs by limiting their liability for user-generated content and also restrict libel tourism. However, it might also require authors of anonymous posts to identify themselves for the ISPs to be protected.[51] The bill is expected to be enacted in late 2012 or 2013.

In addition to questions surrounding intellectual property enforcement, the government has taken strong measures against users who post or download information perceived as a security treat. For example, two students, one of whom was taking a course on terrorism, were detained in 2008 under the Terrorism Act of 2000 for downloading material deemed to be terrorist in nature.

General laws such as the Public Order Act and the 2003 Communications Act are increasingly being used to charge individuals with crimes for posting threatening or harassing materials on the internet. For example, a man was convicted in 2010 under the Communications Act for using Twitter to express dismay at the closing of the local airport, jokingly writing that he would blow up the airport if it did not reopen within a week.[52] The High Court overruled his conviction in July 2012, finding that the statement did not

[2010] EWHC 608 (Ch) (company that provides indexing of copyrighted files liable); *Kaschke v. Gray & Anor* [2010] EWHC 690 (QB) (host that moderates user comments liable). See also Electronic Commerce Directive (Hatred against Persons on Religious Grounds or the Grounds of Sexual Orientation) Regulations.

[47] "Libel Tourism: Writ Large," The Economist, January 8, 2009, http://www.economist.com/world/international/displaystory.cfm?story_id=12903058.

[48] Tamiz v Google Inc [2012] EWHC 449 (QB).

[49] Cairns v Modi [2012] EWHC 756 (QB) (March 26, 2012); See also, Gervase de Wilde, "Case Law: Cairns v Modi – Defendant found liable for Twitter comments," Inforrm Blog, March 28, 2012, http://inforrm.wordpress.com/2012/03/28/case-law-cairns-v-modi-defendant-found-liable-for-twitter-comments-gervase-de-wilde/.

[50] See, Parliamentary Joint Select Committee on Draft Defamation Bill, Defamation Bill 2012-13 (HC Bill 51), http://services.parliament.uk/bills/2012-13/defamation.html.

[51] See, Ministry of Justice, "The Government's Response to the Report of the Joint Committee on the Draft Defamation Bill," February 2012, 77-88, http://www.justice.gov.uk/downloads/publications/policy/moj/government-response-draft-defamation-bill.pdf.

[52] David Allen Green, "Paul Chambers: A Disgraceful and Illiberal Judgment," Jack of Kent (blog), May 11, 2010, http://jackofkent.blogspot.com/2010/05/paul-chambers-disgraceful-and-illiberal.html.

represent a credible threat.[53] There have also been a series of arrests of individuals in the past year for the posting of allegedly racist materials,[54] including a man sentenced to 56 days in prison in March 2012 for posting racially-biased statements on Twitter about a footballer who had fallen gravely ill on the field.[55]

There is continued concern about surveillance as authorities have increasingly used or misused the powers granted under the Regulation of Investigatory Powers Act (RIPA).[56] The law covers the interception of communications; the acquisition of communications data, including billing data; intrusive surveillance, such as on residential premises or in private vehicles; covert surveillance in the course of specific operations; the use of covert human intelligence sources like agents, informants, and undercover officers; and access to encrypted data. It requires that communications providers maintain interception capabilities, including systems to record internet traffic on a large scale.

RIPA allows national government agencies and over 400 local bodies to access communication records for a variety of reasons, from national security to tax collection. Orders for interception and access to the content of communications require approval from the home secretary or another secretary of state. In 2011, there were 494,078 requests for communications data from telephone companies (including mobile phone service providers) and ISPs—a decrease of 11 percent from the previous year.[57] According to the Interception Commissioner, there were nearly 900 instances where records were incorrectly obtained by authorities and two persons were incorrectly detained based on mistakes in the communications data.[58]

The Protection of Freedoms Act, a major promise of the government, was formally approved on May 1 2012. The act sets up new rules in a variety of areas including retention of DNA, fingerprints of school children, and surveillance cameras. On cyber-related issues, it amends RIPA to require a magistrate's approval for access to communications data by local authorities, thereby limiting their surveillance powers.[59]

---

[53] Chambers v Director of Public Prosecutions [2012] EWHC 2157 (QB), July 27, 2012.
[54] See, Martin Wainwright, "Man who racially abused Stan Collymore on Twitter spared prison," Guardian, March 21, 2012, http://www.guardian.co.uk/technology/2012/mar/21/man-racially-abused-collymore-twitter-spared-prison; "Teenagers given final warnings over racist tweets aimed at Sammy Ameobi," Guardian, February 7, 2012, http://www.guardian.co.uk/football/2012/feb/07/teenagers-warning-racist-tweets-sammy-ameobi.
[55] Steven Morris, "Student jailed for racist Fabrice Muamba tweets," Guardian, March 27, 2012. http://www.guardian.co.uk/uk/2012/mar/27/student-jailed-fabrice-muamba-tweets.
[56] See generally, the Explanatory Notes to Regulation of Investigatory Powers Act, accessed January 2009, http://www.opsi.gov.uk/acts/acts2000/en/ukpgaen_20000023_en_1.
[57] Rt Hon Sir Paul Kennedy, "2011 Annual Report of the Interception of Communications Commissioner," House of Commons, June 13, 2012, http://www.intelligencecommissioners.com/docs/0496.pdf.
[58] "Snooping errors twice led to wrongful detention, watchdog reveals," Guardian, July 13, 2012.
[59] Protection of Freedoms Bill (HL Bill 99), http://www.publications.parliament.uk/pa/bills/lbill/2010-2012/0099/lbill_2010-20120099_en_1.htm.

In 2009, regulations to implement the EU Data Retention Directive were adopted.[60] Under the directive, providers must retain communications data on all users for 12 months, including mobile phone location and email logs. ISPs also continue to "voluntarily" store web-access logs, and government agencies access this information through the procedures in RIPA. In May 2012, the government announced the Communications Capabilities Development Programme (CCDP), a proposal that if implemented would require ICT service providers to retain data on phone calls, emails, text messages, and communications on social-networking sites in order to combat terrorism and organized crime.[61] The CCDP would also expand the real time surveillance capabilities of the security services and require ISPs to monitor users.[62] Under the previous government, the program was hotly debated in 2009 but failed to move forward as a bill.[63]

There are no public restrictions on the use of encryption technologies. However, under Part 3 of RIPA, it is a crime not to disclose an encryption key upon an order from a senior policeman or a High Court judge. The Court of Appeal ruled in 2008 that self-incrimination protections do not apply.[64] There has been increasing use of the provision to obtain court orders to force disclosure of keys. Between April 2011 and March 2012, there were 33 court orders for decryption, 14 people charged with refusing to disclose their keys, and two convictions for refusal to disclose.[65]

There have been numerous cyber-hacking incidents in the UK in the previous year. Apart from intrusions for fraud and other criminal purposes, activist hacking groups have targeted police websites,[66] government bodies, and newspapers.[67] In addition, police have launched two major investigations as a spin off of the phone hacking investigation—Operation Tuleta

[60] The Data Retention (EC Directive) Regulations 2009 (SI 2009 No. 859), April 2, 2009.
[61] David Barrett, "Phone and email records to be stored in new spy plan," The Telegraph, February 18, 2012, http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html.
[62] "Queen's Speech: Communications Data Bill", SCL, May 9, 2012; See also, Robert Booth, "Government plans increased email and social network surveillance," The Guardian, April 1, 2012. http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance.
[63] London School of Economics Policy Engagement Network, *Briefing on the Interception Modernisation Programme* (London: London School of Economics and Political Science, June 2009), http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf.
[64] S & Anor, R v [2008] EWCA Crim 2177 (October 09, 2008).
[65] Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012* (London: Stationary Office, July 2012), http://www.official-documents.gov.uk/document/hc1213/hc04/0498/0498.pdf; Chris Williams, "UK Jails Schizophrenic for Refusal to Decrypt Files," The Register, November 24, 2009, http://www.theregister.co.uk/2009/11/24/ripa_jfl/.
[66] "Soca website taken down after LulzSec 'DDoS attack,'" BBC News, June 20, 2011; "Attack takes Soca crime agency website down," BBC News, May 3, 2012.
[67] "Hacked Sun site greatly exaggerates Murdoch's death," The Register, July 18, 2011.

and Operation Kalmyk—into whether News International illegally hacked the emails of various persons,[68] resulting in a number of arrests.

[68] "Leveson Inquiry: Police reveal 'likely' victim numbers," BBC News, February 6, 2012, http://www.bbc.co.uk/news/uk-16905465.

UNITED STATES OF AMERICA

	2011	2012
INTERNET FREEDOM STATUS	**Free**	**Free**
Obstacles to Access (0-25)	4	4
Limits on Content (0-35)	2	1
Violations of User Rights (0-40)	7	7
Total (0-100)	**13**	**12**

* 0=most free, 100=least free

POPULATION: 314 million
INTERNET PENETRATION 2011: 78 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Access to the internet in the United States remains relatively free compared with the rest of the world. Users face few restrictions on their ability to access and publish content online. The courts have consistently held that federal and state constitutional prohibitions against government regulation of speech apply to material published on the internet. The law also protects online service providers from liability for infractions committed by their users, a policy that fosters business models that permit open discourse and the free exchange of information.

Several developments in recent years, however, have placed the government and internet freedom advocates at odds over aspects of internet regulation as well as issues surrounding online surveillance and privacy. The United States lags behind many major industrialized countries in terms of broadband penetration, and network operators have challenged recent rules concerning network neutrality. The current administration appears committed to maintaining broad surveillance powers with the aim of combating terrorism, child pornography, and other criminal activity. Moreover, reports have emerged that the Federal Bureau of Investigation (FBI) is seeking expanded authority to control the design of internet services to ensure that communications can be intercepted when necessary.[1]

In early 2012, digital rights advocates, citizens, and several technology companies enacted an internet "blackout" to voice their opposition to two Congressional bills—the Stop Online

[1] Charlie Savage, "U.S. Tries to Make it Easier to Wiretap the Internet," New York Times, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1.

Piracy Act (SOPA) and PROTECT IP Act (PIPA)—that aimed to combat piracy on non-U.S. websites hosting material allegedly infringing on U.S. copyrights. Both laws would have allowed the Attorney General to order that internet service providers (ISPs) block any website containing infringing content. Both bills were withdrawn in response to public outcry. In another recent trend, social networks and microblogging sites have become more prominent targets for government monitoring of citizen activities. The microblogging site Twitter has received multiple subpoenas requesting the personal data of users, including individuals affiliated with the anti-secrecy organization WikiLeaks and the Occupy Wall Street movement. Twitter has challenged both of these requests in court.

OBSTACLES TO ACCESS

Access to the internet in the United States is largely unregulated. It is provided and controlled in practice by a small group of private cable television and telephone companies that own and manage the network infrastructure. This model has come into question in recent years: observers have warned that insufficient competition in the ISP market could lead to increases in the cost of access, thus adversely affecting the economy and individuals' participation in civic life, which increasingly occurs online.[2] Observers have cautioned that if recent "network neutrality" regulations (discussed in greater detail below) prove too weak or are rejected by Congress or the courts, the dominant companies may decide not to continue to carry internet traffic in a content-neutral fashion.

Although the United States is one of the most connected countries in the world, it has fallen behind many other developed countries in terms of internet speed, cost, and broadband availability.[3] In 2011, approximately 78 percent of all Americans had access to the internet,[4] but only 66 percent of adults used high-speed broadband connections.[5] While the broadband penetration rate is considered high by global standards, it puts the United States significantly behind countries such as Japan, South Korea, Norway, and Sweden. Lack of high-speed internet access is especially prevalent in rural areas, where low population densities make it

[2] Mark Cooper, "The Socio-Economics of Digital Exclusion in America, 2010," paper presented at 2010 TPRC: 38th Research Conference on Communications, Information, and Internet Policy, Arlington, Virginia, October 1–3, 2010.

[3] According to a study by the Organization for Economic Cooperation and Development (OECD), as of June 2011 the United States was ranked 7th among the OECD member countries in terms of mobile wireless broadband subscriptions per 100 inhabitants, and was ranked even lower, at 15th, on fixed-line broadband penetration. See, OECD Broadband Statistics, "OECD Fixed (Wired) Broadband Subscriptions per 100 Inhabitants, by Technology, June 2011," and "OECD Terrestrial Mobile Wireless Broadband Subscriptions per 100 Inhabitants, by Technology, June 2011," accessed January 24, 2012, http://www.oecd.org/dataoecd/21/35/39574709.xls.

[4] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[5] "Internet Use and Home Broadband Connections," Pew Internet & American Life Project, July 24, 2012. http://pewinternet.org/Infographics/2012/Internet-Use-and-Home-Broadband-Connections.aspx.

difficult for private companies to justify large investments in network infrastructure. Broadband service is not yet available to 5 to 10 percent of U.S. residents, most of who live in rural counties.[6] A June 2011 Federal Communications Commission (FCC) report to Congress indicated that 28 percent of rural residents in the United States lack access to fixed broadband.[7]

African-Americans, residents of rural areas, and those earning less than US$30,000 annually are the groups least likely to have access to the internet, though internet penetration has been growing at significantly higher rates among African-Americans than it has within the general population. In a survey conducted by the Pew Internet and American Life Project, when asked why they do not use the internet, many nonusers said they did not see the internet's relevance in their lives. They also cited factors such as availability, usability, and price as key deterrents. About 61 percent of nonusers said they would need assistance in order to use the internet.[8]

Mobile telephones have become ubiquitous in the United States with a penetration rate of roughly 106 percent in 2011.[9] As of mid-2011, about 44 percent of mobile phone users reported accessing the internet on their phones, and roughly half of those users accessed the internet on a daily basis.[10] A growing number of people use their phones to check email, visit social-networking sites such as Facebook, and engage in online commerce. This has prompted many companies to develop special applications and versions of their websites that are designed for mobile phone viewing.

No single agency governs the internet in the United States. The FCC, an independent agency of the executive branch, is charged with regulating radio and television broadcasting, all interstate communications, and all international telecommunications that originate or terminate in the United States. Although the FCC is not specifically tasked with regulating the internet or ISPs, it has claimed jurisdiction over some internet-related issues, such as the recent rules on network neutrality. Other government agencies, such as the National Telecommunications and Information Administration (NTIA), also play advisory or executive roles with respect to telecommunications, economic, and technological policies and regulations. It is the role of the U.S. Congress to create laws that govern the internet

[6] Amy Schatz, "Want Broadband? New Maps Show Options," Digits blog, Wall Street Journal, February 17, 2011, http://blogs.wsj.com/digits/2011/02/17/want-broadband-new-map-shows-options/.
[7] Sharon Gillett, "Progress Made on the Road To Bring Broadband to Rural Areas, but Many Miles To Go," Official FCC Blog, June 22, 2011, http://www.fcc.gov/blog/progress-made-road-bring-broadband-rural-areas-many-miles-go.
[8] Aaron Smith, "Home Broadband 2010," Pew Internet and American Life Project, August 11, 2010, http://www.pewinternet.org/Reports/2010/Home-Broadband-2010/Summary-of-Findings.aspx.
[9] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[10] Aaron Smith, "Americans and their Cell Phones," Pew Internet and American Life Project, April 15, 2011, http://pewinternet.org/Reports/2011/Cell-Phones.aspx.

and delegate regulatory authority. Government agencies such as the FCC and the NTIA must act within the bounds of Congressional legislation.

Recognizing that internet penetration and connection speeds in the United States have been outpaced by those in several other developed countries, Congress has devoted funding to improving the nation's broadband infrastructure and has instructed the FCC to create a National Broadband Plan that will promote broadband availability for all U.S. residents. Lawmakers required that this plan include a detailed strategy for reducing costs to consumers and maximizing the use of broadband to enhance health care delivery, energy efficiency, economic growth, education, and other public goods.[11] After issuing a notice of inquiry in April 2009 and weighing input from a wide variety of business, government, and civil society organizations,[12] the FCC issued its National Broadband Plan in March 2010. First among the goals is to provide at least 100 million U.S. homes with "affordable access to actual download speeds of at least 100 megabits per second and actual upload speeds of at least 50 megabits per second."[13] As part of the initiative, the government has started providing subsidies to ISPs that offer satellite-based internet access in rural areas.[14] In 2009, the NTIA announced its Broadband Technology Opportunity Program, which has initiated a range of state-level partnerships with private and non-profit institutions that aim to increase broadband adoption among low-income families by offering low-cost equipment, broadband service, and digital education.[15] There are several other public-private and private-non-profit initiatives underway with similar aims.[16]

Despite the recent economic recession, the United States is home to a thriving communications start-up community where innovators and entrepreneurs regularly offer new technological tools at no monetary cost to the public. Popular web applications like Twitter, the video-sharing site YouTube, the social-networking site Facebook, and international blog-hosting services such as WordPress are all freely available.

Between 3,000 and 4,000 ISPs currently operate in the United States, although 15 of them control approximately 80 percent of the market, and four—AT&T, Comcast, Time Warner, and Verizon—control approximately the top 50 percent and own the majority of

[11] American Recovery and Reinvestment Act of 2009, H.R. 1, 111th Cong. (2009).
[12] Stephanie Condon and Marguerite Reardon, "FCC Seeks Input on National Broadband Plan," CNet News, April 8, 2009, http://news.cnet.com/8301-13578_3-10214974-38.html.
[13] "National Broadband Plan: Connecting America," Federal Communications Commission (FCC), 2010, http://www.broadband.gov/download-plan/.
[14] Rural Utilities Service Broadband Initiatives Program, "Round Two Application Directory: Satellite, Technical Assistance, and Rural Library Broadband Grant Applications," U.S. Department of Agriculture, August 30, 2010, http://www.broadbandusa.gov/BIPportal/files/BIP_Sat_TA_RLB_App_Directory.pdf.
[15] "About: Broadband Technology Opportunities Program," NTIA, http://www2.ntia.doc.gov/about.
[16] See, e.g., http://connect2compete.org.

network cables and other infrastructure.[17] Until 2005, those companies were required to grant "nondiscriminatory" access to their wire networks to other ISPs to ensure open retail-level competition and optimal service for consumers. However, in 2005, the FCC embraced an aggressive deregulation agenda and freed the network owners from the obligation to lease their lines to competing ISPs. The proponents of deregulation claimed that this step would provide more incentive for large cable and telephone companies to further develop and upgrade their networks, while opponents claimed that it would lead to higher prices, fewer options for consumers, and worse service. Broadband speeds have increased, but a majority of Americans remain limited to three or fewer options when choosing a broadband provider.[18]

Over the last decade, policymakers in the United States have engaged in deep debates over the concept of "network neutrality," according to which network providers must treat all content, websites, and platforms equally when managing data traffic.[19] Supporters of the principle argue that without it, ISPs would be able to block certain content and applications, or give preferential treatment to some content providers for a fee, a practice that could place limitations on citizen access to information and online services.

Although concerns about net neutrality began emerging in the early 2000s, the issue did not gain widespread attention until 2007 when investigators found that Comcast, a cable-television company and major ISP, had begun slowing down and blocking certain types of peer-to-peer file-sharing traffic.[20] Comcast claimed that it was forced to do this because high-volume users were clogging its network by repeatedly sharing large files. Yet its blocks were inconsistent and seemingly deceptive: for example, while engaged in peer-to-peer file sharing, a user would receive a message instructing him to stop the communication. The message was designed to look as if it had come from the computer of the user's peer, when in fact Comcast had issued the message. A number of public-interest groups and academics requested that the FCC declare such blocking to be a violation of the agency's internet policy principles.[21] The FCC agreed, and Comcast appealed to the federal courts.[22] In April 2010, a federal appeals court sided with Comcast and overturned the FCC's ruling against the company. The decision, which came shortly after the release of the National Broadband

[17] "ISP Usage and Market Share: ISP Trends, Stats and Analysis," StatOwl.com, January 2012, http://www.statowl.com/network_isp_market_share.php.
[18] Federal Communications Commission (FCC), "Internet Access Services: Status as of December 31, 2010," http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-310261A1.pdf.
[19] Tim Wu, "Network Neutrality FAQ," Timwu.org, accessed August 17, 2011, http://timwu.org/network_neutrality.html.
[20] Peter Svensson, "Comcast Blocks Some Internet Traffic," MSNBC, October 19, 2007, http://www.msnbc.msn.com/id/21376597/ns/technology_and_science-internet/.
[21] "Comcast Complaint," Public Knowledge, accessed March 4, 2011, http://www.publicknowledge.org/issues/comcastcomplaint.
[22] FCC, "Commission Orders Comcast to End Discriminatory Network Management Practices," news release, August 1, 2008, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf.

Plan, also found that the FCC did not have the authority to regulate ISPs under the legal framework the agency had cited, challenging its ability to protect consumers on the internet.[23]

In December 2010, the FCC issued a compromise ruling on net neutrality that instructs fixed-line service providers not to block access to, or unreasonably discriminate against, lawful websites, applications, or devices. The rules for wireless broadband providers are much more limited, however, restricting only some types of blocking and saying nothing about discrimination. Under separate FCC licensing rules covering the operation of a particular range of radio communication frequencies, some wireless carriers are barred from discriminating among devices and applications, but these rules are not universally applied.[24] Some advocates have accused one wireless carrier of violating the terms of these licenses, but the FCC has not yet addressed these complaints.[25]

Under the new regulations, ISPs remain allowed to offer tiered services at different prices.[26] FCC chairman Julius Genachowski claimed that the rules would protect "internet freedom and openness and promote robust innovation and investment."[27] Some civil society organizations expressed disappointment that the commission did not take a stronger stance on net neutrality that would have applied the Communications Act's "common carrier" provisions, though they agreed that the FCC operated in a free, fair, and independent manner.[28] The FCC's rules officially took effect in November 2011 and have been challenged in court. Challenges have come both from public interest groups who feel the rules do not go far enough by not fully extending to wireless networks,[29] and from ISPs that oppose the regulations.[30] The Washington D.C. Circuit Court of Appeals, the same appellate court that overturned the FCC's ruling in the Comcast case, will once again consider the FCC's authority to enact the rules, making the long-term status of the rules uncertain.

[23] Comcast Corporation v. Federal Communications Commission, No. 08-1291, U.S. Court of Appeals for the District of Columbia Circuit (April 6, 2010), http://www.cadc.uscourts.gov/internet/opinions.nsf/EA10373FA9C20DEA85257807005BD63F/$file/08-1291-1238302.pdf.

[24] U.S. Code of Federal Regulations, Title 47, sec. 27.16, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=82f1f40e3b6b119c316bbb90292bb254&rgn=div8&view=text&node=47:2.0.1.1.5.2.49.7&idno=47.

[25] FCC, Letter from Free Press to Marlene Dortch, August 3, 2011, http://fjallfoss.fcc.gov/ecfs/document/view?id=7021700316.

[26] "Report and Order: In the Matter of Preserving the Open Internet, Broadband Industry Practices," FCC 10-201, December 21, 2010, http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db1223/FCC-10-201A1.pdf.

[27] Sara Jerome, "Genachowski on Net-neutrality: 'I Reject Both Extremes,'" Hillicon Valley blog, The Hill, December 20, 2010, http://thehill.com/blogs/hillicon-valley/technology/134597-genachowski-on-net-neutrality-i-reject-both-extremes.

[28] "Network Neutrality," Public Knowledge, http://www.publicknowledge.org/issues/network-neutrality.

[29] Petition for Review, Free Press v. FCC, 11-1411, DC Circuit.

[30] Ibid.; Petition for Review, MetroPCS v. FCC, 11-1403, DC Circuit.

LIMITS ON CONTENT

Access to information on the internet is generally free from government interference. There is no government-run filtering mechanism affecting content passing over the internet or mobile phone networks. Users with opposing viewpoints engage in vibrant online political discourse and face almost no legal or technical restrictions on their expressive activities online.

Although the government does not restrict any political or social content, legal rules that apply to other spheres of life have increasingly been extended to the internet. For example, concerns over copyright violations, child pornography, protection of minors from harmful or indecent content, harassing or defamatory comments, publication of confidential information, gambling, and financial crime have presented a strong impetus for aggressive legislative and executive action.

Advertisement, production, distribution, and possession of child pornography—on the internet and in all other media—is prohibited under federal law and can carry a sentence of up to 30 years in prison. According to the Child Protection and Obscenity Enforcement Act of 1988, all producers of sexually explicit material must keep records proving that their models and actors are over 18 years old. In addition to prosecuting individual offenders, the Department of Justice, the Department of Homeland Security, and other law enforcement agencies have asserted their authority to seize the domain name of a website allegedly hosting child abuse images after obtaining a court order.[31]

Congress has passed several laws designed to restrict adult pornography and shield children from harmful or indecent content, such as the Child Online Protection Act of 1998 (COPA), but they have been overturned by courts due to their ambiguity and potential infringements on the First Amendment of the U.S. Constitution, which protects freedoms of speech and the press. One law currently in force is the Children's Internet Protection Act of 2000 (CIPA), which requires public libraries that receive certain federal government subsidies to install filtering software that prevents users from accessing "visual depictions that are obscene, child pornography, or harmful to minors." Libraries that do not receive the specified subsidies from the federal government are not obliged to comply with CIPA, and about one-third of public libraries in 2007 decided to forgo such financial support to avoid the filtering requirement.[32] Under the U.S. Supreme Court's interpretation of the law, adult users can request that the filtering be removed without having to provide a

[31] Treating domain names as property subject to criminal forfeiture, 18 U.S.C. 2253.

[32] Charles C. McClure and Paul T. Jaeger, *Public Libraries and Internet Service Roles: Measuring and Maximizing Internet Services* (Chicago: American Library Association, 2009), 42.

justification. However, not all libraries allow this option and the law has been challenged in recent years.[33]

Apart from universally illegal content such as child pornography, the government in recent years has started more aggressively pursuing alleged infringements of intellectual property rights on the internet. Since 2010, the Immigration and Customs Enforcement (ICE) division of the Department of Homeland Security has engaged in several rounds of domain-name seizures, with targets including blogs and file-sharing sites that allegedly link to illegal copies of music and films, and sites that sell counterfeit goods.[34] These seizures have been criticized as extreme and overly secretive; for example, ICE seized the domain name of a legitimate hip-hop music site in November of 2010 and refused to return it for an entire year. The decision to withhold the domain was based on sealed court proceedings to which the owners of the domain were not allowed access.[35]

In 2011, two bills that sought to target websites outside of the United States that hosted material allegedly infringing on U.S. copyrights, PIPA and SOPA, were introduced with bipartisan support in the Senate and House of Representatives, respectively. These bills were based on ideas proposed with Democratic and Republican support in the 2010 bill Combating Online Infringements and Counterfeits Act (COICA). They would have permitted the Attorney General to seek orders directing ISPs to block access to domain names of sites allegedly dedicated to infringing activity, among other things. The bills provided for only minimal judicial review (or a complete lack thereof) of sites allegedly engaged in copyright infringement; the bills also authorized the blocking of domain names for websites that contained infringing content among other lawful content.

Both of these bills, if passed, would have suppressed legitimate, unquestionably legal speech and would pose a threat to the infrastructure of the internet. In recognition of these concerns, technologists, digital rights advocates, companies such as Google and Mozilla, and the internet community at large voiced resounding opposition to the bills. In response to

[33] Bob Bocher, "Children's Internet Protection Act, CIPA: A Brief FAQ on Public Library Compliance," Wisconsin Department of Public Instruction, February 2004, updated March 11, 2010, http://dpi.state.wi.us/pld/cipafaqlite.html. The requirement that libraries disable filters upon patron request is being challenged by some librarians, who view the use of filters on library computers as a form of curation/collection development decision that would typically fall within a library's discretion. See, e.g., Bradburn v. North Central Regional Library District (Washington state Supreme Court found library right to enforce filtering, Bradburn v. NCLRD, No. 82200-0 (May 6, 2010); case pending review in federal court, Bradburn v. NCLR, NO. CV-06-327-EFS (E.D. Wash.)); Hunter v. City of Salem (E.D. Missouri). The American Library Association is firmly opposed to this idea and supports patrons' rights to access whatever legal material they wish.

[34] Corynne McSherry, "U.S. Government Seizes 82 Websites: A Glimpse at the Draconian Future of Copyright Enforcement?" Electronic Frontier Foundation, November 29, 2010, https://www.eff.org/deeplinks/2010/11/us-government-seizes-82-websites-draconian-future.

[35] Trevor Timm, "Blacklist Bills Ripe for Abuse Part II: Expansion of Government Powers," Deeplinks Blog, Electronic Frontier Foundation, December 9, 2011, https://www.eff.org/deeplinks/2011/12/blacklist-bills-ripe-abuse-part-ii-expansion-government-powers.

these and internal concerns, members of Congress withdrew the bills from consideration. The bills remained shelved as of mid-2012.

The activities of WikiLeaks, which in 2010 published several tranches of U.S. government material that was allegedly leaked by U.S. Army intelligence analyst Bradley Manning, triggered a serious debate about the use of the internet to publicize sensitive or classified government documents.[36] WikiLeaks has faced some actions by non-government entities that restricted its ability to operate. The site was removed from Amazon's data storage service, which claimed that WikiLeaks had violated its terms of service.[37] EveryDNS, Wikileaks' domain name service provider, terminated its service for WikiLeaks after suffering distributed denial-of-service (DDoS) attacks by opponents of the site.[38] While these and other companies that severed ties with WikiLeaks claimed to be acting independently and without government influence, their decisions came amid fierce public criticism of WikiLeaks by executive branch officials and prominent members of Congress.[39] As of August 2012, the U.S. government had not filed charges over the publication of the leaked documents by WikiLeaks or any of the press outlets that republished the documents.

The internet plays a significant role in civic activism in the United States, and the growth of the blogosphere and citizen journalism has changed the ways in which many people receive news. Blogs and electronic media outlets reporting from various points on the political spectrum now have greater readership than most printed periodicals. Nearly all nongovernmental organizations and causes have a presence on the internet and use it for advocacy and social mobilization. Email campaigns, online petitions, and YouTube videos have been instrumental in organizing protests, lobbying government bodies, and putting a spotlight on issues ranging from environmental degradation to hate crimes.[40] Most recently, significant online activism against SOPA and PIPA strongly influenced Congress to drop the proposed legislation in early 2012. Some estimates of user involvement in this effort include

[36] This information included video footage of a 2007 incident in which journalists and Iraqi civilians were killed by U.S. forces, documents on the wars in Afghanistan and Iraq, diplomatic cables from the U.S. State Department, and reports on prisoners held in Guantanamo Bay military prison, all of which number in the tens and (in the case of the Iraq war) hundreds of thousands.

[37] Geoffrey A. Fowler, "Amazon Says WikiLeaks Violated Terms of Service," Wall Street Journal, December 3, 2010, http://online.wsj.com/article/SB10001424052748703377504575651321402763304.html.

[38] Kevin Poulsen, "WikiLeaks Attacks Reveal Surprising, Avoidable Vulnerabilities," Wired, December 3, 2010, http://www.wired.com/threatlevel/2010/12/wikileaks-domain/.

[39] Ewen MacAskill, "WikiLeaks Website Pulled by Amazon After US Political Pressure," Guardian, December 2, 2010, http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon.

[40] See for example the Credo "Stop the Tar Sands Pipeline" petition at http://www.credoaction.com/campaign/keystone_obama/index2.html. See also: Steve Williams, "President Obama Signs Hate Crimes Bill—Thank You to the 25,000 Care2 Members That Helped It Reach His Desk!" Care2, October 28, 2009, http://www.care2.com/causes/civil-rights/blog/25-000-care2-members-help-secure-presidents-signature-on-hate-crimes-bill/.

over 10 million signatures to petitions, three million emails to legislators, and 115,000 sites blacking out or going dim in protest.[41]

The internet also has profoundly influenced political campaigning and fundraising. Until recently, most election campaigns relied on large donations from a limited pool of wealthy contributors. However, the success of current U.S. President Barack Obama's 2008 campaign, which was propelled by millions of small, online contributions, demonstrated the efficacy of the internet in mobilizing mass political support. President Obama's election team was able to raise over half a billion dollars in internet-based donations, with an average donation of about US$80.[42] In addition, the campaign's use of email, social-networking tools, and online videos was watched and eventually emulated by political operatives in the United States and around the world.

VIOLATIONS OF USER RIGHTS

The U.S. Constitution includes strong protections for free speech and freedom of the press. In 1997, the U.S. Supreme Court held that internet speech was entitled to the highest form of protection under the Constitution, and lower courts have consistently struck down attempts to regulate online content. Two federal laws also provide significant protections for online speech: Section 230 of the Communications Act of 1934 (as amended by the Telecommunications Act of 1996) provides immunity for ISPs and online platforms such as YouTube and Facebook that carry content created by third parties. The Digital Millennium Copyright Act (DMCA) provides a safe harbor to intermediaries that take down allegedly infringing material after notice from the copyright owner. These statutes enable companies to develop internet applications and websites without fear that they will be held liable for content posted by users.[43]

The U.S. government generally does not prosecute individuals for posting information on the internet, with the notable exceptions of child pornography and content that infringes copyright. As of mid-2012, it had taken no decisive action against either WikiLeaks or site founder Julian Assange, yet some suspect that federal officials may build a case alleging that WikiLeaks played a conspiratorial role in the unauthorized downloading of classified

[41] Fight for the Future, http://sopastrike.com/numbers/.
[42] Jose Antonio Vargas, "Obama Raised Half a Billion Online," 44 (blog), Washington Post, November 20, 2008, http://voices.washingtonpost.com/44/2008/11/obama-raised-half-a-billion-on.html.
[43] "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," Center for Democracy and Technology, April 2010, http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf.

documents from U.S. military computers or in the subsequent transmission of the material to WikiLeaks.[44]

In 2012, Federal authorities issued a subpoena to the microblogging service Twitter, requesting information from the Twitter accounts of Manning, Assange, and others associated with WikiLeaks. With the subpoena came a gag order compelling Twitter not to disclose this information to anyone, including the users in question; Twitter attorneys successfully challenged the gag order in court and were able to notify users before disclosing their information to government officials.[45] A similar case took place in May 2012 when New York City's district attorney issued a subpoena to Twitter, requesting tweets and account information of an Occupy Wall Street protester. Twitter asked a state judge to throw out the request, arguing that the protester merited protection under the Fourth Amendment, given that prosecutors had failed to show probable cause necessary to obtain a warrant for the information.[46]

In August 2011, public transit authorities in San Francisco suspended cell phone service in several underground stations of the Bay Area Rapid Transit (BART) system in an effort to impede planned demonstrations regarding the fatal shooting of a man by BART police the month prior. Numerous digital rights advocates and First Amendment scholars called the decision a violation of BART passengers' First Amendment rights and pointed to the international implications of BART's actions.[47] Following the incident, various civil liberties groups filed an emergency petition with the FCC requesting that the agency declares the BART shutdown a violation of the Communications Act.[48] As of mid-2012, the FCC has not directly responded to these requests but did make a call for public comment on the issue at large, the results of which have yet to be evaluated.[49] The California State Assembly has

[44] Charlie Savage, "U.S. Weighs Prosecution of Wikileaks Founder, but Legal Scholar Warns of Steep Hurdles," New York Times, December 1, 2010, http://www.nytimes.com/2010/12/02/world/02legal.html.
[45] Ryan Singel, "Twitter's Response to WikiLeaks Subpoena Should Be the Industry Standard," Wired, January 10, 2011, http://www.wired.com/threatlevel/2011/01/twitter/.
[46] Dan Goodin, "Twitter fights government subpoena demanding Occupy Wall Street protester info," Ars Technica, May 5, 2012, http://arstechnica.com/tech-policy/2012/05/twitter-fights-government-subpoena-demanding-occupy-wall-street-protester-info/.
[47] David Streitfeld, "Bay Area Officials Cut Cell Coverage to Thwart Protestors," Bits Blog, NYTimes.com, August 12, 2011, http://bits.blogs.nytimes.com/2011/08/12/bay-area-authorities-cut-cell-coverage-to-thwart-protestors/. See also, Cynthia Wong, "Welcome to San Francisco – Next Stop, Cairo?" CDT blog, August 23, 2011, http://cdt.org/blogs/cynthia-wong/238welcome-san-francisco-next-stop-cairo.
[48] Mike Masnick, "FCC Asked For Declaratory Ruling That BART Shutting Off Mobile Phone Service Was Illegal," TechDirt (blog), August 31, 2011, http://www.techdirt.com/blog/wireless/articles/20110830/11591515740/fcc-asked-declaratory-ruling-that-bart-shutting-off-mobile-phone-service-was-illegal.shtml.
[49] "Commission Seeks Comment on Certain Wireless Interruptions," Federal Communications Commission, March 1, 2012, http://www.fcc.gov/document/commission-seeks-comment-certain-wireless-service-interruptions.

approved a bill that would require a court order before allowing for cell network interruption; Senate approval of the bill was pending as of mid-2012.[50]

Although some of the most popular social media platforms in the United States require users to register and create accounts using their real names,[51] there are no legal restrictions on user anonymity on the internet. Constitutional precedents protect the right to anonymous speech in many contexts. There are also state laws that stipulate journalists' right to withhold the identities of anonymous sources, and at least one such law has been found to apply to bloggers.[52] In June 2010, the Obama administration released plans for a National Strategy for Trusted Identities in Cyberspace (NSTIC). The stated goal of the effort is to ensure the creation of an "identity ecosystem" in which internet users and organizations can more completely trust one another's identities and systems when carrying out online transactions requiring assurance of identity.[53] The plan specifically endorses anonymous online speech.[54]

Laws that protect internet communications from government monitoring are complex. While in transit, the contents of internet communications are generally protected from government intrusion by constitutional rules against unreasonable searches and seizures,[55] although there is more legal ambiguity with data stored in "the cloud." The courts, however, have held that transactional data about communications—the who, when, and where of communications between different individuals—is not protected by the Constitution.[56] Law enforcement and intelligence agencies can access such information under varying degrees of oversight as part of criminal or national security investigations. In criminal probes, law enforcement authorities can monitor internet communications in real time only if they have obtained a court order, issued by a judge. The order must reflect a finding that there is probable cause to believe that a crime has been, is being, or is about to be committed. However, the Electronic Communications Privacy Act states that the government can obtain

[50] Hannah Dreier, "Calif. Bill bars agencies from cellphone jamming," San Jose Mercury News, August 9, 2012, http://www.mercurynews.com/news/ci_21274392/bill-would-bar-cellphone-jamming-by-calif-agencies.
[51] Erica Newland, Caroline Nolan, Cynthia Wong, and Jillian York, "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users," Global Network Initiative, September 2011, http://cyber.law.harvard.edu/node/7080.
[52] "Apple v. Does," Electronic Frontier Foundation, accessed August 1, 2012, http://www.eff.org/cases/apple-v-does.
[53] A site created to foster discussion on the proposed strategy can be found at http://www.nstic.us/.
[54] Jay Stanley, "Don't Put Your Trust in 'Trusted Identities,'" Blog of Rights (blog), American Civil Liberties Union, January 7, 2011, http://www.aclu.org/blog/technology-and-liberty/dont-put-your-trust-trusted-identities. See also, Jim Dempsey, "New Urban Myth: The Internet ID Scare," Policy Beta (blog), Center for Democracy and Technology, January 11, 2011, http://www.cdt.org/blogs/jim-dempsey/new-urban-myth-internet-id-scare.
[55] Paul Ohm, "Court Rules Email Protected by Fourth Amendment," Freedom to Tinker, December 14, 2010, http://www.freedom-to-tinker.com/blog/paul/court-rules-email-protected-fourth-amendment.
[56] "A Brief History of Surveillance Law," Center for Democracy & Technology, accessed August 17, 2011, https://www.cdt.org/issue/wiretap-ecpa.

access to email or other documents stored in the cloud with a subpoena issued by a prosecutor or investigator without judicial approval.[57]

The Communications Assistance for Law Enforcement Act (CALEA) requires telephone companies, broadband carriers, and interconnected Voice over Internet Protocol (VoIP) providers to design their systems so that communications can be easily intercepted when government agencies have the legal authority to do so.[58] The FBI suggested in late 2010 that the law should be expanded to impose design requirements on online communications tools such as Gmail, Skype, and Facebook,[59] but as of February 2012, no legislation has been proposed.

Following the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act, which expanded some of the government's surveillance and investigative powers in cases involving terrorism as well as in ordinary criminal investigations. Three expiring provisions of the PATRIOT Act—including the government's broad authority to conduct roving wiretaps of unidentified or "John Doe" targets, to wiretap "lone wolf" suspects who have no known connections to terrorist networks, and to secretly access a wide range of private business records without warrants under Section 215—were renewed for an additional four years in May 2011.[60]

Law enforcement agencies have also begun to use open, public websites, and social media to monitor different groups for suspected criminal activity. One notable example that stoked controversy in February 2012 was an initiative by the New York Police Department (NYPD) to monitor Muslim student groups at various universities in northeastern United States. Associated Press reported that from 2006 onward, the NYPD Cyber Intelligence unit had monitored blogs, websites, and online forums of Muslim student groups and produced a series of secret "Muslim Student Association" reports describing group activities, religious instruction, and the frequency of prayer by the groups.[61] The New York City mayor defended the practice by stating that the NYPD did not break any laws by monitoring websites and online activity that was already publicly available, although others pointed to the religious-profiling nature of the activity.

[57] Ibid.
[58] The FCC does not classify Skype as an "interconnected VoIP" service.
[59] Charlie Savage, "U.S. Tries to Make it Easier to Wiretap the Internet."
[60] "Patriot Act Excesses," New York Times, October 7, 2009, http://www.nytimes.com/2009/10/08/opinion/08thu1.html.
[61] Al Baker and Kate Taylor, "Bloomberg Defends Police's Monitoring of Muslim Student Web Sites," New York Times, February 22, 2012, http://www.nytimes.com/2012/02/22/nyregion/bloomberg-defends-polices-monitoring-of-muslim-student-web-sites.html.

UZBEKISTAN

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Not Free**
Obstacles to Access (0-25)	n/a	19
Limits on Content (0-35)	n/a	28
Violations of User Rights (0-40)	n/a	30
Total (0-100)	**n/a**	**77**

* 0=most free, 100=least free

POPULATION: 30 million
INTERNET PENETRATION 2011: 30 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Uzbekistan has significantly improved its telecommunications infrastructure over the last two decades. President Islam Karimov, who has been in power for over 20 years, has publicly acknowledged the importance of the internet and information and communication technologies (ICTs) to the lives of Uzbek citizens.[1] At the same time, however, Karimov's regime employs a range of legal, administrative, and technical measures to undermine the internet's role as an avenue for open and pluralistic communication, rendering the country's internet regulation the most restrictive in Central Asia. These measures have increased since May 2005 following the violent suppression of public protests in the city of Andijan during which ICTs were used to circulate uncensored information amidst a news blackout in the traditional media.[2]

In 2011, the state-owned telecommunications carrier Uztelecom retained centralized control over the country's connection to the international internet, facilitating nationwide censorship and surveillance. The Uzbek authorities block access to a wide range of international news websites, human rights groups, and exile publications, while limiting access at educational and cultural institutions to the ZiyoNet intranet system. Over the past year and a half, what limited space existed for open online discussion shrunk even further.

[1] Speech of the President RU, "Последовательное продолжение курса на модернизацию страны – Решающий фактор нашего развития" [Consistent Continuation of the Course Toward Modernization of the Country – The Decisive Factor for our Development], December 7, 2010, http://www.press-service.uz/#ru/news/show/dokladi/posledovatelnoe_prodoljenie_kursa_na__1/.

[2] OSCE, "Coverage of the Events and Governmental Handling of the Press During the Andijan Crisis in Uzbekistan: Observations and recommendations," June 15, 2005, http://www.osce.org/fom/15617.

The closure of the popular online forum Arbuz by its owner after the detention of several of its contributors was particularly notable. In addition, in early 2012, two reporters were punished with high fines for online comments or news articles they claimed they had not written, while two others are serving long sentences on trumped-up charges.

Uzbekistan was first connected to the internet in 1997 and in 1999, the government began to seriously invest in the telecommunications infrastructure. Access to online information was relatively open until 2001 when the authorities began filtering politically sensitive websites and reportedly intercepting email communication.[3]

OBSTACLES TO ACCESS

The government of Uzbekistan began investing in telecommunications infrastructure in 1999.[4] Since then, the percentage of the population accessing the internet has grown dramatically, from 6.4 percent in 2006 to over 30 percent in 2011.[5] In practice, there remains a digital divide between urban and rural areas, with the capital Tashkent having the highest internet penetration rate in the country. Rural citizens typically lack the computer literacy to get online, while problems with the electrical grid also limit the usefulness of the telecommunications infrastructure. [6]

In addition to household and workplace access, cybercafes and other public access points remain popular sites for users to get online.[7] Libraries and nearly all of the country's educational institutions connect to the internet via the ZiyoNet intranet network, a system developed by the government for the purpose of providing a "singular platform to gather data and information resources."[8] The ZiyoNet intranet requires user identification and provides access to only "approved" sites, some of which are knock-offs of popular social media sites such as Utube.uz.

[3] "Country Profile: Uzbekistan," OpenNet Initiative, December 21, 2010, http://opennet.net/research/profiles/uzbekistan.
[4] See, UNDP ICT Project, Report "Review of Information and Communication Technologies Development in Uzbekistan: 2005," Tashkent 2006, p. 3, http://www.undp.uz/en/publications/publication.php?id=19.
[5] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[6] See, ITU project in Uzbekistan, "Sustainable electricity supply of telecommunications objects in rural and remote areas," from 2011-2013, accessed September 21, 2012, http://www.itu.int/ITU-D/projects/display.asp?ProjectNo=2UZB11003.
[7] As of October 1, 2011, the number of "points of collective access," including internet cafes, reached 1,032. See, UzACI, "Коллегия УзАСИ подвела итоги деятельности 9 месяцев" [The UzACI Board Summed up 9 Months of its Activity], October 25, 2011, http://www.aci.uz/ru/news/uzaci/article/1407.
[8] Resolution of the Cabinet of Ministers RU "О дальнейшем развитии сети 'ZiyoNET'" [On the Further Development of a ZiyoNET Network], No. 282, December 28, 2005, *SZ RU* (2005) No. 52, 389.

Users can access the internet via ADSL broadband or a dial-up connection, with the latter being more common in rural than urban areas. In 2011, the government made a commitment to expand the number of internet users through dial-up connections from 3 to 3.5 million users.[9] President Karimov also set the target of reaching 100,000 broadband subscribers as a national priority for 2011, a target that was reportedly reached.[10] In August 2011, the government thus launched the mass production of broadband modems and network devices together with the Chinese telecommunications equipment supplier ZTE.[11] WiMAX broadband is available, though in March 2011, internet service providers (ISPs) were officially banned from providing internet via satellite.[12]

The price for internet access dropped in 2011 but remains beyond the reach of large segments of the population. During the year, the state-owned telecommunications operator Uztelecom reduced prices by 22 percent.[13] In January 2012, Uztelecom began offering households ADSL broadband packages for between 9,000 and 85,000 Uzbek soms (US$5-$47) per month for speeds ranging from 600 Kbps to 2 Mbps, respectively.[14] Still, given that the official average monthly wage was 711,633 Uzbek soms (US$407) as of September 2011, the higher speeds remain too expensive for many Uzbeks.[15]

[9] Uztelecom, "Рассмотрены перспективы развития телекоммуникационных сетей" [The Prospective for the Development of Telecommunications Networks Has Been Analyzed], February 21, 2011, http://www.uztelecom.uz/ru/press/media/2011/141/.

[10] According to the ITU, the country had 147,760 fixed line broadband subscriptions by the end of 2011. See, International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011. Report of the President RU to the Government, "Все наши устремления и программы – Во имя дальнейшего развития родины и повышения благосостояния народа" [All our aspirations and programs – in the name of the further development of the motherland and improvement of the welfare of the people], February 21, 2011, http://www.press-service.uz/ru/news/archive/dokladi/#ru/news/show/dokladi/vse_nashi_ustremleniya_i_programmyi___1/.

[11] Since opening its Uzbekistan office in 2003, ZTE has become a leading supplier of telecommunications equipment in the country. Uztelecom, "Запущена в эксплуатацию технологическая линия по производству DSLAM оборудования и ADSL модемов" [A Technological Production of DSLAM Equipment and ADSL modems Has Been Launched], August 31, 2011, http://www.uztelecom.uz/ru/press/news/2011/187/.

[12] IREX, "Uzbekistan."

[13] UzACI, "Президент Республики Узбекистан отметил ускоренный рост сферы связи и информатизации" [The President of the Republic of Uzbekistan Remarked on the Accelerated Development in the Field of Communication and Informatization], January 20, 2012, http://www.aci.uz/ru/news/uzaci/article/1436/.

[14] FTTB broadband is available only to legal entities. See, Uztelecom, "Преискурант на основные и дополнительные услуги 'Uzonline'" [Price List for Basic and Additional Services 'Uzonline'], Annex II http://uzonline.uz/upload/files/oferta_yanv.pdf.

[15] In reality, the average salary is much less than official figures. For the estimation of official figures compare statistics data in Ministry of Economy of the RU, "Об итогах социально-экономического развития Республики Узбекистан за девять месяцев 2010 года," September 9, 2010 http://www.mineconomy.uz/node/320 and "Об итогах социально-экономического развития Республики Узбекистан за девять месяцев 2011 года," November 7, 2011 http://uza.uz/ru/business/16933/.

Mobile phone penetration is substantially higher than for the internet, with over 25 million Uzbeks (over 85 percent of the population) having a mobile phone subscription in 2011.[16] Mobile phone connectivity via 3G technology is widely available, though as of October 2011, only 23 percent of mobile phone subscribers had used the device to access the internet.[17] MTS-Uzbekistan launched the country's first 4G network in July 2010, but it was available only in limited parts of the capital Tashkent.[18]

The telecommunications infrastructure in Uzbekistan is centralized and controlled by state-owned Uztelecom, which enjoys a monopoly over the country's connection to the international internet.[19] Private carriers, such as mobile phone companies and ISPs, must access international telecommunications networks exclusively through Uztelecom's infrastructure. This dominant position was further cemented in February 2011, when the government issued an administrative order prohibiting private ISPs from establishing their own satellite connection.[20] Such restrictions have firmly established Uztelecom as an upstream ISP, with private ISPs required to have their networks pass through a single node controlled by Uztelecom.[21] Uztelecom can also control the price at which it sells traffic to downstream ISPs. From January 2011 to January 2012, it lowered this price substantially, from around US$850 for 1 Mbps to US$500. As noted above, this reduction was partially passed down to consumers.[22]

The government's control over the internet infrastructure and its influence on mobile phone operators enables it to limit or block connectivity to Web 2.0 applications at will, which it appears to have done on several occasions in recent years. In August 2011, users and independent news websites reported that the Google search engine and its Russian equivalent Rambler were blocked for several days amidst a broader increase in blocked

[16] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[17] However, it is not clear whether this official data also include statistics of internet access provided by private mobile phone companies. See, UzACI, "Коллегия УзАСИ подвела итоги деятельности 9 месяцев" [The UzACI Board Summed up 9 Months of its Activity], October 25, 2011, http://www.aci.uz/ru/news/uzaci/article/1407.

[18] UzDaily, "МТС-Узбекистан начал продавать 4G модемы" [MTS-Uzbekistan Started to Sell 4G Modems], December 22, 2011, http://www.uzdaily.uz/articles-id-9334.htm.

[19] See note 3 above.

[20] Приказ генерального директора Узбекского агенства связи и информатизации "О внесении изменений в Положение о порядке регулирования межсетевого взаимодействия Интернет-провайдеров на сетях передачи данных" [Order of the General Director of UzACI 'On Amendements to the Rules on the Procedure Regulating Network Interconnection Among Internet Providers on Data Networks'], No. 4-Yu, February 28, 2011, *SZRU* (2011) No. 10-11 (458-459), item 108, at Annex.

[21] See, Law RU, "O telekommunikatsiiakh" [On Telecommunications], No. 822-I, 20 August 1999, *VOM RU* (1999) No. 9, 219, as amended by Law No. ЗРУ-314 on December 30, 2011, at Art. 17, para. 3.

[22] Uztelecom, "Очередное снижение тарифов на интернет-услуги для провайдеров" [Another reduction of tariffs for Internet services providers], January 21, 2012, http://www.uztelecom.uz/ru/investors/shareholders/2011/272/.

websites (see "Limits on Content").[23] Government officials and service providers denied that the disruptions were intentional, but observers suspected that the restrictions were related to the upcoming 20th anniversary of the end of the Soviet era in September 2011 and the government's fear that it might trigger social media-inspired protests in Uzbekistan.[24]

In an unusual incident on August 2, 2011, mobile phone operators throughout the country suspended text message and internet services for one day (voice conversations were not affected), coinciding with national university entrance exams. The shutdown was an apparent effort by the government to prevent cheating, though it affected all of the country's mobile phone users.[25] Apart from these sporadic restrictions, the video-sharing site YouTube, social-networking site Facebook, microblogging service Twitter, and popular Russian virtual community LiveJournal remained generally available in 2011, though some individual pages were blocked. In March 2012, however, reports emerged that the Uzbek authorities had blocked LiveJournal out of concern that potential protests could erupt over the results of the Russian presidential elections.[26] Unconfirmed reports also indicate that the blog-hosting platform Wordpress is blocked.[27]

Private ISPs and hosting providers require a government license to operate in Uzbekistan. They totaled 939 by October 2011 but, as noted above, all must connect via Uztelecom. As of May 2012, the market for mobile phone services was shared by Uztelecom and four private operators: Ucell, the Russian firms Beeline and MTS-Uzbekistan, and Perfectum Mobile.

As private ISPs are unable to establish their own international internet connections, since 2004, several providers have sought to connect with each other via the Tashkent Internet Exchange, or TAS-IX network.[28] By 2011, 37 ISPs were connected via the exchange. Under an agreement signed between the ISPs, the network enables them to route data among their networks without applying mutual charges and without having to pass through Uztelecom's

[23] Reporters Without Borders, "Uzbekistan," *Enemies of the Internet 2012*, March 12, 2012, http://en.rsf.org/uzbekistan-uzbekistan-12-03-2012,42079.html.
[24] Institute for War & Peace Reporting, "Tashkent Spooked by Web Interest in Arab Protests," February 24, 2011, http://iwpr.net/report-news/tashkent-spooked-web-interest-arab-protests; "В Узбекистане блокируют Живой Журнал и поисковые системы" [LiveJournal and Search Engines are Blocked in Uzbekistan], Ferghana News, August 10, 2011, http://www.ferghananews.com/news.php?id=17125; Catherine A. Fitzpatrick, "Uzbekistan: Internet Sites Blocked," Eurasianet.org, August 10, 2011, http://www.eurasianet.org/node/64026.
[25] "Uzbekistan 'halts mobile Internet, SMS' for exam day," AFP, August 2, 2011, http://www.google.com/hostednews/afp/article/ALeqM5iAt_J3V1eR_Homvu0Osp2K3mqMdQ.
[26] "LiveJournal website blocked in Uzbekistan," Uznews.net, March 20, 2012, http://www.uznews.net/news_single.php?nid=19380.
[27] IREX, "Uzbekistan."
[28] Центр взаимодействия сетей передачи данных, "TAS-IX," accessed September 20, 2012, http://www.tas-ix.uz.

network. The TAS-IX network provides users with access to websites and data hosted within Uzbekistan without additional charges.[29]

The Uzbek Agency for Communications and Information (UzACI) is the national telecommunications regulator responsible for issuing licenses to private ISPs, mobile phone companies, and cybercafes. It is a governmental body and lacks institutional independence. Service providers are required to have a license to operate, and in 2005, the Cabinet of Ministers adopted Resolution No. 155, which stipulates that telecommunications providers must first register as a legal entity before being issued a license. Thereafter, the licensing procedure is fairly straightforward but is often encumbered by political interests in practice, with applicants from outside the government's inner circle regularly denied licenses for unjustifiable reasons.[30]

The director-general of UzACI is appointed by the president, although this position has also been filled by the Uzbek deputy prime minister in the past.[31] In addition to issuing licenses, UzACI approves the regulatory policies for the use of domain names registered with the ".uz" country-code.[32] The Computerization and Information Technologies Development Centre (Uzinfocom), a structural division of UzACI is the ".uz" top-level domain manager. It is also the largest provider of web hosting services within the country. As of December 2011, its servers hosted 1,235 websites—or nearly 20 percent—of all of Uzbekistan's domestically hosted websites.[33]

LIMITS ON CONTENT

The Uzbek government engages in pervasive and systematic blocking of internet content that contains information about human rights, criticism of the government, and censure of the president.[34] The most recent tests by the OpenNet Initiative (ONI) in 2007-2008 found widespread blocking of local and international human rights groups' websites, independent online news outlets, and opposition websites, as well as some content related to local civil society and religious groups. Websites associated with the BBC Uzbek Service, the U.S. government-funded Radio Free Europe/Radio Liberty (RFE/RL), and the German public broadcaster Deutsche Welle are also inaccessible. Online media such as Uznews.net,

[29] Uztelecom sells the connection to the TAS-IX network at the average connection speed of 2 Mb/sec. See note 7 above.
[30] IREX, "Uzbekistan."
[31] European Bank for Reconstruction and Development, "Legal Transition Program: Comparative Assessment of the Telecommunications Sector in the Transition Countries: Assessment Report Uzbekistan," December 2008, http://www.ebrd.com/downloads/legal/telecomms/uzbek.pdf.
[32] Law RU, "On Telecommunications," Art. 8.
[33] See, WWW.UZ, Statistical Data, "Хостеры по количетву сайтов" [Hosting Providers' Rating], December 28, 2011, http://www.uz/ru/providers/.
[34] Reporters Without Borders, "Uzbekistan," *Enemies of the Internet 2012*.

Ferghana, Harakat.net Mediauz.ucoz.ru and the websites of Uzbek opposition groups in exile are among those permanently blocked. In addition to being blocked, none of these websites appear in the results of the national search engine www.uz,[35] which is regulated by the government and catalogues primarily sites with ".uz" domain names.

These restrictions remained in place as of April 2012. Moreover, new rounds of censorship were implemented throughout 2011. During the year, a number of websites were rendered inaccessible, including those of the Institute for War and Peace Reporting, and Reuters, as well as Russian-language news websites such as EurasiaNet, and Voice of Freedom. In some instances, the blocks were temporary and lasted only a few days. For example, in August 2011, around the 20th anniversary of the end of the Soviet era, dozens of websites with the ".ru" domain became inaccessible in Uzbekistan, including the sites of the Russian newspapers *Pravda, Izvestiya, Kommersant,* and *Parlamentskaya*.[36] In other cases, blocks appeared indefinite, such as for the websites of Human Rights Watch, Reporters Without Borders, and Amnesty International, among numerous others. Freedom House's website nevertheless remained unblocked as of August 2011.[37] At the time, some observers suggested that the source of the disruptions may have been technical problems rather than political motivations, as some websites with the ".uz" domain that were not considered controversial also encountered problems.[38]

In employing censorship, the Uzbek authorities appear to have fairly sophisticated technology at their disposal. This enables them to not only block whole domains, but also restrict access to individual pages that contain politically sensitive content while retaining access to other parts of a particular site. For example, in February 2011, after people started discussing anti-government protests erupting in the Middle East, including expressing solidarity with demonstrators and sharing news links about what was happening, users began reporting that certain pages and discussions on Facebook, LiveJournal, and Twitter were being blocked, though the social media tools as a whole remained available.[39] Similarly, in February 2012, the media reported that the Uzbek-language pages of the online encyclopedia Wikipedia were being blocked, while their Russian counterparts remained available, although the latter typically contain more information on often censored topics

[35] Resolution of the President RU "О дополнительных мерах по дальнейшему развитию информационных технологий" [Program on the Establishment and Development of a National Information Search System], No.ПП-117, signed July 8, 2005, Annex 3, *SZRU* (2005) No.27, 189.
[36] IREX, "Uzbekistan."
[37] "Uzbek media censors are back at work," Neweurasia.net, August 10, 2011, http://www.neweurasia.net/media-and-internet/uzbek-media-censors-are-back-at-work/; Inga Sikorskaya, "Cyber-Censorship in Uzbekistan," Institute for War & Peace Reporting, March 15, 2011, http://iwpr.net/report-news/cyber-censorship-uzbekistan.
[38] "Dozens of Websites in Uzbekistan Suffer Access Problems," RFE/RL, August 12, 2011, http://www.rferl.org/content/dozens_of_websites_in_uzbekistan_experience_access_problems/24295316.html.
[39] Institute for War & Peace Reporting, "Tashkent Spooked by Web Interest in Arab Protests," news briefing, February 24, 2011, http://iwpr.net/report-news/tashkent-spooked-web-interest-arab-protests.

like human rights abuses. Analysts speculated that the block was more related to the government's nationalistic wish to monopolize Uzbek-language content than because of concerns that users would access politically sensitive information.[40]

Most censorship takes place at the country's international internet connection operated by Uztelecom. However, under the 1999 Law on Telecommunications and several other government resolutions, lower tier ISPs may have their license revoked if they fail to take measures to prevent their computer networks from being used for exchanging information deemed to violate national laws, including ones that restrict political speech. Under Order No. 216 passed in 2004, ISPs and operators "cannot disseminate information that, inter alia, calls for violent overthrow of the constitutional order of Uzbekistan, instigates war and violence, contains pornography, or degrades and defames human dignity."[41] Given these restrictions, many individuals and organizations prefer to host their websites outside the country.[42]

Pressures have also been put on mobile phone operators. In March 2011, amidst growing unrest in the Middle East, regulators demanded that operators notify the government of any attempts to circulate mass text messages with "suspicious content" and reportedly warned that the providers would be required to shut down internet connections provided to mobile users at the authorities' request.[43]

Several government-linked entities monitor and control online communications, though the opaque system offers few details on how decisions are made or what websites are blocked at any given time. The Center for the Monitoring of the Mass Communications Sphere, an operational arm of UzACI established in 2004, takes various measures to maintain compliance with national legislation that restricts free expression.[44] Its key objectives are "to analyze the content of information disseminated online and ensure its consistency with

[40] Jillian C. York, "This Week in Censorship: Syrian, Moroccan Bloggers Under Fire; New Censorship in Uzbekistan," Electronic Frontier Foundation, March 1, 2012, https://www.eff.org/deeplinks/2012/02/week-censorship-blogger-threats-syria-morocco-uzbek-censorship; Sarah Kendzior, "Censorship as Performance Art: Uzbekistan's Bizarre Wikipedia Ban," The Atlantic, February 23, 2012, http://www.theatlantic.com/international/archive/2012/02/censorship-as-performance-art-uzbekistans-bizarre-wikipedia-ban/253485/.

[41] Regulation "О порядке предоставления доступа к сети Интернет в общественных пунктах пользования" [On Adoption of the Terms of Provision of Access to the Internet Network in Public Points of Use], promulgated by Order of the Communications and Information Agency of Uzbekistan No. 216, 23 July 2004, *SZRU* (2004) No. 30, item 350.

[42] According to government figures, only about 30 percent of websites with ".uz" domain names were hosted on servers based in Uzbekistan as of December 2011. See Uzinfocom, "Только цифры" [Only Numbers], January 5, 2012, http://www.uzinfocom.uz/news/center/show/395/.

[43] Murat Sadykov, "Uzbekistan Tightens Control over Mobile Internet," Eurasianet.org, March 15, 2011, http://www.eurasianet.org/node/63076.

[44] Zhanna Hördegen, "The Future of Internet Media in Uzbekistan: Transformation from State Censorship to Monitoring of Information Space since Independence," in Eric Freedman and Richard Schafer (eds.), *After the Czars and Commissars: Journalism in Authoritarian Post-Soviet Central Asia* (The Eurasian Political Economy and Public Policy Studies Series, Michigan State University Press, April 2011), 99-121.

existing laws and regulations."[45] Based on its systematic monitoring of online content, the Center has contributed to the shuttering of independent websites.[46] In March 2010, for example, at the Center's request, a court ordered the closure of eDoctor.uz, one of the country's most prominent medical advice websites, claiming that its references to sexuality were pornographic.[47] The site was re-launched in 2011 and accessible as of May 2012. Also in 2010, the Center facilitated the criminal prosecution of two independent online journalists (see "Violations of User Rights").

In August 2011, the government created a new secretive body—the Expert Commission on Information and Mass Communications—to oversee online controls, including the work of the Monitoring Center.[48] The Commission is not independent and must submit quarterly reports to the Cabinet of Ministers.[49] Furthermore, its membership is not made public,[50] although the body is reportedly comprised exclusively of government employees.[51] The new Commission is mandated to evaluate online publications and determine if they (1) have a "destructive and negative informational-psychological influence on the public consciousness of citizens;" (2) fail to "maintain and ensure continuity of national and cultural traditions and heritage;" or (3) aim to "destabilize the public and political situation," or commit other potential content violations.[52]

The Commission also assesses publications referred to it by the Monitoring Center or other state bodies, including the courts and law enforcement, drawing on a designated pool of government-approved experts.[53] The experts submit reports to the Commission whose members then vote on whether or not a violation had been committed. If a violation is found, the decision becomes the basis for action to be taken by state bodies, including courts, and by "other organizations," presumably private ISPs.[54] There are no procedures in place that require notification of those whose content is affected by the decision or that grant

[45] Paragraph 1, Regulation No. 555, On the Measures of Improving the Organizational Structures in the Sphere of Mass Telecommunications, adopted by the Cabinet of Ministers of Uzbekistan on November 24, 2004, via OpenNet Intiative, "Uzbekistan," December 2010, http://opennet.net/research/profiles/uzbekistan#footnote37_1d627h4.

[46] A news website *Informator.Uz* was shut down in 2007. See, "Pochemu zakrito nezavisimoe SMI Uzbekistana—Informator.Uz?" [Why the independent mass media of Uzbekistan, Informator.Uz, is closed?], September 20, 2007, www.uforum.uz/showthread.php?t=2565.

[47] A medical website eDoctor.uz was shut down by a court decision. See, Uznews.net, "В Узбекистане закрывается лучший медицинский сайт" [The Best Medical Website is Going to be Shut Down in Uzbekistan], March 25, 2010, http://www.uznews.net/news_single.php?lng=ru&cid=30&sub=&nid=13072.

[48] Resolution of the Cabinet of Ministers RU, "О дополнительных мерах по совершенствованию системы мониторинга в сфере массовых коммуникаций" [On Supplementary Measures for the Improvement of the Monitoring System for the Sphere of Mass Communications], No. 228, 5 August 2011, *SZ RU* (2011) No. 32-33, item 336.

[49] Ibid., at Annex II, Art. 31.

[50] Ibid., Annex I, containing a list of the Commission's members, is not made public.

[51] Reporters Without Borders, "Uzbekistan," *Enemies of the Internet 2012*.

[52] Resolution of the Cabinet of Ministers RU, No. 228, at Art. 1 and Annex II, Art. 5. See note 50 above.

[53] Ibid., at Art. 1 and Annex II, Art. 14.

[54] Ibid., at Annex II, Arts. 26 and 29.

them an opportunity to defend the speech in question, nor is there a clear avenue to appeal the decision after it is made. As of May 2012, the commission appeared to be functioning but little information on its activities was available. The broadly defined violations and wide discretion granted to the Commission raised concerns of how it could be used to suppress or punish free speech—including ordering ISPs to delete content or encouraging the arbitrary imprisonment of bloggers—particularly given the Uzbek government's track record of politically motivated censorship.[55]

Self-censorship is pervasive given the government's tight controls over the media and harsh punishment of those who report on topics deemed "taboo," be they criticism of the president, revelations about corruption, or health education.[56] Given the government's history of harassing traditional journalists, as well as their families, many online writers are cautious about what they post.

In an apparent effort to develop the country's media and information society, President Karimov signed a decree in December 2011 that extends tax preferences to media outlets. Taking effect on January 1, 2012, the decree exempts media services from the value added tax (VAT) and decreases the single tax payment required of media organizations from 6 to 5 percent, among other changes.[57] While the decree purportedly aims to strengthen "public control over the activities of state power and control,"[58] observers have noted that without an overall change in the regime's attitude to independent media, the new benefits will unlikely have a meaningful effect on freedom of speech in the country.[59]

The editorial direction of the online versions of state-run news outlets is often determined by unofficial guidelines from the government. Although proxy servers and anonymizers are available to circumvent the government's blocking of websites, they require computer skills beyond the capacity of many ordinary users in Uzbekistan.

According to the website rating firm Alexa, international social media websites like Facebook, YouTube, and Twitter, as well their Russian equivalents are among the most

[55] For the detailed discussion of the governmental regulation of speech on ideological grounds, see: Zhanna Kozhamberdiyeva, "Freedom of Expression on the Internet: A Case Study of Uzbekistan," *Review of Central and East European Law* Vol. 33 (1) 2008, 95-134.

[56] Uznews.net, "В Узбекистане закрывается лучший медицинский сайт" [The Best Medical Website is Going to be Shut Down in Uzbekistan], March 25, 2010, http://www.uznews.net/news_single.php?lng=ru&cid=30&sub=&nid=13072; Catherine A. Fitzpatrick, "Uzbekistan: AIDS Activist Released, But Other Human Rights Defenders Harassed," September 6, 2011, http://www.eurasianet.org/node/64131.

[57] Alastair Carthew and Simon Winkelmann, "Uzbekistan – Overview," Konrad-Adenauer-Stiftung - Media Programme Asia, last updated May 24, 2012, http://www.kas.de/medien-asien/en/pages/10117/.

[58] "President of Uzbekistan Provides Tax Preferences to Media," The Journal of Turkish Weekly, December 31, 2011, http://www.turkishweekly.net/news/129114/president-of-uzbekistan-provides-tax-preferences-to-media.html.

[59] IREX, "Uzbekistan."

visited in Uzbekistan. The most popular social-networking site is the Russian Odnoklassniki.ru, which reportedly had 350,000-400,000 users a day as of September 2011.[60] Facebook is ranked second with over 120,000 members from Uzbekistan by April 2012, a notable increase from the year before.[61]

As social-networking sites and blogging platforms have grown in popularity, the government has adopted a new approach to influencing the information circulated on them—by creating and promoting Uzbek alternatives to popular global or regional brands. In 2010, the state-run Uzinfocom Center began creating a "social media zone" specifically geared towards users of the ZiyoNet intranet in Uzbekistan. The zone includes a range of Web 2.0 applications, including Id.uz (a social-networking site), Fikr.uz (a blog-hosting platform), Utube.uz (a video-sharing platform), Smsg.uz (an instant messenger service), and Desk.uz (a site for personal widgets). Access to these applications requires users to register their personal data, including passport numbers in some cases. Though for the moment, the zone's applications remain less popular than international brands, as of May 2012, over 23,000 people had registered at Id.uz.[62] Uzinfocom Center's close relationship to the government has also raised concerns over the pressure the applications may receive from the authorities to censor and monitor users.

Besides the social media zone aimed at ZiyoNet users, two other social-networking websites were created in recent years with government support.[63] The more popular of the two is Muloqot.uz, (meaning "dialogue") launched in September 2011 in an apparent effort to offset the growing influence of Facebook.[64] It is open only to Uzbek citizens residing in Uzbekistan and at least one incident of censorship has been reported.[65] On the first day the social network was launched, staff of the Uzbek service of RFE/RL reportedly registered accounts and posted RFE/RL content, which is usually blocked, to a general "wall." According to their reports, within 15 minutes, their profiles were deleted.[66]

Meanwhile, in December 2011, one of the country's most popular online forums, Arbuz.com, was shut down following government pressure. Launched in 2002, Arbuz had

[60] "Top Sites in Uzbekistan," Alexa.com, accessed May 1, 2012, http://www.alexa.com/topsites/countries/UZ; Luke Allnutt, "Uzbekistan Launches Its Own Facebook, Except It's Not For Everyone," Movements.org, August 28, 2011, http://www.movements.org/blog/entry/uzbekistan-launches-its-own-facebook-except-its-not-for-everyone/.

[61] "Uzbekistan Facebook Statistics," SocialBakers, accessed May 1, 2012, http://www.socialbakers.com.

[62] Uzinfocom, "Только цифры" [Only Numbers], May 5, 2012, http://www.uzinfocom.uz/news/center/show/426/.

[63] See, UzACI, "Развиваются национальные информационные ресурсы. - УзА" [National information Resources are Developing - UzA], which reports on the creation of http://my.olam.uz/ with support of Uztelecom, http://www.aci.uz/ru/news/about_ict/article/1079/.

[64] "Manifest of the Community Muloqot.Uz," Muloqot, accessed May 1, 2012, http://muloqot.uz/help/about.

[65] Freedom House, "Uzbekistan Launches Government-Run Social Networking Site on Anniversary of Independence," Freedom Alert, August 31, 2011, http://www.freedomhouse.org/article/uzbekistan-launches-government-run-social-networking-site-anniversary-independence.

[66] Luke Allnutt, "Uzbekistan Launches Its Own Facebook, Except It's Not For Everyone."

grown to become a popular collection of chat-rooms and online conversations, particularly among Uzbek youth. Much of the content covered entertainment news or personal matters, but it was also a haven for relatively open political discussion in Uzbekistan's closed media environment. During times of crisis, such as the 2005 Andijan massacre or the 2010 violence against Uzbeks in Kyrgyzstan, the forum emerged as a crucial space for citizens to share information and critique government action amidst a traditional media blackout.[67] In January 2011, the National Security Service (NSS) reportedly arrested several people who had posted anonymous comments on Arbuz. The site was temporarily shut down and then resurfaced a month later, with the administrators having removed discussion threads related to sensitive topics such as domestic politics, religion, and events in Kyrgyzstan.[68] During that time, the website was blocked, though many Uzbeks continued to access it with circumvention tools. Still fearing for the safety of users, the administrators decided to close down the site altogether in December 2011;[69] they opened a new forum at Choyxona.com in January 2012.[70]

The blogosphere in Uzbekistan is weak and, due to the repressive environment, unable to significantly facilitate public discourse on political and social issues. A few blogs and forums critical of the regime are affiliated with independent online news sites run by the Uzbek diaspora and registered at domains with servers located outside Uzbekistan.[71] Although there were no significant cases of political mobilization via social media, these tools have been important for exposing and disseminating information related to human rights abuses. In May 2005, for example, videos documenting Uzbek security forces opening fire on unarmed protesters in Andijan were uploaded to YouTube and regular updates were posted on Arbuz, contributing to international condemnation of the incident.

More recently in 2011, Malohat Eshonkulova and Saodat Amonova—two reporters for the state-controlled TV station Yoshlar who were fired in December 2010 for exposing the censorship and embezzlement at the National Broadcasting Company—used Twitter to document their pursuit of justice. The journalists filed a lawsuit against the station for unfair dismissal, but the court prohibited media coverage of the April 2011 hearings and barred

[67] Sarah Kendzior, "Breeding an 'activism without activists' in Central Asia," Al Jazeera, March 5, 2012, http://www.aljazeera.com/indepth/opinion/2012/03/201234144346963257.html.

[68] The three removed threads were: "Uzbekistan: Problems and Solutions," "Religion," and "Tragic Events in Kyrgyzstan." "Узбекистанский форум "Arbuz.com" – под «колпаком» СНБ" [Uzbek Forum Arbuz.com is under the "Hat" of National Security Service], Uznews.uz, February 9, 2011, http://www.uznews.net/news_single.php?lng=ru&cid=3&nid=16295.

[69] Barno Anvar, "Arbuz.com охир-оқибат ёпилди" [in Uzbek], Ozodlik.org, December 8, 2011, http://www.ozodlik.org/content/article/24415432.html; IWPR, "Web Use Spirals in Uzbekistan Despite Curbs," news briefing, January 3, 2012, at http://iwpr.net/report-news/web-use-spirals-uzbekistan-despite-curbs; Sarah Kendzior, "Breeding an 'activism without activists' in Central Asia."

[70] IWPR, "Web Use Spirals in Uzbekistan Despite Curbs"; "Arbuz.com форуми Choyxona.comга кўчди" [Arbuz.com moved to Choyxona.com], Ozodlik.org, January 9, 2012, http://www.ozodlik.org/content/article/24446394.html.

[71] See, e.g., Turonzamin.org (run since 2003) and Jahonnoma.com. Also FromUz.com – a website of Uzbek immigrants – has a popular forum and chat room.

access to independent observers. The journalists instead tweeted reports of the courtroom proceedings.[72] In June 2011, the two went on hunger strike and continued using Twitter to report the harassment they encountered from the authorities and others.[73]

VIOLATIONS OF USER RIGHTS

The Constitution of Uzbekistan guarantees freedom of expression, freedom of information (Articles 29 and 30), and freedom for the mass media. It also contains a prohibition on censorship (Article 62). In practice, however, these rights are severely restricted, both by contradictory laws and due to the lack of an independent judiciary to uphold these constitutional protections. The president appoints all judges.[74]

Under the Law on Mass Media, journalists in Uzbekistan are required to register with the government, and amendments to the law in 2007 extended the definition of the "press" to apply to websites as well. To be regarded as a news source, websites must obtain a government-issued registration certificate, following a typically arbitrary and politicized press procedure.[75] As of December 2011, there were about 160 private websites registered as mass media in Uzbekistan.[76] The law, however, fails to mention blogs so it remains unclear whether bloggers unaffiliated with traditional news media outlets are considered journalists and thus covered by statutory protections given to print and broadcast journalists under the Law on Protection of the Professional Activities of Journalists.

The 2007 amendments to the Law on Mass Media were added with the express purpose of extending its scope to websites, including overseas ones whose content is accessible from within the territory of Uzbekistan.[77] Consequently, restrictive legislation governing the

[72] "Иск журналисток ТВ «Ёшлар» будет рассматривать та же судья" [A Same Judge Will Examine a Complain by Two Journalists of TV "Yoshlar"], Uznews.uz, April 4, 2011, http://www.uznews.net/news_single.php?lng=ru&cid=3&nid=16817.

[73] See, Twitter account „@ Malohat_Saodat." See also, Catherine A. Fitzpatrick, "Uzbekistan: Hunger-Stricking Journalists Cancel Press Conference," Eurasianet.org, July 8, 2011, http://www.eurasianet.org/node/63828.

[74] Art. 106 of Uzbek Constitution explicitly guarantees the independence of the judiciary. But see, Joint Resolution of the Plenums of the Supreme Court and Higher Economic Court, "О судебной власти" [On the Judicial Branch of Power], No. 1, December 20, 1996, as amended Dec. 22, 2006 (No. 14/151), at para. 3.

[75] See, Resolution of the Cabinet of Ministers RU "О внесении изменений и дополнений в Положение о порядке государственной регистрации средств массовой информации в Республике Узбекистан" [On the Changes and Ammendements to the Regulation on State Registration of the Mass Media in the Republic of Uzbekistan], No. 68, Apr. 2, 2007, in *SZ RU* (2007) No. 14, item 141, at Annex II. See Human Rights Committee, Mavlonov and Sa'di v. the Republic of Uzbekistan, Communication No. 1334/2004, Views adopted on April 29, 2009, UN Doc. CCPR/C/95/D/1334/2004, at paras. 2.4-2.14.

[76] See, Parliament RU, "Меры поддержки негосударственных СМИ" [Measures Supporting Independent Mass Media], December 28, 2011, http://www.parliament.gov.uz/ru/analytics/5051?sphrase_id=12000.

[77] Law RU, "О средствах массовой информации" [On the Mass Media] No. 541-I, adopted 26 December 1997, as amended on 15 January 2007, *SZRU* (2007) No. 3, item 20, Arts. 2 and 4.

publication of content by traditional media now also applies to online communications. While there are no laws that specifically criminalize acts involving ICTs, some laws have been used to punish individuals for posting or accessing content deemed to violate vague information security rules.[78] Under the Criminal Code, for example, slander (Article 139) and insult (Article 140)—including of the president (Article 158)—are criminal offenses that also apply to online content, as do provisions that punish activities such as "dissemination of materials posing a threat to public safety." Both slander and insult are punishable with fines ranging from 50 to 100 times the minimum monthly wage, correctional labor of two to three years, arrest of up to six months, or detention for up to six years.[79]

In recent years, these provisions have been used to prosecute journalists for online expression, including two cases in 2010. In October of that year, Vladimir Berezovsky, a Russian citizen and editor of the Vesti.uz website living in Uzbekistan, was convicted of libel and insult but was immediately granted amnesty and released.[80] That same month, a court convicted Abdumalik Boboyev—an Uzbek national and reporter for the U.S. government-funded Voice of America's Uzbek Service and website—of defamation, insult, and disseminating material that threatened national security.[81] The indictment was based on materials that Boboyev had produced for Voice of America, which covered a wide range of domestic social, political, and economic issues, including human rights abuses and youth unemployment.[82] Boboyev was ordered to pay a fine of 400 times the minimum wage, or 18.86 million soms (US$11,500). Though such a sum is prohibitively expensive for an Uzbek journalist, the ruling was seen as a relatively mild sentence, since the crimes can carry a punishment of five to eight years in prison.[83] Though his fine had been paid, in May 2011, the government denied Boboyev an exit visa to go to Germany to study on a scholarship;[84] following international pressure, however, he received permission to leave in

[78] Zhanna Kozhamberdiyeva, "Freedom of Expression on the Internet: A Case Study of Uzbekistan."
[79] Article 139 and Article 140, Criminal Code of the Republic of Uzbekistan, http://www.ctbto.org/fileadmin/user_upload/pdf/Legal_documents/national_provisions/Uzbekistan_CriminalCode_220994.pdf.
[80] His writings covered topics such as a gas explosion, train collision, and drug trafficking. See, United States Mission to the OSCE, "Statement on Media Freedom in Uzbekistan," September 23, 2010, http://osce.usmission.gov; http://www.ifex.org/uzbekistan/2010/10/26/boboyev_sentence/
[81] For the text of the indictment and "expert opinion" of the UzACI's Monitoring Center see, "In Uzbekistan, the new VOA reporter Malik Boboeva tried for slander against the democratic order (text indictment and expert opinions" [in Russian], Fergana News, October 7, 2010, www.ferghana.ru/article.php?id=6754.
[82] IWPR, "Voice of America Reporter Charged in Uzbekistan," new briefing, September 17, 2010, http://iwpr.net/report-news/voice-america-reporter-charged-uzbekistan.
[83] IFEX, "Two journalists found guilty of slander in separate cases," alert, October 26, 2012, http://www.ifex.org/uzbekistan/2010/10/26/boboyev_sentence/.
[84] "Embattled reporter prevented from leaving Uzbekistan," Committee to Protect Journalists, May 25, 2011, http://cpj.org/2011/05/in-uzbekistan-embattled-reporter-prevented-from-le.php.

June.[85] In both cases, the Uzbek courts followed the recommendations of UzACI's Monitoring Center and their assessment of the unlawfulness of the content under consideration.

In two more recent cases, journalists known for their critical reporting on independent online news outlets faced prosecution and high fines in defamation cases lodged by private entities. Some observers saw these as politically motivated and an effort by the authorities to obscure any official connection to the legal harassment.[86] In March 2012, Viktor Krymzalov, an investigative journalist, faced defamation charges for an article published on the news website Centrasia.ru, involving embezzlement allegations related to the eviction of a pensioner.[87] Although the prosecution failed to prove that Krymzalov wrote the article, a court found both him and the pensioner liable for libel and insult.[88] The journalist lost an appeal and was required to pay a fine of 60 times the minimum wage for a total of about US$2,000.[89] The following month, Elena Bondar was found guilty of an administrative offense prohibiting the production, storage, and propagation of materials inciting national, racial, or religious animosity over comments posted to a series of articles about political and social issues on the online outlets Uznews.net and Ferghana.[90] Despite the absence of evidence proving Bondar's authorship of the comments, the journalist was ordered to pay a fine of 100 times the minimum wage (approximately US$3,400). This was the second time within a year that Bondar encountered official harassment. In August 2011, she was detained and interrogated for several hours at the Tashkent airport upon her return from an Organization for Security and Cooperation in Europe (OSCE) training on modern journalism tools in Kyrgyzstan.[91] She was accused of violating customs regulations for not

[85] "Uzbek journalist allowed to leave country," Uznews.net, June 21, 2011, http://www.uznews.net/news_single.php?lng=en&cid=3&sub=&nid=17422.

[86] Alexei Volosevich, "Uzbekistan: New members of the 'persecuted jounralists' club," Ferghana News, May 3, 2012, http://enews.fergananews.com/article.php?id=2751.

[87] "Журналисту Крымзалову добавили еще одну статью" [The Journalist Krymzalov was convicted for an additional offence], Uznews.net, April 5, 2012, http://www.uznews.net/news_single.php?lng=ru&cid=3&nid=19527.

[88] For the text of the article, see, Vladimir Husainov, "Узбекистан в пропасти безнравственности. В канун юбилея независимости суд выкинул старика на улицу" [Uzbekistan in the Abyss of Immorality. On the Eve of the Independence Day a Court Threw Out an Old Man to the Street], Centrasia.ru, August 31, 2011, http://www.centrasia.ru/newsA.php?st=1314800640.

[89] See, Arts. 40 and 41, Administrative Code, *SZ RU* (2005) No. 52, item 384. Compared to the criminal provisions on defamation and insult, the administrative offences are punishable by a fine of up to 20 to 60 times the minimum wage.

[90] Mariya Yanovskaya, "Узбекистан: Журналистке Елене Бондарь «шьют» новое дело" [Uzbekistan: The Authorities "Sew" a New Case Against the Journalist Elena Bondar], Ferghana News, March 30, 2012, http://www.fergananews.com/article.php?id=7324; See court decision in, Mariya Yanovskaya, " Суд над журналисткой Еленой Бондарь: Терминальная стадия узбекского правосудия" [The Trial of the Journalist Elena Bondar: The Terminal Stage of Uzbek Style Justice," Ferghana News, April 20, 2012, http://www.fergananews.com/article.php?id=7345.

[91] "Узбекистан: В ташкентском аэропорту задержана выпускница Академии ОБСЕ и «Немецкой волны» Елена Бондарь" [Uzbekistan: Tashkent airport detained a graduate of the Academy of the OSCE and the "Deutsche Welle" Elena Bondar], Ferghana News, August 22, 2011, http://www.fergananews.com/news.php?id=17166; "Charges Dropped Against Freelance Journalist Elena Bondar," Reporters Without Borders, September 8, 2011, http://en.rsf.org/ouzbekistan-freelance-journalist-elena-bondar-30-08-2011,40844.html.

declaring her media devices (a number of USB drives and CDs), which the NSS subsequently confiscated but later returned with the statement that they "did not find any illegal information."[92]

In another defamation case that received international attention in 2011, the daughter of the president, Lola Karimova, filed a lawsuit against the French news website Rue89 seeking damages for a May 2010 article that referred to her as the daughter of "dictator Karimov" who was "whitewashing Uzbekistan's image" through charity events. The French court dismissed the claim in July 2011.[93]

As of May 2012, two Uzbek online journalists remained in jail on ostensibly fabricated criminal charges. Solidzhon Abdurakhmanov, a reporter for the independent news website Uznews.net, continues to serve a 10-year sentence imposed in October 2008 for allegedly selling drugs. Prior to his arrest, he had reported on human rights, and economic and social issues, including corruption in the Nukus traffic police, which fueled suspicions that the drug charges were trumped-up and in retaliation for his reporting.[94] Dilmurod Saiid, a freelance journalist and human rights activist, is serving a 12 and a half year sentence imposed in July 2009 on extortion charges. Before his detention, he had covered government corruption in Uzbekistan's agricultural sector for local media and independent news websites.[95] No new cases of prison sentences were documented between January 2011 and May 2012.

The authorities have also used various forms of arbitrary detention and intimidation to silence online critics. In November 2011, the government released Jamshid Karimov, an independent journalist and nephew of the president, from a psychiatric hospital where he had been kept against his will since September 2006. Prior to his detention, he regularly published articles on online websites, including about human rights abuses in Uzbekistan. He is widely believed to have been detained in retaliation for his journalistic activity. In January 2012, he suddenly disappeared again and his whereabouts remain unknown as of mid-2012.[96] In another case, Aleksei Volosevich, an Uzbekistan correspondent for the Moscow-

[92] IREX, "Uzbekistan."
[93] "Uzbekistan: Attempt to Silence Criticism Backfires: French Court Case Shines Spotlight on Tashkent's Repression," Human Rights Watch, July 1, 2011, http://www.hrw.org/news/2011/07/01/uzbekistan-attempt-silence-criticism-backfires.
[94] "Government increases pressure on Uzbek journalists," Committee to Protect Journalists, February 17, 2010, http://cpj.org/2010/02/government-increases-pressure-on-uzbek-journalists.php.
[95] "Uzbek appeals court should overturn harsh sentence," Committee to Protect Journalists, September 3, 2009, http://cpj.org/2009/09/uzbek-appeals-court-should-overturn-harsh-sentence.php; See also, "Дождется ли Дильмурад Сайид справедливости?" [Will Dilmurad Saiid receive justice?], Uznews.net, April 2, 2010, http://www.uznews.net/news_single.php?lng=ru&cid=3&nid=13210.
[96] "Jamshid has the rights to live freely!" Human Rights Society of Uzbekistan, January 20, 2012, http://en.hrsu.org/archives/1367; "Uzbekistan: UPDATE – Human rights defender released from forcible detention in psychiatric hospital," Front Line Defenders, November 30, 2011, http://www.frontlinedefenders.org/node/16704.

based news website Ferghana,[97] was interrogated and held without charge in June 2010 for three days after reporting on ethnic violence against Uzbeks in the city of Osh in Kyrgyzstan.[98] The above cases of politically motivated prosecution and harassment have had a chilling effect on freedom of expression in Uzbekistan.

While there have been no reports of government agents physically attacking bloggers or online activists, the National Security Service (NSS) has been known to employ various intimidation tactics to restrict online freedom of expression. For example, in June 2011, there were reports of NSS officers confiscating electronic media devices at the airport, checking browsing histories on travelers' laptops, and interrogating individuals with a record of visiting websites critical of the government.[99]

The space for anonymous online communication in Uzbekistan is steadily shrinking. As mentioned above, the year 2011 saw the closure of Arbuz.com, one of the country's most important online forums for anonymous discussion after the arrest of several users. The site's founder told media that several people who had been active contributors to a forum about Kyrgyz-Uzbek ethnic clashes in 2010 had been detained.[100] According to some reports, the NSS had tracked them through their internet protocol (IP) addresses.[101] Increasingly, few options remain for posting anonymous comments on other online forums—such as Uforum.uz,[102] which is administered by the state-run Uzinfocom Center—as individuals are increasingly encouraged to register with their real names to participate in such discussions.[103] Individuals must also provide a passport to buy a SIM card.[104] There are no explicit limitations on encryption, though in practice, the government strictly regulates the use of such technologies.[105]

[97] "CPJ condemns attack on independent journalist," Committee to Protect Journalists, November 10, 2005, http://cpj.org/2005/11/cpj-condemns-attack-on-independent-journalist.php.
[98] "Andijan police release independent journalist," Committee to Protect Journalists, June 18, 2010, http://cpj.org/2010/06/andijan-police-release-independent-journalist.php.
[99] "Farg'ona aeroportida yo'lovchilar noutbuki tekshirilmoqda" [At the Ferghana Airport, the Laptop Computers of Passengers Are Being Checked], Ozodlik.org, June 2, 2011, http://www.ozodlik.org/content/fargona_aeroportida_yolovchilar_noutbuki_tekshirilmoqda/24212860.html.
[100] "Uzbek chat room closes political topics after government pressure," Uznews.net, Februar 9, 2011, http://www.uznews.net/news_single.php?lng=en&cid=3&sub=&nid=16297.
[101] IWPR "Web Use Spirals in Uzbekistan Despite Curbs," news briefing, January 3, 2012, http://iwpr.net/report-news/web-use-spirals-uzbekistan-despite-curbs.
[102] UForum.uz, "Правила форума" [Terms of Use], at http://uforum.uz/misc.php?do=cfrules.
[103] U.S. Department of State, "Uzbekistan," Counter Reports on Human Righst Practices for 2011, p 16, http://www.state.gov/documents/organization/186693.pdf.
[104] See, e.g., MTC Uzbekistan, "How to subscribe," at http://www.mts.uz/en/join/.
[105] Resolution of the President RU "О мерах по организации криптографической защиты информации в Республике Узбекистан" [On Organizational Measures for Cryptographic Protection of Information in the Republic of Uzbekistan] No. ПП-614, April 3, 2007, *SZ RU* (2007) No 14, item 140, at Art. 1.

Although Article 27 of the Constitution guarantees the secrecy of "written communications and telephone conversations," the government employs systematic surveillance of internet and ICT activities, including the email correspondence of Uzbek political activists and comments in online forums. A 2006 Resolution of the President authorizes the NSS to conduct electronic surveillance of the national telecommunications network by employing a "system for operational investigative measures" (SORM), including for the purposes of preventing terrorism and extremism.[106] The state-owned telecommunications carrier Uztelecom, private ISPs, and mobile phone companies are required to aid the NSS in intercepting citizens' communications and accessing user data. This includes a requirement to install SORM equipment in order to obtain an ISP license.[107] ISPs face possible financial sanctions or license revocation if they fail to design their networks to accommodate electronic interception.

The scope of violations against digital media users' privacy is difficult to evaluate amidst government secrecy and a provision in the Law on Telecommunications that prohibits service providers from disclosing details on surveillance methods.[108] Moreover, there is no independent oversight to guard against abusive surveillance, leaving the NSS wide discretion in its activities.[109] Content intercepted via internet surveillance is admissible as evidence in court.

Since July 2004, cybercafes and other providers of public internet access have been required to monitor their users and cooperate with state bodies, an obligation that is generally enforced.[110] Uzbek security agents stepped up surveillance of cybercafes after violent clashes between ethnic Kyrgyz and Uzbeks took place in Kyrgyzstan during the summer 2010.[111] In March 2012, the president signed a resolution "On measures for the further implementation and development of modern information-communication technologies," which outlines a stage-by-stage plan for the establishment of a national information system integrating the information systems of state bodies as well as individuals between 2012 and 2014.[112] The

[106] Resolution of the President RU "О мерах по повышению эффективности организации оперативно-розыскных мероприятий на сетях телекоммуникаций Республики Узбекистан" [On Measures for Increasing the Effectiveness of Operational and Investigative Actions on the Telecommunications Networks of the Republic of Uzbekistan] No. ПП-513, November 21, 2006, at Preamble and Arts. 2-3.
[107] Ibid., at Art. 5.8. Infra., note 110. Also, tax and custom exemptions apply for import of the SORM equipment by domestic ISPs, see Tax Code of RU, at Arts. 208, 211, 230 part 2, and 269.
[108] Law RU, "On Telecommunications," at Art. 18.
[109] Resolution of the President RU, note 108 above. See, Criminal Procedural Code of RU, *Vedomosti Oliy Mazhlisa RU* (1995) No. 12, item 12, at Art. 339 part 2, "Tasks of Investigation," and Art. 382, "Competences of the Prosecutor." Resolution of the President RU No. ПП-513, note 87 above, at Art. 4.
[110] See note 23 above.
[111] "Attacks on the Press 2010: Uzbekistan," Committee to Protect Journalists, February 15, 2011, http://www.cpj.org/2011/02/attacks-on-the-press-2010-uzbekistan.php.
[112] See Resolution of the President RU "О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий" [On Measures on the Further Impelmentation and Development of

announcement raised concerns that the integrated system might enable greater state surveillance of user activities.

Technical attacks are becoming increasingly common, though not yet widespread. In February 2012, the independent news service Uznews.net reported that it had come under a distributed denial-of-service (DDoS) attack, the first since its founding in 2005. The attack paralyzed the website for several days. The site's editor-in-chief speculated that it was related to a series of articles the online outlet had just published about an assassination attempt against an Uzbek cleric in Sweden.[113] The cleric is known to be a prominent critic of the regime and is wanted in Uzbekistan on charges of alleged religious extremism and terrorism, causing some to believe the attempt was orchestrated by the NSS.[114] Earlier in the month, RFE/RL's Uzbek service reported an apparent phishing attack wherein a mirror of the service's website had been created that included RFE/RL's logo and branding colors. In order to access articles on the mirror website, users had to provide a name, email address, and password, adding to suspicions that the mirror had been created by the security services to identify and track users who were accessing RFE/RL's content, which is otherwise blocked in Uzbekistan.[115]

In addition to the above attacks on independent websites critical of the government, there were reported DDoS attacks against a private ISP and the websites of four government bodies during the summer of 2011.[116] The parliament quickly attributed the attack to forces "outside of the country" but did not provide further details. In 2005, the government established the Computer Emergency Readiness Team (UZ-CERT) as an operational arm of the UzACI dealing with cybercrime.[117] UZ-CERT cooperates with law enforcement bodies to prosecute cybercriminals, and the Criminal Code contains several provisions addressing

Modern Information and Communication Technologies], No. ПП-1730, 21 March 2010, SZRU (2012), 13 (513), item 139, at Annex II.

[113] "Uznews.net server comes under DDoS attack," Uznews.net, March 2, 2012, http://www.uznews.net/news_single.php?nid=19245; "An independent media site dedicated to Uzbekistan under DDoS attack," Ferghana News, March 2, 2012, http://enews.fergananews.com/news.php?id=2215.

[114] "Uzbek assassination plot rocks quiet Swedish town," BBC News, July 26, 2012, http://www.bbc.co.uk/news/world-europe-18998039.

[115] Luke Allnutt, "Attack of the Cloned Websites…This Time in Uzbekistan," Tangled Web (blog), RFE/RL, February 15, 2012, http://www.rferl.org/content/attack_of_the_cloned_websites_this_time_in_uzbekistan/24485124.html.

[116] Catherine A. Fitzpatrick, "Uzbekistan: Government Sites Hacked," Eurasianet.org, August 10, 2011, http://www.eurasianet.org/node/64022; "Хакеры атаковали сайты госорганов Узбекистана" [Hackers Attacked Government Websites in Uzbekistan], UzDaily, July 29, 2011, http://www.uzdaily.uz/articles-id-7654.htm.

[117] Resolution of the President RU "О дополнительных мерах по обеспечению компьютерной безопасности национальных информационно-коммуникационных систем" [On Further Measures Supporting the Maintenance of Information Security of the National Information and Communication Systems], No. 167, September 5, 2005, at Preamble and Arts. 2 and 7.

these issues in a section dedicated to information technology crimes.[118] Nevertheless, there is no publicly available statistical data on the enforcement of sanctions.

[118] Ibid., at Annex II, Art. 8. See, Criminal Code Article 278-1 "Violation of the Rules of Informatization"; Article 278-2 "Illegal (Unsanctioned) Access to Computer Information"; Article 278-3 "Production and Dissemination of Special Tools for Illegal (Unsanctioned) Access to Computer Information"; Article 278-4 "Modification of Computer Information"; and Article 278-5 "Computer Sabotage."

VENEZUELA

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	15	15
Limits on Content (0-35)	13	14
Violations of User Rights (0-40)	18	19
Total (0-100)	**46**	**48**

* 0=most free, 100=least free

POPULATION: 30 million
INTERNET PENETRATION 2011: 40 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Internet access in Venezuela has notably increased over the past decade, though the pace has slowed relative to other countries since the renationalization of the main service provider in 2007. Amidst growing restrictions on broadcast outlets and severe political polarization in the traditional media, new media—especially blogs, the social-networking site Facebook, and the microblogging platform Twitter—have become important spaces for disseminating information and opinions on political and social topics.[1] As government opponents have mobilized via these platforms, the ruling party has increased its efforts in recent years to influence online discussions, while hinting at future attempts to restrict online content.

Venezuelan authorities do not engage in systematic filtering or large-scale arrests of bloggers. Nevertheless, there have been periodic interruptions of access to opposition or independent websites, efforts to intimidate users posting comments critical of the government, and a series of laws passed in December 2010 that lay the foundation for potentially much greater censorship. Perhaps the most disturbing development since then has been a series of hacking attacks on the Twitter accounts of activists and prominent figures in Venezuelan society who had expressed criticism of the government. Beginning in August 2011, dozens of accounts were targeted, with the hackers typically hijacking the accounts and posting messages that would either discredit the opposition or praise the government. Although such activities are illegal under Venezuelan law, no perpetrators had been arrested as of May 2012.

[1] Marcelino Bisbal, *Hegemonía y control comunicacional [Hegemony and Communicational Control]* (Caracas: Editorial Alfa, 2009), 270.

The internet arrived in Venezuela in 1992, but its popularization began in 1996, when the first commercial internet service providers (ISPs) were granted licenses by the National Telecommunications Committee (CONATEL).[2] The 1999 constitution obliges the state to provide the public with access to new information and communication technologies (ICTs),[3] and the 2000 Organic Law of Telecommunications enables private companies to enter the market.[4]

OBSTACLES TO ACCESS

In recent years, partly due to government investment, internet penetration has grown rapidly, increasing from 15 percent in 2006 to over 40 percent—almost 12 million users—at the end of 2011.[5] This figure does not include connections via mobile phones, indicating that penetration may be even higher. There has also been a significant shift from dial-up to broadband. By the end of 2011, over 95 percent of the more than three million internet subscriptions were broadband, and about 40 percent of those were via mobile devices.[6] The majority of upper- and middle-income users access the internet from home, while those from the lowest income brackets are more likely to get online at a cybercafe.

The most substantial obstacles to internet access in Venezuela are lack of service availability, geographic isolation in rural areas, low computer literacy, and the expense of necessary equipment. The cost of access itself is a relatively less significant obstacle.[7] There is a marked digital divide across regions: the Capital District and Miranda State have penetration rates of over 80 percent, while access in poorer states like Amazonas and Apure is about 15 percent.[8] In addition, rural areas have been severely hit by an electricity crisis that has led to rationing in every city but the capital Caracas, also affecting internet connectivity. Regional

[2] United Nations Development Programme (UNDP), *Las Tecnologías de Información y Comunicación al Servicio del Desarrollo* [Information and Communication Technologies for Development] (Caracas: UNDP, 2002), 249.
[3] See Articles 108 and 110 of the constitution, available at http://www.tsj.gov.ve/legislacion/constitucion1999.htm[in Spanish].
[4] In July 2008, a plan to reform the law was leaked to the press. Due to the opposition it garnered, the measure was not introduced in the National Assembly. The proposed modifications included the establishment of a single node for internet service, provided by Conatel, which would have constituted a risk to the neutrality of internet service and management.
[5] Vicepresidencia de la Republica Bolivariana Venezuela [Vice President of the Bolivarian Republic of Venezuela], "Telecommunication Sector Statistics at the end of 2011" [in Spanish], Conatel Comunicaciones, accessed May 26, 2011, http://www.conatel.gob.ve/files/Indicadores/indicadores2011/cierre_2011.pdf; International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[6] Vicepresidencia de la Republica Bolivariana Venezuela [Vice President of the Bolivarian Republic of Venezuela], "Telecommunication Sector Statistics at the end of 2011."
[7] "State of the Internet in Venezuela and its impact on Business" [in Spanish], Tendencias Digitales, November 23, 2011, http://www.redusers.com/noticias/indice-redusers-%C2%BFen-que-pais-de-latinoamerica-es-mas-accesible-la-tecnologia/.
[8] Vicepresidencia de la Republica Bolivariana Venezuela [Vice President of the Bolivarian Republic of Venezuela], "Telecommunication Sector Statistics at the end of 2011."

disparities are evident in the expansion plans of telecommunications companies, who typically focus new investments on the capital and surrounding areas.[9]

Mobile phones are almost ubiquitous, though the penetration rate fell slightly compared to 2010, amounting to 98 percent at the end of 2011.[10] There is a growing contingent of people using BlackBerry devices, reaching 2.7 million by the end of 2011.[11] Although not all BlackBerry users necessarily subscribe to mobile phone data plans, there has been a visible increase in the use of mobile broadband. By the end of 2011, official figures placed the number of subscribers at close to 1.2 million.[12] Mobile phone connections are an attractive alternative to ADSL, but like elsewhere in Latin America, are largely limited to the capital city or high income users.[13]

Despite the growth of broadband internet access, the quality of service is lower than in other countries in the region. The state-owned telecommunications firm National Telephone Company of Venezuela (CANTV) offers relatively low prices, but its connections are slow, and the company's dominant position stifles competition. Nationally, the average connection speed is about 1 Mbps,[14] at a cost of about US$40 per month,[15] compared to an average monthly income of about US$1,000 and a minimum wage of about US$420.[16] CANTV, which was renationalized in 2007, monopolizes ADSL service and controls more than 90 percent of the internet market.[17] The firm has benefited financially from state ownership, particularly with regard to currency controls.[18] There are about two dozen other telecommunications operators in the country, as well as some competition from cable

[9] *Inside Telecom*, 12/19/2912 Vol III No. 95 (Excerpted from weekly and monthly newsletter offered by this company under subscription, not available on the internet.)
[10] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[11] Vicepresidencia de la Republica Bolivariana Venezuela [Vice President of the Bolivarian Republic of Venezuela], "Telecommunication Sector Statistics at the end of 2011."
[12] Ibid.
[13] "Broadband in Latin America 2010/2011 Pool Barometer from Cisco Systems," [in Spanish], Prensario TI Latin America, accessed December 16, 2011, http://www.prensariotila.com/pdf/Informe_Banda_Ancha_0111.pdf.
[14] "Household Download Index," Ookla Net Index, accessed December 12, 2012, http://netindex.com/download/allcountries/; "Speeds of internet connection – Venezuela vs the world" [in Spanish], El Mundo online, April 24, 2012, http://blogs.elmundo.com.ve/Blogs/NEGOCIOS-EN-INTERNET-y-algo-mas----/April-2012/Velocidades-de-Conexion-a-la-Internet-—-Venezuela-.aspx (site discontinued).
[15] Hernan Galperin, "The broadband rates in Latin America and the Caribbean: Benchmarking and trends" [in Spanish], *Dialogo Regional sobre la Sociedad de la Informacion*, accessed December 12, 2011, http://www.dirsi.net/sites/default/files/PB%20tarifas%20banda%20ancha%202011.pdf.
[16] "Gross national income per capita 2011, Atlas method and PPP," World Bank, July 9, 2012, http://databank.worldbank.org/databank/download/GNIPC.pdf.
[17] Roberto Deniz, "Crece el peso del Estado en las telecomunicaciones" [Statements by the Minister of Science, Technology and Intermediate Industries, Jesse Chacón], El Universal, June 8, 2009, http://www.eluniversal.com/2009/06/08/eco_art_crece-el-peso-del-es_1422582.shtml.
[18] Casetel Chamber of Business Telecommunications Services, "Oswaldo Cisneros sigue apostándole a Venezuela: Digitel busca vías para consolidarse en 3G" [Oswaldo Cisneros Still Betting on Venezuela: Digitel Seeks Ways to Consolidate in 3G], Casetel, June 23, 2010, http://www.casetel.org/detalle_noticia.php?id_noticia=509.

modems, mobile broadband, and satellite connections. Inter, the company that places a distant second in the market, offers a triple pack that includes cable television, cable modem and telephony.[19]

Two privately-owned companies provide mobile phone services besides CANTV's Movilnet: Digitel and Movistar. However, they have had to decrease their investments in infrastructure and have begun to ration their services because of the discriminatory currency controls. As a result, according to industry insiders, by the end of 2011, Movilnet lead the mobile phone market with 15.5 million subscribers, out of a total of 29 million. Movistar had almost ten million subscribers and the remainder used Digitel's services.[20] There are no special restrictions on the opening of cybercafes.

Despite the growth in internet and mobile phone use in recent years, development in the ICT sector has slowed overall and, in some respects, slid backwards since 2007 when CANTV was renationalized. The sector's contribution to GDP has declined,[21] and in several recent cross-country studies assessing ICT trends over the past half-decade, Venezuela has been among the countries to have fallen farthest in the rankings relative to its peers.[22] This is in large part due to the difficulties that private providers have had competing with CANTV's rates, and how the lack of competition has reduced incentives for providers to retain a high quality of services.[23]

CANTV's position as a dominant, state-owned ISP and mobile phone provider has also raised concerns about the ease with which systemic content filtering and surveillance could be implemented in the future. In recent years, there have been isolated incidents of CANTV engaging in censorship and monitoring when other providers have not, but more systematic controls were not evident.

---

[19] "Latin American Broadband and Internet Market," BuddeComm Report, accessed December 14, 2011, http://www.budde.com.au/Research/Latin-American-Broadband-and-Internet-Market.html.

[20] Interview with mobile phone company employee who requested to remain anonymous, February 2012.

[21] *Inside Telecom* 7, no. 86 (2011). (Excerpted from weekly and monthly newsletter offered by this company under subscription, not available on the internet.)

[22] For example, in the the World Economic Forum's *Global Report on Information Technology* 2010-2011, assessing the impact of ICTs on development, Venezuela was among the top ten countries with the biggest drops, falling from 83rd (out of 122) in 2006 to 119 (out of 138) in 2011. See, Kai Bucher, "Las Economias Latinoamericanas todavia estan atrasadas en el Aprovechamiento de las Tecnologias de la Informacion…" [The Latin American Economies are still behind in the use of Information Technologies], World Economic Forum, accessed December 12, 2011, http://www.weforum.org/news/las-econom%C3%ADas-latinoamericanas-todav%C3%ADa-est%C3%A1n-atrasadas-en-el-aprovechamiento-de-las-tecnolog%C3%ADas?fo=1. Venezuela also dropped several spots in the ITU's 2011 Measuring the Information Society (2011) índex. See, International Telecommunication Union, *Measuring the Information Society 2011* (Geneva: International Telecommunication Union, 2011), http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf.

[23] Jorge Espinoza, "Argumentos in situ de las operadoras móviles privadas: Smartphones e Internet móvil suplen carencias fijas" [Topics on private mobile operators: Smartphones and Mobile Internet still have supplement gaps], Inside Telecom, May 25, 2012, http://m.insidetele.com/index.php?article_id=3563838343945133547.

The state acts as both the dominant service provider, through CANTV, and the sector's regulator and licensing authority, through CONATEL. The president has the power to name and remove CONATEL's director and the four members of its Directive Council. Although Article 35 of the Organic Law of Telecommunications provides for CONATEL's operational and administrative autonomy, a series of presidential decrees over the past decade has shifted oversight of the commission to various ministries and finally to the vice president,[24] which has increased the agency's politicization.[25] CONATEL continued in 2011 to demonstrate progovernment bias in decisions related to broadcast media, but it has not yet made comparable judgments affecting internet or mobile phone service.

LIMITS ON CONTENT

In March 2010, President Hugo Chavez declared that the internet could not be "a free thing where you do and say whatever you want."[26] Despite such warnings, the Venezuelan authorities have not engaged in systematic filtering to block citizens' access to information. Chavez and the ruling party have instead used social media to proactively disseminate their views and counter opponents. This trend has intensified since early 2011, as Chavez and his supporters have sought to gain the upper hand in a medium heavily used by the political opposition, sometimes doing so openly and on equal footing, but at times also using nontransparent, manipulative tactics.

No systematic blocking or cases of judicially imposed censorship have been reported in Venezuela. The sites of international news sources and human rights organizations like Freedom House, Reporters Without Borders, and Amnesty International are freely available. Advanced applications such as Facebook, Twitter, and the video-sharing site YouTube are also freely accessible and growing in popularity.[27]

Nonetheless, since the renationalization of CANTV in 2007, there have been sporadic incidents of blocks linked to sensitive political information. For example, in the run-up to parliamentary elections in September 2010, the news-aggregator site Noticiero Digital, one of the country's most popular websites at the time, was temporarily inaccessible from

[24] Andrés Cañizález, "Conatel, La joya de la corona" [Conatel, the Jewel in the Crown], Tal Cual, August 9, 2010, http://www.talcualdigital.com/Blogs/Viewer.aspx?id=38920.
[25] Jesús Urbina Serjant, "Venezuela," Las mordazas invisibles: Nuevas y viejas barreras a la diversidad en la radiodifusión [Invisible Jaws: New and Old Barriers to Diversity in Broadcasting], 2009, http://legislaciones.amarc.org/mordazas/VEN_pais.htm
[26] "Chavez: Hay que actuar contra Noticiero Digital (y Globovision)" [Chavez speaking about the Internet], YouTube video, 8:44, posted by "cadvsm," March 13, 2010, http://youtu.be/3f0kCyUZhHI.
[27] "Top Sites in Venezuela," Alexa Web Information Company, accessed July 10, 2012, http://www.alexa.com/topsites/countries;0/VE.

Venezuela for customers of CANTV.[28] Similarly, international blog-hosting services have occasionally been subject to brief blocks surrounding politically sensitive events, such as during the February 2009 constitutional referendum and the September 2010 parliamentary elections.[29] Sporadic disruptions continued to be recorded during 2011, with media reporting in August that bloggers had been complaining for weeks of problems accessing Google's Blogger platform via CANTV internet connections.[30]

Neither the government nor CANTV have made any effort to clarify the causes of these disruptions. The lack of clarity on whether the government is responsible for these cases of apparent blocking is compounded by the political situation in the country, in which there are no established checks and balances between the different branches of government, and the judiciary lacks independence. In this context, there is no transparent process or independent institutions through which website owners and content producers can pursue complaints of disruptions.

In December 2010, the National Assembly adopted a reform of the 2004 Law of Social Responsibility in Radio and Television (Resorte) that extended it to online and electronic media.[31] This laid the groundwork for censorship by websites and service providers of content transmitted by other users. Under the amended law, online media outlets are expected to establish mechanisms to restrict content that would violate the law, according to the Committee to Protect Journalists. Websites found in violation may be fined up to 13,000 bolivars (US$3,000) and service providers who do not respond to government inquiries risk high fines and temporary suspension of operations.[32] In practice, however, the authorities have not vigorously enforced the law and online content providers do not appear to be engaging in politically-motivated deletions of user comments.

Rather than engaging in significant censorship, the president and other government representatives are making substantial use of social media, seeking to dominate online discussions. In April 2010, Chavez opened his own Twitter account. By May 2012, he had

[28] David Sasaki, "Internet Censorship and Freedom of Expression in Latin America," Información Civica, November 1, 2010, http://informacioncivica.info/new/internet-censorship-and-freedom-of-expression-in-latin-america/; Noticiero Digital, "Carta abierta a Cantv, de parte de Noticiero Digital" [Open Letter to Cantv, from Noticiero Digital], news release, September 28, 2010, http://www.noticierodigital.com/forum/viewtopic.php?t=696877.

[29] "Chavez y CANTV bloquean Blogger y Blogspot ayer en Venezuela" [Chavez blocked CANTV Blogger and Blogspot Yesterday in Venezuela], CristaLab (blog), February 16, 2009, http://www.cristalab.com/blog/chavez-y-cantv-bloquean-blogger-y-blogspot-ayer-en-venezuela-c68770l/; David Sasaki, "Internet Censorship and Freedom of Expression in Latin America."

[30] Andres Tovar, "Blogueros reportan problemas con CANTV" [Bloggers report problems with CANTV], Ultimas Noticias, August 20, 2011, http://www.ultimasnoticias.com.ve/noticias/tecnologia/blogueros-denuncian-problemas-con-cantv.aspx.

[31] "The Law of Social Responsibility in Radio, Television and Electronic Media" [in Spanish] (Copy of Government Document), Scribd, accessed December 19, 2010, http://www.scribd.com/doc/45291089/Proyecto-de-Ley-de-Responsabilidad-en-Radio-Television-y-Medios-Electronicos.

[32] International Freedom of Expression eXchange (IFEX), "CPJ Condemns Two Media Laws," news release, December 22, 2010, http://www.ifex.org/venezuela/2010/12/22/two_reforms_approved/.

the largest number of followers for any Venezuelan with over 2.8 million.[33] The president's use of Twitter increased and took on greater importance after he began receiving treatments for cancer in Cuba in mid-2011 and was unable to make public appearances in Venezuela.[34] More broadly, the ruling party and its supporters have created pro-Chavez platforms, such as the website www.aporrea.org, launched in 2002, or the Twitter feed "@RedVergataria." The latter was launched in October 2011 with the support of CANTV's Movilnet and the Ministry of Popular Power for Science and Technology;[35] its declared aim is to achieve Chavez's reelection in presidential polls scheduled for October 2012.[36] Members of the public have also occasionally complained of the ruling party using state resources and programs to promote a partisan ideology via ICTs.[37]

More significant for the atmosphere of free online debate on political and social issues have been various efforts of the ruling party or its supporters to manipulate online conversations, discredit opposition voices, and encourage self-censorship. Allegations have surfaced of the government attempting to influence online news coverage by manipulating the allocation of advertising. Online media outlets critical of the government do not receive advertising revenue from state agencies and some private advertisers have been pressured to withdraw their funding from outlets like Noticiero Digital and Codigo Venezuela.[38]

---

[33] Leff, A. "Does Chavez govern by twitter?" Globalpost, May 4, 2012, http://www.globalpost.com/dispatches/globalpost-blogs/chatter/hugo-chavez-twitter-government (site discontinued).

[34] Ezequiel Minyaya, & Kejal Vyas, "When chávez tweets, venezuelans listen," The Wall Street Journal, April 25, 2012, http://online.wsj.com/article/SB10001424052702303990604577366123856023452.html.

[35] Red Vergataria (blog), accessed December 14, 2011, http://www.redvergataria.com/.

[36] Anais Lucena, "Lanzamiento de red social "vergataria" en twitter se efectuó desde el Zulia" [Launch of social networking 'Vergataria' on Twitter was made from Zulia State], Radio Mundial, October, 27, 2011, http://www.radiomundial.com.ve/article/lanzamiento-de-red-social-"vergataria"-en-twitter-se-efectuó-desde-el-zulia; "Colectivos de telecomunicaciones lanzan @redvergataria para organizacion politica" [Collective @redvergataria telecommunications to throw political organization], Patria Grande, October 10, 2011, http://www.patriagrande.com.ve/temas/politica/colectivos-telecomunicaciones-lanzan-redvergataria-organizacion-politica/.

[37] For example, on Christmas Eve 2011, a text message in Chavez's name was sent to more than 27 million mobile phone subscribers, encouraging people to celebrate, "our unstoppable march towards a Good and Pretty Country." Although there are no laws restricting such communications, critics complained that it was an abuse of power to force mobile phone companies to disseminate partisan propaganda. In another case, the Canaima Education project, under which the government committed to supply over one million laptops to elementary school children, came under criticism in 2011. Critics claimed that on the computers—over 700,000 of which had already been distributed by October 2011— the section dedicated to parents contained content directed at promoting the political ideology and image of the president, though the materials for children were not so blatantly politicized. See, "Hugo Chavez' Christmas Spam to all Venezuelans," Devils Excrement (blog), December 27, 2011, http://devilsexcrement.com/2011/12/27/hugo-chavez-christmas-spam-to-all-venezuelans/; "Telefonicas asumieron costo del mensajito navideno presidencial" [Assumed cost of Presidential Christmas Phone Message], Noticiero Digital, December 28, 2011, http://www.noticierodigital.com/2011/12/telefonicas-asumieron-costo-del-mensajito-navideno-presidencial/; "Venezuela ensamblará 500 mil computadoras para proyecto educativo" [Venezuela will join 500 000 computers for educational Project] Canaima Educativo, October 4, 2011, http://www.canaimaeducativo.gob.ve/index.php?option=com_content&view=article&id=193:venezuela-ensamblara-500-mil-computadoras-para-proyecto-educativo&catid=50:noticias-2011&Itemid=59; Ariana Guevara Gomez, "Las Canaima inculcan el socialismo" [Canaimas instill socialism], Reportero 24, September 23, 2011, http://www.reportero24.com/2011/09/ideologizacion-las-canaimitas-fomentan-el-culto-a-la-figura-del-lider/.

[38] Interviews with employees of the two websites, who requested to remain anonymous, October 2011.

Venezuelans are avid users of digital media, which have emerged as an important avenue for circulating information and expressing opinions at a time when independent television and radio stations have come under increased pressure. During 2011, over 90 million text messages were sent,[39] and approximately three-quarters of internet users have visited YouTube.[40] The country has the fifth-largest number of Facebook users in Latin America (about 9.5 million as of April 2012)[41] and the second-largest number of Twitter users (some estimates place the total at over two million as of July 2011).[42]

Beginning in late August 2011, the blogs and Twitter accounts of at least two dozen government critics and prominent figures in Venezuelan society were hacked, hijacked, and used to disseminate progovernment messages. Among those targeted in waves of attacks in late 2011 and early 2012 were journalists, artists, economists, activists, and opposition politicians, including the Miranda State governor and presidential candidate Henrique Capriles Radonski.[43] In some cases, the pro-government nature of the impersonated messages was palpable and immediately raised suspicions that a particular account had been compromised. But in many other instances, the hackers' approach was more cunning. Pro-government statements published were subtly convincing, while other comments produced negative impressions of the poster. Examples included a statement by the usually critical economist Jose Guerra suddenly praising the president's price control policy,[44] supposed criticism by the opposition-linked pollster Luis Vicente Leon regarding one of the opposition's own presidential candidates, and threatening comments seemingly from political activist Luis Trincado towards other users.[45] Email accounts associated with

[39] Vicepresidencia de la Republica Bolivariana Venezuela [Vice President of the Bolivarian Republic of Venezuela], "Telecommunication Sector Statistics at the end of 2011."
[40] Carlos Jiménez, "Medios sociales: Venezuela en el mundo" [Social Media: Venezuela in the World], El Universal, July 22, 2011, http://www.eluniversal.com/2011/07/22/medios-sociales-venezuela-en-el-mundo.shtml.
[41] "Venezuela Facebook Statistics," SocialBakers, accessed May 25, 2012, http://www.socialbakers.com/countries/detail/venezuela.
[42] Carlos Jiménez, "Medios sociales: Venezuela en el mundo" [Social Media: Venezuela in the World], El Universal, July 22, 2011, http://www.eluniversal.com/2011/07/22/medios-sociales-venezuela-en-el-mundo.shtml.
[43] Adriana Prado, "Pro-chavez hackers steal twitter passwords from venezuelan journalists," Knight Center for Journalism in the Americas, September 13, 2011, http://knightcenter.utexas.edu/blog/pro-chavez-hackers-steal-twitter-passwords-venezuelan-journalists; Natalia Mazotte, "More venezuelan opposition journalists' twitter accounts hacked" Knight Center for Journalism in the Americas, February 1, 2011, http://knightcenter.utexas.edu/blog/more-venezuelan-opposition-journalists-twiiter-accounts-hacked-after-publishing-critical-report; "Hackean la página web de la gobernación de Miranda" [Hacked the website of the governorship of Miranda], La Patilla, February 12, 2012, http://www.lapatilla.com/site/2012/02/12/hackean-la-pagina-web-de-la-gobernacion-de-miranda/.
[44] "Continuan los ataques informaticos en Twitter y Gmail" [Continuing attacks on Twitter and Gmail], Espacio Publico, November 25, 2011, http://espaciopublico.org/index.php/noticias/1-libertad-de-expresi/1163-continuan-los-ataques-informaticos-en-twitter-y-gmail?utm_source=dlvr.it&utm_medium=twitter.
[45] Francisco Toro, "Hack a Mole," The New York Times, November 28, 2011, http://latitude.blogs.nytimes.com/2011/11/28/hack-a-mole/.

activists' Twitter feeds or blogs have also been compromised, and at least one blogger had the contents of his blog erased.[46]

Whether the government is directly behind these attacks remains unclear. On the one hand, a group of hackers calling itself N33 has taken responsibility for the attacks, claiming they support the president but are not acting at the behest of the government.[47] On the other hand, one victim of hacking, Milagros Socorro (editor of the opposition news site Codigo Venezuela), received an email from an anonymous sympathizer who claimed to work at the Ministry of Science and Technology and reported that an entire floor of the ministry was devoted to following and hacking opposition activists' online communications; the allegation remains unconfirmed, however.[48] More concretely, police and prosecutors have not investigated victims' complaints and some N33 statements have been aired on state-run television (see "Violations of User Rights"). Taken together, these circumstances have led many observers to believe that the president or other top officials are either directly or implicitly supporting the attackers.

In February 2012, online activists took matters into their own hands in response to the Twitter hackings, launching what they called Operation BAS (short for Operation Block and Spam).[49] The effort entailed marking as "blocked" or "spam" tweets coming from compromised accounts or feeds belonging to suspected paid government commentators. The activists also filed complaints with Twitter that such accounts had violated the company's terms of service. Estimates vary on the number of accounts suspended as a result of the campaign, but at least several dozen seem to have been affected. Observers noted that among the targeted accounts were also ones belonging to genuine Chavez supporters, not paid commentators, and that the campaign thus posed a restriction on their freedom of expression.[50]

[46] "Continuan los ataques informaticos en Twitter y Gmail" [Continuing attacks on Twitter and Gmail], Espacio Publico, November 25, 2011, http://espaciopublico.org/index.php/noticias/1-libertad-de-expresi/1163-continuan-los-ataques-informaticos-en-twitter-y-gmail?utm_source=dlvr.it&utm_medium=twitter.;
Fernando Nunez Noda, "Hackeo de cuentas o Vietnam cibernetico?" [Hacking of stories or Vietnam cyberspace?], Info Ciudadano Revista Colaborativa, September 13, 2011, http://www.infociudadano.com/2011/09/13/hackeo-de-cuentas-o-vietnam-cibernetico-i/

[47] Laura Vidal, "Venezuela: Government opponents' twitter accounts hacked" Global Voices Online (blog), December 5, 2011, http://globalvoicesonline.org/2011/12/06/venezuela-government-opponents-twitter-accounts-hacked/.

[48] Francisco Toro, "Hack a Mole," The New York Times, November 28, 2011, http://latitude.blogs.nytimes.com/2011/11/28/hack-a-mole/.

[49] "Operación BAS ha suspendido un centenar de usuarios que violan las normas de Twitter" [BAS operation has suspended one hundred users who violate the rules of Twitter], 6toPoder, March 11, 2012, http://www.6topoder.com/2012/03/11/operacion-bas-ha-suspendido-un-centenar-de-usuarios-que-violan-las-normas-de-twitter-investigacion/.

[50] Luis Carlos Díaz, "El descubrimiento de la multitud" [The discovery of many], Periodismo de paz (blog), April 3, 2012, http://www.periodismodepaz.org/index.php/2012/03/04/el-descubrimiento-de-la-multitud/.

Apart from such online campaigns, there were no notable examples of social media being used to mobilize large-scale offline protests between early 2011 and mid-2012.[51] For example, neither primary elections in February 2012 nor a new controversial labor law stirred concerted efforts to mobilize protests via social media, though many Twitter users voiced their own individual views, often critical of the government. Still, academic studies have noted a correlation between the consumption of digital media and political participation in Venezuela and so, these tools may play an increasingly important role in the run-up to presidential elections in October 2012.[52]

VIOLATIONS OF USER RIGHTS

Freedoms of speech and the press are constitutionally guaranteed, and the 1999 constitution establishes an obligation on the state to provide public access to ICTs.[53] However, various laws and decrees have been used to restrict media and online freedom or otherwise undermine these commitments. Meanwhile, the lack of institutional checks and balances and the market dominance of state-owned CANTV open the possibility for the government to monitor or harass political opponents with impunity.

In addition to passing the Resorte Law, in December 2010, legislators also amended the Telecommunications Act that deemed telecommunications networks and services to be of public rather than general interest, meaning they would be subject to greater state control.[54] These changes were among more than a dozen laws passed in the final days of the outgoing National Assembly, which was set to be replaced by a newly elected chamber with a substantial opposition presence.[55] The assembly also delegated its powers to the president for 18 months, allowing him to legislate by decree in areas including ICTs.[56] When freedom of expression advocates demanded to participate in the lawmakers' deliberations,[57] they were harassed and assaulted by government supporters at the doors of the chamber.[58]

[51] A. Artigas et al., "Caracterizando las elecciones venezolanas a través de Twitter. Caso: #26s" [Characterizing Venezuelan elections through Twitter. Case: #26s], *Anuario Electrónico de Estudios en Comunicación Social Disertaciones*, (2012): 5(1).
[52] I. Puyosa, "Conectados versus mediáticos ¿Politizados o Despolitizados?" [Conected vs broadcast media consumers: politicized or depoliticized?], *Anuario Electrónico de Estudios en Comunicación Social "Disertaciones,* (2012): 5(1).
[53] Asamblea Nacional Constituyente, *Constitution* [in Spanish], March 24, 2000, 108:110, http://www.tsj.gov.ve/legislacion/constitucion1999.htm.
[54] "Ley Organica de Telecomunicaciones" [Law of Organic Telecommunications], (Copy of Government Document), Scribd, accessed December 19, 2010, http://www.scribd.com/doc/45293016/Nueva-Ley-Organica-de-Telecomunicaciones.
[55] Sara Carolina Díaz, "En 15 días Asamblea aprobó 16 leyes" [In 15 Days Assembly Approves 16 Laws], El Universal, December 19, 2010, http://politica.eluniversal.com/2010/12/19/pol_art_en-15-dias-asamblea_2141341.shtml.
[56] "Texto de la Ley Habilitante entregada al la AN" [Text of the Enabling Act Submitted to the National Assembly], Panorama.com.ve, December 14, 2010, http://www.panorama.com.ve/14-12-2010/avances/0chavez-martes-emergencia2.html.
[57] "Periodistas y ONG solicitan audiencia a la AN para defender la libertad de expresión" [Journalists and NGOs Seek Hearing at the National Assembly to Defend Freedom of Expression], El Nacional, December 16, 2010, http://www.el-nacional.com/www/site/p_contenido.php?q=nodo/172357/Naci%C3%B3n/Periodistas-y-ONG-solicitan-audiencia-a-la-AN-

The courts are subject to the influence of the executive branch, particularly with regards to politically important cases, and the Supreme Court of Justice has passed down at least ten judgments since 2001 that have placed curbs on freedom of expression.[59] A 2005 reform of the penal code included significant restrictions on expression, especially in cases involving contempt or disrespect. Article 147 of the penal code stipulates that defamation of the president is punishable by 6 to 30 months in prison, while offenses against lower-ranking officials carry lighter punishments under Article 148.[60] In addition, the penal code includes vague language criminalizing the dissemination of "false information," punishable by two to five years in prison.[61] Given that the internet is classified as a channel of mass distribution of information, some violations of the penal code (such as defamation or incitement of hatred or rebellion) may be considered more severe online than in other media forms.[62]

Although in past years, Twitter users and citizen journalists were detained for their online communications, no such cases were recorded in 2011 and early 2012. Nevertheless, the above laws were used during this period to prosecute and imprison traditional media journalists and government opponents, indicating that the risk of prosecution for online activists remains.

The constitution prohibits anonymity, and the rule applies to all media.[63] Since 2005, CONATEL has required mobile phone operators to collect copies of their subscribers' identity documents, address, fingerprints, and signature.[64] According to the Computer Crimes Act, this information must be delivered to state security agencies upon presentation of a judicial warrant. Service providers are also obliged to keep detailed logs of all calls,

para-defender-la-libertad-de-expresi%C3%B3n; "Esperamos respuesta oportuna de AN a documento Por una internet de contenido libre" [We Expect a Timely Response from the National Assembly to Document 'For an Internet of Free Content'], Todos en Red (blog), December 17, 2010, http://todosenred.wordpress.com/2010/12/17/esperamos-respuesta-oportuna-de-an-a-documento-por-una-internet-de-contenido-libre/.

[58] Patty Fuentes Gimón, "Respuesta oficial" [Official Response], Tal Cual, December 17, 2010, http://www.talcualdigital.com/Avances/Viewer.aspx?id=45795&secid=28.

[59] Juan Francisco Alonso, "'Jueces buscan limitar libre expresión'" ['Judges Seek to Limit Free Expression'], El Universal, August 21, 2010, http://politica.eluniversal.com/2010/08/21/pol_art_jueces-buscan-limit_2012844.shtml.

[60] "Respeto a la libertad de expresión: ¿Limita el código penal la libertad de expresión?" [Respect for Freedom of Expression: Does the Penal Code Limit Freedom of Expression?], Sumate, accessed August 22, 2010, http://infovenezuela.org/democracy/cap4_es_2.htm.

[61] "Summary of the National Assembly" [in Spanish], Gaceta Oficial [Official Gazette] no. 5.763 Extraordinario, March 16, 2005, http://www.tsj.gov.ve/gaceta_ext/marzo/160305/160305-5763-01.html.

[62] Rafael Martínez, "Twitter: Esos Malditos 140 Caracteres" [Twitter: Those Damned 140 Characters], SoyRafael.com (blog), February 22, 1010, http://soyrafael.com/2010/02/22/twitter-esos-malditos-140-caracteres/. (Article 285 of the penal code states: "Anyone who incites disobedience of the laws or hatred among its people or makes apology for acts that the law provides as crimes, so as to endanger the public peace, shall be punished with imprisonment of three years to six years.")

[63] Article 57: "Everyone has the right to freely express their thoughts, ideas or opinions orally, in writing or any other form of expression, and to make use of any means of communication and diffusion, and no censorship shall be established. Anyone making use of this right assumes full responsibility for everything expressed. Anonymity, war propaganda, discriminatory messages or those promoting religious intolerance are not allowed."

[64] Gaceta Oficial [Official Gazette] no. 38.157, April 1, 2005, http://www.tsj.gov.ve/gaceta/abril/010405/010405-38157-20.html.

including the phone number of the caller, the destination phone number, the date, time, and duration of the call, the location and direction of the base station where the call is initiated, and the location and direction of the base station where the call is received, provided it belongs to the same network. The Law Against Kidnapping and Extortion obliges the providers of telecommunications, banking, or financial services to supply data to prosecutors upon presentation of a judicial warrant. In practice, given the lack of judicial independence, there are few safeguards in place to limit security agencies' access to user data and private communications. Nonetheless, National Assembly deputies from the ruling party have reported receiving complaints from law enforcement agencies that only the state-owned Movilnet provides information immediately.[65] Cybercafe customers are not required to register their identity documents to gain internet access, and there are no known cases in which such users' activities have been tracked.

The full scale of surveillance of user communications remains unclear. However, on occasion, state representatives have signalled the government's ability to track Twitter users. In February 2011, when official news agencies were slow to release information about a fire on the premises of the Compañía Anonima Venezolana Military Industries (Cavim), people began to share details about the incident over social networks, especially Twitter. A military commander subsequently warned that it was "technologically feasible" for the state to track down the origin of those messages and take action against those who had committed the crime of generating public anxiety; no arrests were made at the time, however.[66]

The 2001 Special Law against Information Crimes[67] and the 1991 Communications Privacy Protection Law safeguard the privacy, confidentiality, inviolability and secrecy of communications and impose prison terms of up to six years on those who illegally intercept others' communications.[68] However, over the past year and a half, there have been numerous incidents of government opponents' communications being hacked, recorded, or manipulated with impunity. The fruits of these actions have been published in state-run media, indicating there may have been government involvement.[69] For example, in

[65] "Presionan a brindar información personal" [Pressure to Provide Personal Information], BlackBerryVzla.com, June 24, 2010, http://www.blackberryvzla.com/2010/06/presionan-brindar-informacion-personal.html.
[66] "Sebin y DIM investigarán mensajes de Twitter sobre caso Cavim" [Sebin and investigate DIM case Twitter messages on Cavim], Espacio Publico, February 2, 2011, http://espaciopublico.org/index.php/noticias/1-libertad-de-expresi/963-sebin-y-dim-investigaran-mensajes-de-twitter-sobre-caso-cavim.
[67] The National Assembly, *Special Law Against Cybercrime* [in Spanish], accessed December 12, 2011, http://www.tsj.gov.ve/legislacion/ledi.htm.
[68] Ibid.
[69] Gregorio Salazar, "Under chávez: Media harassed with online hacking, phone tapping and censorship," Sampsonia Way, January 23, 2012, http://www.sampsoniaway.org/bi-monthly/2012/01/23/under-chavez-media-harassed-with-online-hacking-phone-tapping-and-censorship/2/.

November 2011, a mobile phone conversation between opposition presidential candidate María Corina Machado and her mother was intercepted and aired on state-run television.[70]

Meanwhile, as noted above, beginning in August 2011, a wave of hacking and impersonation attacks struck the Twitter accounts of government critics. Some websites have also faced hacking attacks. In October 2011, the news portal La Patilla, ranked as the 16th most visited website in Venezuela, reported being the target of an intense hacking attack, but successfully fending it off.[71] A few weeks earlier, the N33 hacking group, which claimed responsibility for other attacks, had named the site's editor Alberto Federico Ravel as an important future target.[72]

Several victims filed complaints with the competent bodies, calling for an investigation. Nevertheless, as of May 2012, state bodies had not properly investigated the source of the attacks nor had the government publicly condemned them. On the contrary, a statement by the N33 hacking group was transmitted via a state-run television channel during a popular show hosted by a ruling party spokesman. In the statement, the hackers declared that the attacks' purpose was to silence those expressing opinions contrary to those of the government.[73] In December 2011, several prominent figures whose accounts had been hacked held a press conference and published an open letter denouncing the attacks as part of a policy of "computer terrorism" endorsed by the government.[74] They complained that although the Committee for Scientific, Penal and Criminal Investigations (CICPC) had successfully identified several perpetrators, the investigation was halted and the lead investigator was relieved of his duties.[75]

[70] "María Machado denunció grabación ilegal en fiscalía" [Maria Machado denounced illegal recording in Office], El Universal, November 29, 2011, http://www.eluniversal.com/nacional-y-politica/111129/maria-machado-denuncio-grabacion-ilegal-en-fiscalia; Edgar Lopez, "Vtv involucra al estado en grabaciones ilegales" [VTV involves the state in ilegal recordings], El Nacional, December 5, 2011, http://movil.el-nacional.com/n.php?id=12743.

[71] "La patilla informa a sus lectores sobre ataque a su plataforma" [La Patilla informs its readers about your platform attack], La Patilla, October 1, 2011, http://www.lapatilla.com/site/2011/10/01/la-patilla-informa-a-sus-lectores-sobre-ataque-a-su-plataforma/.

[72] Adriana Prado, "Pro-chavez hackers steal twitter passwords from venezuelan journalists," Knight Center for Journalism in the Americas, September 13, 2011, http://knightcenter.utexas.edu/blog/pro-chavez-hackers-steal-twitter-passwords-venezuelan-journalists; Juan Carlos Figueroa, "Hacker del n33 advierte: La joya de la corona es alberto ravell" [Hacker warns of N33: The jewel in the Crown is Alberto Ravell], El Tiempo, September 7, 2011, http://eltiempo.com.ve/venezuela/entrevista/hacker-del-n33-advierte-la-joya-de-la-corona-es-alberto-ravell/31259.

[73] "Grupo Hacker #N33 se pronuncia y se atribuye hackeos a cuentas de personajes conocidos en twitter-Venezuela" [Hacker Group # N33 attributed the attack of accounts of famous people on twitter-Venezuela], Redpres News Release, September 2, 2011, http://redpres.forolatin.com/t1648-grupo-hacker-n33-se-pronuncia-y-se-atribuye-hackeos-a-cuentas-de-personajes-conocidos-en-twitter-venezuela.

[74] "Hackeados e indiganados denunciaron el terrorismo informatico" [People being hacked denounced computer terrorism], Liderazgo y Vision Asociacion Civil, December 2, 2011, http://www.liderazgoyvision.org/2011/12/02/hackeados-e-indignados-denunciaron-el-terrorismo-informatico/.

[75] "Denuncian 'terrorismo informatico' impulsado por el gobierno de Chavez" [Denounce "computer terrorism" driven by the Chavez government], Globovision, December 2, 2011, http://www.globovision.com/news.php?nid=210517.

Online activists have also been subject to physical intimidation and attacks. The offices of Espacio Publico, one of the civil society groups most active in defending freedom of expression online, were burglarized twice in November 2011.[76] Although there was no evidence that government actors were behind the thefts, the group has repeatedly been the target of discrediting campaigns in state-run media and the authorities' slow investigation, despite the availability of security camera footage, raised suspicions that these were not random acts of violence.[77] Several days after the second attack, a respected journalist known for teaching cyber activism workshops throughout the country began receiving anonymous threats over the phone and to his Twitter account.[78]

[76] Natalia Mazotte, "Back-to-back robberies, slow state response suspicious, says Venezuelan freedom of expression NGO," Knight Center for Journalism in the Americas, November 30, 2011, http://knightcenter.utexas.edu/en/blog/back-back-robberies-slow-state-response-suspicious-says-venezuelan-freedom-expression-ngo; International Freedom of Expression eXchange (IFEX), "Freedom of expression NGO robbed," news release, November 23, 2011, http://www.ifex.org/venezuela/2011/11/23/espacio_publico_robbery/.

[77] "Venezuela debe terminar con la campana contra prestigioso defensor de derechos humanos" [Venezuela must end with the campaign against prestigious human rights defender], Human Rights Watch, August 19, 2010, http://www.hrw.org/news/2010/08/19/venezuela-debe-terminar-con-la-campa-contra-prestigioso-defensor-de-derechos-humanos; International Freedom of Expression eXchange (IFEX), "Authorities drag heels in investigation of two burglaries at offices of free speech NGO," news release, December 5, 2011, http://www.ifex.org/venezuela/2011/12/05/second_robbery/; "Roban por segunda vez sede de Espacio Publico" [Stolen a second time headquarters of Public Space], El Universal, November 26, 2011, http://www.eluniversal.com/caracas/sucesos/111126/roban-por-segunda-vez-sede-de-espacio-publico.

[78] Natalia Mazotte, "Twitter becoming a common way to threaten journalists in Venezuela," Knight Center for Journalism in the Americas, November 28, 2011, http://knightcenter.utexas.edu/en/blog/twitter-becoming-common-way-threaten-journalists-venezuela; Natalia Mazotte, "Online Attacks Against Reporters in Venezuela become latest form of censorship (Interview)," Knight Center for Journalism in the Americas, January 18, 2012, http://knightcenter.utexas.edu/en/blog/online-attacks-against-reporters-venezuela-become-latest-form-censorship-interview.

VIETNAM

	2011	2012
INTERNET FREEDOM STATUS	**Not Free**	**Not Free**
Obstacles to Access (0-25)	16	16
Limits on Content (0-35)	25	26
Violations of User Rights (0-40)	32	31
Total (0-100)	**73**	**73**

* 0=most free, 100=least free

POPULATION: 89 million
INTERNET PENETRATION 2011: 35 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Internet usage in Vietnam has continued to grow steadily, thanks to decreasing costs and the improvement of electricity and telecommunications networks. Nevertheless, since the medium's introduction in 1997, the ruling Vietnamese Communist Party (VCP) has demonstrated concern that the internet could be used to challenge its monopoly on political power, leading to contradictory policies designed to support or suppress online activities.

On the one hand, the government has invested in expanding citizens' access to information and communication technologies (ICTs), as seen in the so-called Taking-Off Strategy 2011–2020,[1] which aims to raise Vietnam's ICT sector to the level of its regional neighbors. On the other hand, the government has intensified its efforts to monitor and censor online content. After a relative easing of repression from 2004 to 2006 as Vietnam prepared to host an Asia-Pacific Economic Cooperation summit and join the World Trade Organization, the environment for free expression has deteriorated, and a growing number of online activists have faced arrest, harassment, and imprisonment.

The space for free expression tightened even further in the months leading to the Communist Party Congress in January 2011, and contrary to expectations that the situation would relax after the Congress, it remained harsh over the year. In 2011, at least nine journalists who primarily work online were jailed—a big jump from only five jailed journalists at the end of 2010—making Vietnam one of the worst jailers of journalists in the

[1] "'Taking-off Strategy,' Does it stepping up the development of the ICT industry in Vietnam?," Business-in-Asia.com, accessed June 22, 2012, http://www.business-in-asia.com/vietnam/vietnam_ict.html.

world.[2] Cyberattacks on websites critical of the government that began in late 2009 continued throughout 2011, highlighting an additional threat to internet freedom both within and beyond Vietnam's borders.

OBSTACLES TO ACCESS

Vietnam's internet penetration rate has grown dramatically over the past decade, from 0.3 percent in 2000 to about 35 percent (with 30 million users) at the end of 2011, up from 17.3 percent in 2006, according to International Telecommunication Union (ITU).[3] About 14 percent of users are broadband subscribers. Total international connection bandwidth of the country grew 250 percent between 2010 and 2011.[4] While a few years ago, most users relied on internet cafes for their access, 88 percent of users now access the net from their home. Access via smart phones has also increased significantly to among 30 percent of users, reaching a similar level of access at internet cafes. In the latest ICT Development Index of the ITU, Vietnam moved up ten positions from 91 (out of 152 countries measured) in 2008 to 81 in 2010, placing third in the top ten most dynamic countries in the ranking.[5]

The internet's growth is largely driven by the demands of Vietnam's booming economy and relatively young population; some 60 percent of the country's total population is under 35. Internet access points are easily found in urban areas throughout the country. In most towns, citizens can access the internet in their homes and workplaces. WiFi connections are available free of charge in many semi-public spaces such as airports, cafes, restaurants, and hotels. Cybercafes are affordable for most urban dwellers,[6] but their importance has decreased, as almost 90 percent of urban users now access the internet from home or work. In large cities, the internet has surpassed newspapers as the most popular source for information.[7]

[2] "In Vietnam, crackdown on journalists in past six months," Committee to Protect Journalists, October 3, 2011, http://www.cpj.org/2011/10/in-vietnam-crackdown-on-journalists-in-past-six-mo.php.

[3] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2006 & 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[4] "Statistics on Internet development up to 12/2011," Report on internet statistics of Vietnam, Vietnam Internet Network Information Center (VNNIC) [in Vietnamese], http://www.thongkeinternet.vn/jsp/trangchu/index.jsp.

[5] "Chỉ số ICT của Viêt Nam tăng 10 bậc" [Vietnam ICT Index rose 10 spots], Lao Dong, September 28, 2011, http://laodong.com.vn/Tin-Tuc/Chi-so-ICT-cua-Viet-Nam-tang-10-bac/60297.

[6] "Việt Nam: 20% không tin tưởng thông tin trên Internet" [Vietnam: 20% do not trust the information on the Internet], PA News, April 15, 2010, http://news.pavietnam.vn/archives/1547.

[7] "Tình hình sử dụng Internet tại Việt Nam 2011" [The Situation of Internet Use in Vietnam in 2011], VNVIC.com, August 3, 2011, http://vnvic.com/tin-tuc-cong-nghe/140-tinh-hinh-su-dung-internet-tai-viet-nam-2011.html.

Given Vietnam's 92 percent literacy rate, illiteracy does not pose a barrier to access.[8] The availability of the internet in rural areas remains limited, although programs backed by the government and international donors have increased access in recent years. Ethnic minorities and the poor who live primarily in remote areas are especially at a disadvantage.

The country's General Statistics Office (GSO) gave an estimate of 158 million mobile subscribers by mid-2011, a growth of 28 percent from the previous year.[9] In 2011, mobile phone penetration stood at 143 percent, according to the latest ITU data.[10] Although the figures exceed the total population, it was estimated in 2010 that some 30 million (nearly one in three) Vietnamese people lacked mobile phones, while others own two mobile devices or multiple SIM cards.[11] A third-generation (3G) network, which enables internet access via mobile phones, has been operating since the end of 2009, and the number of users is slowly expanding. As of the end of 2011, there were estimated to be less than ten million 3G users.[12]

YouTube, Twitter, and international blog-hosting services are freely available and growing in popularity. However, in September 2009, the Ministry of Public Security (MPS) began circulating a mandate instructing internet service providers (ISPs) to block Facebook,[13] which had roughly a million users in Vietnam at the time.[14] By November 2009, users were reporting difficulty accessing the website. It remained sporadically inaccessible throughout 2011, but the government refused to officially acknowledge its efforts to block the site.[15]

While no laws prohibit the use of circumvention tools, a 2008 decree makes it illegal to access blocked websites.[16] Nevertheless, information on circumventing the Facebook block circulated fairly widely, including via videos and blog posts,[17] and Facebook continues to be an important tool among younger internet users. In spite of the block, its membership grew

[8] UNICEF, "At a Glance: Vietnam," accessed August 25, 2010, http://www.unicef.org/infobycountry/vietnam_statistics.html.
[9] "Vietnam subscriber base touches 174.3 millions as of the end of April," Business Times, May 6, 2011, http://vietnambusiness.asia/vietnam-subscriber-base-touches-174-3m-as-at-the-end-of-april/.
[10] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[11] "Mobile Subscribers Touch 110 Million in 2009," Business Times, March 7, 2010, http://vietnambusiness.asia/mobile-subscribers-touch-110-million-in-2009/.
[12] "3G market eyes 2014 breakthrough," VietnamNet Bridge, December 12, 2011, http://english.vietnamnet.vn/en/science-technology/16502/3g-market-eyes-2014-breakthrough.html.
[13] "Decree to Block Facebook in Vietnam," Viet Tan, September 1, 2010, http://www.viettan.org/spip.php?article9390.
[14] An Khanh, "Vietnamese Still Using Facebook," Radio Free Asia, April 20, 2010, http://www.rfa.org/english/news/vietnam/facebook-04202010121723.html.
[15] "Vietnam to Block Facebook," CNN iReport, November 10, 2009, http://ireport.cnn.com/docs/DOC-354181.
[16] Ministry of Information and Communications, "Regarding the management, provision and use of Internet services and electronic information on the internet," Decree 97/2008/NĐ-CP, issued August 28, 2008, http://mic.gov.vn/VBQPPL/vn/documentdetail/8769/index.mic.
[17] Brannon Cullum, "Spotlighting Digital Activism in Vietnam," Movements.org, November 2, 2010, http://allyoumov.3cdn.net/9c97d7925e99e3232d_e5m6b99t7.pdf.

to an estimated four million by the end of 2011.[18] Vietnam has a few local competitors to Facebook, the strongest one being Zing Me with five million users by early 2011.[19] In May 2010, the Ministry of Information and Culture (MIC) also launched a government-backed social network called GoOnline (formerly Go VN), which requires users to register with their real name and government-issued identity number when creating an account. The initial response to the new initiative was limited.[20] As of early 2012, GoOnline had a modest user base but was in no position to compete with Facebook and Zing Me.

The three biggest ISPs are the state-owned Vietnam Post and Telecommunications (VNPT), which holds 74 percent of the market, the military owned Viettel (11 percent), and the privately owned FPT (10 percent). VNPT and Viettel also own the three largest mobile phone service providers in the country (MobiFone, VinaPhone, and Viettel), which reportedly serve 90 percent of the country's subscriber base. Four privately-owned companies share the remainder.[21] While there is no legally imposed monopoly for access providers, informal practices create hurdles for new companies seeking to enter the market, and many find that they lack the political ties or economic clout to do so. Similarly, there is a concentration of internet-exchange providers (IXPs), which serve as gateways to the international internet. Currently there are six IXPs, four of which are state or military-owned.[22]

The Ministry of Post and Telecommunications (MPT), the Ministry of Public Security (MPS), and the Ministry of Culture, Sport, and Tourism (MCST) regulate the management, provision, and usage of internet services. The Vietnam Internet Network Information Center (VNNIC), run by the MPT, manages and allocates internet resources such as domain names.[23] On paper, the MCST is charged with regulating sexual or violent content, while the MPS oversees measures related to politically sensitive content. In practice, however, the ruling VCP issues guidelines to all regulatory bodies as it deems appropriate and in a largely nontransparent manner. In October 2008, the MIC created the Administrative Agency for Radio, Television, and Electronic Information. Among other duties, the agency is tasked

[18] Binh Minh, "Facebook's CEO visits Vietnam," VietnamNet Bridge, December 25, 2011, http://english.vietnamnet.vn/en/science-technology/16933/facebook-s-ceo-visits-vietnam.html.
[19] Huyen Chip, "Vietnam: State of Social Media One Year After Facebook Block," Global Voices, January 25, 2011, http://globalvoicesonline.org/2011/01/25/vietnam-state-of-social-media-one-year-after-facebook-block/.
[20] James Hookway, "In Vietnam, State 'Friends' You," Wall Street Journal, October 4, 2010, http://online.wsj.com/article/SB10001424052748703305004575503561540612900.html.
[21] "Năm 2010: Thị trường thông tin di động sẽ ra sao?" [2010: What Will the Mobile Communication Market Be Like?], Hanoimoi Online, March 5, 2010, http://www.hanoimoi.com.vn/newsdetail/Kinh_te/312116/nam-2010-thi-truong-thong-tin-di-dong-se-ra-sao.htm; Vietnam Posts & Telecommunications Group (VNPT), "Vietnam Telecommunication Report," 2010, http://www.vnpt.com.vn/Portals/0/users/host/052011/05/EBCVT_web.pdf.
[22] The four are: VNPT, Viettel, Hanoi Telecom, and VTC.
[23] Ministry of Information and Communications, "Regulation on Registrar of Domain Name Dot Vn," Vietnam Internet Network Information Center, March 5, 2007, http://www.vnnic.vn/english/5-6-300-0-2-01-20071115.htm.

with regulating online content, which includes drafting guidelines for blogs and managing licenses of online media.[24]

LIMITS ON CONTENT

While the Vietnamese government has fewer resources to devote to online content control than its counterpart in China, the authorities have nonetheless established an effective and increasingly sophisticated content-filtering system. Censorship of online content is implemented by ISPs rather than at the backbone level or the international gateway. There is no real time filtering based on keywords or deep-packet inspections. Instead, specific URLs are identified in advance as targets for censorship and placed on blacklists; ISPs are legally required to block these URLs. In some instances, when users attempt to access a censored website, a "blocked page" notification will appear, informing them that the page has been deliberately blocked rather than rendered unavailable by a technical failure. However, users sometimes receive a vague error message indicating simply that the browser was unable to locate the server for that website.

Although the censorship system is ostensibly aimed at limiting access to sexually explicit content, in practice it primarily targets sites deemed threatening to the VCP's monopoly on political power, such as those related to Vietnamese political dissidents, human rights, democracy, and protests against China's policy in the East Sea dispute. Websites on religious freedom, Buddhism, Roman Catholicism, and the Cao Dai religious group are blocked to a lesser but still significant degree.[25] The Vietnamese authorities largely focus their censorship efforts on Vietnamese-language content, blocking English-language sites less often. For example, while the websites of the *New York Times*, the British Broadcasting Corporation (BBC), Freedom House, Amnesty International, and Human Rights Watch are accessible, those of overseas Vietnamese organizations that are critical of the government—such as Talawas.org, Danluan.org, or Danchimviet.com—are blocked. The websites of the Vietnamese-language services of international media, such as the U.S.-funded Radio Free Asia and the BBC, are also frequently and increasingly blocked.

In 2011, online filtering continued to be strict. Facebook remained banned (although not strictly enforced), and websites related to border and sea disputes between China and Vietnam continued to be firewalled and attacked. The unpredictable and nontransparent

[24] Geoffrey Cain, "Bloggers the New Rebels in Vietnam," SFGate.com, December 14, 2008, http://articles.sfgate.com/2008-12-14/news/17131885_1_bloggers-communist-party-vietnam; Xuan Linh, "Watchdog to Regulate Blogs in Vietnam," VietnamNet Bridge, October 3, 2008, http://english.vietnamnet.vn/politics/2008/10/806781/ (link discontinued).
[25] "Vietnamese Government Expands Internet Censorship to Block Catholic Websites," Catholic News Agency, August 6, 2009, http://www.catholicnewsagency.com/news/vietnamese_government_expands_internet_censorship_to_block_catholic_websites/.

ways in which topics become forbidden make it difficult for users to know where exactly the "red lines" lie. Due to the worsening climate of restrictions on internet expression, the level of self-censorship has increased significantly. State-owned newspapers, such as *Tuoi Tre* and *Thanh Nien*, formerly known for being bold and edgy, have become tame. Notably, *Tuoi Tre* has not even allowed itself to print a single comment in response to the arrest of their prominent journalist Hoang Khuong, who is known for his investigative reporting on corruption in the police force. One common form of self-censorship is for bloggers to disable the readers' comment option on their posts. This acts as a precautionary measure to prevent discussion by commentators from taking a more confrontational tone than what was intended by the original posting.

Online media outlets and internet portals are state-owned and therefore subject to censorship by the VCP. The party's Department for Culture and Ideology and the MPS regularly instruct online newspapers or portals to remove content they perceive as critical of the government. Editors and journalists who post such content risk disciplinary warnings, job loss, or even imprisonment.

In December 2008, the MIC announced a directive requiring blogging platforms to remove "harmful" content, report to the government every six months, and provide information about individual bloggers upon request.[26] This has generally resulted in an increase in the censorship of content that is critical of the VCP, but the impact has been less significant on the many blogs hosted outside the country. In late 2008, the Deputy Minister of Information and Communications reportedly said he would contact international companies such as Google and Yahoo to request cooperation on censorship. However, to date there have been no indications that these companies assist the Vietnamese authorities, for instance by self-censoring search results, as is done in China.[27]

There is no avenue for managers of blocked websites to appeal censorship decisions. Nevertheless, methods to circumvent censorship, such as the use of proxy servers, are relatively well-known among the young and technology-savvy internet users in Vietnam, with some searchable via Google. The authorities have not instituted any major restrictions on content transmitted via email or mobile phone text messages.

Despite government restrictions, Vietnam's internet is vibrant and offers a diversity of content in the Vietnamese language, though most of it is nonpolitical. In 2006, Vietnamese youth discovered blogging as a means to express themselves, and the blogosphere exploded in the three following years. Yahoo! 360 was the most popular platform; at the height of its

[26] Karin Deutsch Karlekar, ed., "Vietnam," *Freedom of the Press 2009* (New York: Freedom House, 2009).
[27] Ann Binlot, "Vietnam's Bloggers Face Government Crackdown," *Time*, December 30, 2008, http://www.time.com/time/world/article/0,8599,1869130,00.html.

popularity, the application reportedly had 15 million Vietnamese users.[28] However, as the program was not particularly popular outside Vietnam, Yahoo terminated the service in mid-2009, starting the decline of the blogging scene in Vietnam. Since then, Vietnam's blogging community has become much more dispersed, with some bloggers migrating to Blogger.com or WordPress.com, others to Yahoo's 360Plus, Facebook, and local networks such as Zing and YuMe.

Although most blogs address personal and nonpolitical topics, citizen journalism has emerged as an important phenomenon and a source of information for many Vietnamese, particularly given the VCP's tight control over traditional media. People now recognize the parallel existence of official and alternative media, the latter of which is exclusively online. Websites such as AnhBaSam.wordpress.com and QueChoa.vn quickly react to and comment on socio-political events and have established themselves as influential opinion makers. In summer 2011, these websites were instrumental in mobilizing people for a series of demonstrations on the streets of Hanoi and Ho Chi Minh City to protest China's claim on the Paracel and Spratly Islands. The protests lasted several months before the authorities cracked down on them and sent one of the organizers to an education camp.[29] In early 2012, blogs played an important role in rallying public opinion and providing evidence against the local government in Hai Phong province after the authorities unlawfully seized the aquacultural land of some farmers, whose violent resistance shocked the country.

VIOLATIONS OF USER RIGHTS

The constitution affirms the right to freedom of expression, but in practice the VCP has strict control over the media. Legislation including internet-related decrees, the penal code, the Publishing Law, and the State Secrets Protection Ordinance has been used to imprison journalists and bloggers. The judiciary is not independent, and many trials related to free expression last only a few hours. When detaining bloggers and online activists, the police routinely fail to follow Vietnamese legal provisions, arresting individuals without a warrant or retaining them in custody beyond the maximum period allowed by law.

In an effort to expand traditional media controls to the blogosphere, the MIC issued Circular 7 in December 2008, which requires blogs to address strictly personal information and refrain from political or social commentary. It also bars internet users from disseminating

[28] Aryeh Sternberg, "Vietnam Online: Then and Now," iMedia Connection, January 5, 2010, http://www.imediaconnection.com/content/25480.asp.

[29] "Người biểu tinh Thu Hằng bị đưa vào trại" [Demonstrator Thu Hang sent to camp], BBC Vietnamese, December 9, 2011, http://www.bbc.co.uk/vietnamese/vietnam/2011/12/111209_bui_hang_arrested.shtml.

press articles, literary works, or other publications that are prohibited by the Press Law.[30] Furthermore, in January 2011 the government issued a new decree that gives authorities more power to penalize journalists and bloggers by stipulating a series of very vague infractions and by outlining penalties for journalists who publish under pseudonyms or refuse to name their sources. The decree aims to impose the same censorship on online media as on traditional media. In particular, it differentiates sharply between journalists accredited by the government and independent bloggers who have far less rights and protection.[31]

In recent years, the Vietnamese authorities have embarked on several crackdowns against bloggers and online writers, subjecting them to extended interrogations, imprisonment, and in some instances physical abuse.[32] In one of the first imprisonment cases of a prominent blogger, Dieu Cay, a vocal critic of the government's human rights record and an advocate for Vietnamese sovereignty over the Spratly Islands, was sentenced in late 2008 to two and a half years in prison on tax evasion charges that most observers viewed as politically motivated.[33] As of April 2012, Dieu Cay was reportedly still behind bars and had been denied access to family and lawyers for 18 months.[34]

Other bloggers have been prosecuted and convicted for "subversion" or "attempting to overthrow the people's government." The authorities have also invoked Articles 79 ("subversion of the people's administration") and 88 ("conducting propaganda against the state") of the penal code to imprison bloggers and online activists.[35] In January 2010, a court in Ho Chi Minh City sentenced four prodemocracy activists to a total of 33 years in prison for using the internet to report rights violations or disseminate pro-democracy views.[36] In October 2010, blogger Le Nguyen Huong Tra (who uses the penname Do Long Girl) was detained on charges of "misusing democratic rights to violate the state's and citizens' interests," after she reported about the family affairs of a high-ranking official.[37] That same

[30] Reporters Without Borders, "Internet Enemies: Vietnam," accessed August 25, 2010, http://en.rsf.org/internet-enemie-vietnam,36694.html.
[31] "Regulations on administrative penalties for violation in media and publishing activities," Decree 02/2011/ND-CP [in Vietnamese], January 6, 2011, http://cpj.org/Vietnam%20media%20decree.pdf.
[32] "Vietnam's Internet Crackdown," CNN Video, June 18, 2010, http://edition.cnn.com/video/#/video/world/2010/06/18/stevens.vietnam.internet.crackdown.cnn?iref=allsearch.
[33] Human Rights Watch, "Banned, Censored, Harassed and Jailed," news release, October 11, 2009, http://www.hrw.org/en/news/2009/10/11/banned-censored-harassed-and-jailed.
[34] "Three bloggers face 20 years in jail for spreading anti-state propaganda," IFEX, April 18, 2012, http://www.ifex.org/vietnam/2012/04/18/bloggers_charged/.
[35] Reporters Without Borders, "Internet Enemies: Vietnam."
[36] Of the four, Le Cong Dinh and Le Thang Long each received five years, Nguyen Tien Trung received seven years, and Tran Huynh Duy Thuc received 16 years. Reporters Without Borders, "Court Sentences Four Netizens and Pro-Democracy Activists to a Total of 33 Years in Jail," news release, January 20, 2010, http://en.rsf.org/vietnam-court-sentences-four-netizens-and-20-01-2010,36156.html.
[37] Vu Mai and Quoc Thang, "Blogger 'Cô gái đồ long' bị bắt khẩn cấp" [Blogger Co Gai Do Long Urgently Arrested], VN Express, October 26, 2010, http://vnexpress.net/GL/Phap-luat/2010/10/3BA221C2/.

month, blogger Phan Thanh Hai (who uses the penname Anh Ba Sai Gon) was arrested on charges of distributing false information on his blog.[38] Most recently in September 2011, a former police officer turned social justice blogger, Ta Phong Tan, was arrested for blog posts that allegedly "denigrated the state."[39] As of April 2012, Ta Phone Tan was still in detention for an open-ended period on vague charges of anti-state activity, according to the Committee to Project Journalists.[40]

In addition to imprisonment, bloggers and online activists have been subjected to physical attacks, job loss, termination of personal internet services, and travel restrictions. For example, in May 2010, Lu Thi Thu Trang, an online activist associated with the pro-democracy movement Bloc 8406, was beaten by the police in front of her five year-old son and then detained for interrogation.[41] That same month, provincial authorities terminated the telephone and internet service connection at the home of Ha Si Phu, one of Vietnam's best-known dissident bloggers, alleging that he had used his telephone line to transmit "anti-government" information. The incidents occurred as part of a broader crackdown on free expression in the lead up to the Communist Party Congress in January 2011, which continued beyond the Congress. In February 2011, independent journalist Nguyen Dan Que was arrested for calling the population "to be inspired by the pro-democratic movements in Africa and Middle East";[42] he was released few days later on the condition that he would cooperate closely with the authorities. In May 2011, poet Bui Chat, head of the underground publishing house, Recycled Paper (Giay vun), was held and questioned several times for no reason after returning from Argentina, where he received the "Freedom to Publish Prize" from International Publisher's Association.[43]

In 2011, the repressive trend against online users has continued with equal severity. According to Reporters Without Borders, a total of 17 bloggers and three journalists are in jail in Vietnam as of August 2011, making Vietnam one of the most repressive countries in the world for bloggers.[44] In January, the pro-democracy online activist and recipient of the 2009 Human Right Award, Vi Duc Hoi, was sentenced to eight years prison and three years house arrest after release (the sentence was later reduced to five year jail and three years

[38] "Another blogger arrested in Vietnam crackdown," Committee to Protect Journalists (CPJ), October 28, 2010, http://cpj.org/2010/10/another-blogger-arrested-in-vietnam-crackdown.php.
[39] "Three Vietnamese journalists given antistate charges," Committee to Protect Journalists (CPJ), April 16, 2012, http://cpj.org/2012/04/three-vietnamese-journalists-given-antistate-charg.php#more.
[40] Ibid.
[41] "Government Suppression of Bloggers and Websites," VietCatholic News, May 27, 2010, http://www.vietcatholic.org/News/Clients/ReadArticle.aspx?ID=80607 (link discontinued).
[42] "Nguyen Dan Que arrested for anti-State activities," Vietnam Plus, February 27, 2011, http://en.baomoi.com/Home/society/en.vietnamplus.vn/Nguyen-Dan-Que-arrested-for-antiState-activities/115657.epi.
[43] "Independent publisher freed, but questioned again," Reporters Without Borders, May 5, 2011, http://en.rsf.org/viet-nam-independent-publisher-freed-but-05-05-2011,40209.html.
[44] "Blogger and poet freed under amnesty, but 17 bloggers and three journalists still held," Reporters Without Borders, August 30, 2011, http://en.rsf.org/vietnam-eight-bloggers-get-sentences-12-10-2009,34653.html.

house arrest). In March, Cu Ha Huy Vu, one of the most vocal and prominent online dissidents, was sentenced to seven years prison and three years house arrest in a trial that barred access to the public and media.[45] In August, Catholic blogger, Paulus Le Son, was brutally abducted on the street by the police and is still under arrest with no prospect of a trial. His blog covered the proceedings of Cu Ha Huy Vu's trial in addition to political and religious issues. Also in August, blogger Lu Van Bay was sentenced to four years in prison for anti-government propaganda in a trial which took only few hours, without access to a lawyer,[46] while French-Vietnamese blogger Pham Minh Hoang was sentenced to three years in prison for attempted subversion.[47]

In November 2011, citizen radio journalists Vu Duc Trung and Le Van Thanh received harsh jail sentences of three years and two years, respectively, for broadcasting Falun Gong programs into China. They were initially accused of illegally operating broadcasting devices, an administrative offence, which was later upgraded into a criminal charge, presumably due to pressure from China.[48] Then in December 2011, well-known journalist Hoang Khuong of *Tuoi Tre* newspaper and author of a series of articles on corruption among the police was arrested on charges of "indirectly bribing a traffic police officer." He was accused of using a broker to pay US$700 to a police officer while doing an undercover investigation.

The Vietnamese authorities employ both technology-based and "low-tech" methods for monitoring online communications. The former methods include monitoring web traffic and emails, especially of political activists, while the latter involve shadowing the movements of known online activists. Cybercafe owners are required to install special software to track and store information about their clients' online activities.[49] In addition, citizens are obliged to provide the details of their government-issued identification documents to register with their ISP when purchasing a home internet connection. In late 2009, the MIC announced that all prepaid mobile phone subscribers would be required to register their details with the operator. Individuals are allowed to register only up to three numbers per carrier.[50] The government argues that such measures are necessary to counter

[45] "Prime Minister urged to free all imprisoned bloggers and journalists," Reporters Without Borders, September 1, 2011, http://en.rsf.org/vietnam-prime-minister-urged-to-free-all-01-09-2011,40879.html.
[46] "Blogger Lu Van Bay Serving Four-Year Sentence," Reporters Without Borders, September 26, 2011, http://en.rsf.org/vietnam-blogger-lu-van-bay-serving-four-26-09-2011,41059.html.
[47] Pham Minh Hoang's jail sentence was halved to 17 months in November 2011; he was released in January 2012 after being in prison since his arrest in August 2010. "Vietnam cuts jail term of French-Vietnamese blogger," AFP, November 28, 2011, http://www.google.com/hostednews/afp/article/ALeqM5hk881ZRwZ4upJPxo8KAnDHRM52uQ?docId=CNG.2c6ad4f9d4378459dbb354b53d6aebcb.4a1.
[48] "Two citizen journalists jailed for illegal broadcasting into China," Reporters Without Borders, November 10, 2011, http://en.rsf.org/vietnam-two-citizen-journalists-jailed-for-10-11-2011,41377.html.
[49] "Internet Censorship Tightening in Vietnam," AsiaNews.it, June 22, 2010, http://www.asianews.it/news-en/Internet-censorship-tightening-in-Vietnam-18746.html.
[50] Phong Quan, "Sim Card Registration Now Required in Vietnam," Vietnam Talking Points, January 16, 2010, http://talk.onevietnam.org/sim-card-registration-now-required-in-vietnam/.

mass text message advertisements that plague many Vietnamese phone users. However, the steps also facilitate surveillance, as service providers are required to share information about users with the government upon request. Nevertheless, there is no requirement for real name registration when blogging or posting online comments and many Vietnamese do so anonymously.

The intensified harassment of bloggers in recent years has coincided with systematic cyberattacks targeting individual blogs as well as websites run by other activists in Vietnam and abroad.[51] Since September 2009, dozens of sites have been attacked, including those operated by Catholics who criticize government confiscation of church property, forums featuring political discussions, and the website raising environmental concerns surrounding bauxite mining.[52] The attackers infected computers with malicious software disguised as a popular keyboard program that allows Microsoft Windows to support the Vietnamese language. Once infected, computers became part of a "botnet" whose command-and-control servers were primarily accessed from internet protocol (IP) addresses inside Vietnam. The network of hijacked computers was then used to carry out the denial-of-service (DoS) attacks described above. Both McAfee, a major internet security firm, and Google reported on the sophisticated attacks, with the latter estimating that "potentially tens of thousands of computers" had been affected, most of which belonged to Vietnamese speakers.[53] McAfee stated that "the perpetrators may have political motivations, and may have some allegiance to the government of the Socialist Republic of Vietnam."[54] The Vietnamese authorities have not taken measures to find or punish the attackers. On the contrary, during a national conference on media held in May 2010, the MPS announced that it had "destroyed 300 'bad' websites and blogs."[55]

In 2011 and early 2012, the number of known cases seems to have decreased, although attacks on sites critical of the government still continue. In June 2011, the well-known website Boxitvn.net, which is critical of the government's pro-Chinese positions and its environmentally-damaging plans to exploit bauxite in the Central Highland, reported several waves of attacks. In August 2011, the U.S.-based organization Viet Tan (or Vietnam Reform Party), accused Vietnam of attacking its website. The attack happened shortly after

[51] Human Rights Watch, "Vietnam: Stop Cyber Attacks Against Online Critics," news release, May 26, 2010, http://www.hrw.org/news/2010/05/26/vietnam-stop-cyber-attacks-against-online-critics.
[52] "Authorities Crush Online Dissent; Activists Detained Incommunicado," *Free News Free Speech* (blog), June 2, 2010, http://freenewsfreespeech.blogspot.com/2010/06/authorities-crush-online-dissent.html.
[53] George Kurtz, "Vietnamese Speakers Targeted in Cyberattack," *CTO* (blog), March 30, 2010, http://siblog.mcafee.com/cto/vietnamese-speakers-targeted-in-cyberattack/; Neel Mehta, "The Chilling Effect of Malware," *Google Online Security Blog*, March 30, 2010, http://googleonlinesecurity.blogspot.com/2010/03/chilling-effects-of-malware.html.
[54] Kurtz, "Vietnamese Speakers Targeted in Cyberattack."
[55] Human Rights Watch, "Vietnam: Stop Cyber Attacks Against Online Critics."

one of the group's members, the French-Vietnamese blogger Pham Minh Hoang, received a prison sentence of three years for his blogging activities.[56]

[56] "Activists accuse Vietnam of cyber attack," Bangkok Post, August 22, 2011, http://www.bangkokpost.com/news/asia/252944/activists-accuse-vietnam-of-cyber-attack.

ZIMBABWE

	2011	2012
INTERNET FREEDOM STATUS	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	16	17
Limits on Content (0-35)	15	14
Violations of User Rights (0-40)	23	23
Total (0-100)	**54**	**54**

* 0=most free, 100=least free

POPULATION: 13 million
INTERNET PENETRATION 2011: 16 percent
WEB 2.0 APPLICATIONS BLOCKED: No
NOTABLE POLITICAL CENSORSHIP: No
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

INTRODUCTION

Despite the restrictive environment for the traditional media, internet and mobile phone usage in Zimbabwe is nominally free from government interference. However, there are indications that the government has a growing desire to curb speech transmitted through information and communication technologies (ICTs), as evidenced by the arrest of a man in 2011 for a comment he made on Facebook. There are also many practical obstacles that hinder citizens' access, including poor infrastructure in urban areas and an almost total lack of infrastructure in rural areas. Over the past decade, the country has experienced a major economic decline, contributing to severe power shortages and accelerated deterioration of the telecommunications system.[1] Low bandwidth has also made internet connections extremely slow in Zimbabwe; nevertheless, internet and mobile phone usage has increased in recent years.

Although the government does not have complete control over ICTs, there have been some worrisome developments over the past five years. For instance, the Interception of Communications Act[2] adopted in 2007 allows the government to monitor postal, telephone and internet traffic, and requires service providers to intercept information on the state's

[1] Zimbabwe's economy contracted significantly between 1999 and 2009 due to a political crisis associated with President Robert Mugabe's controversial land-reform campaign, which entailed seizing white-owned farms and distributing them to black loyalists. Inflation shot to astronomical rates of several billion percent, and the exchange rate of the Zimbabwean dollar tumbled to more than 50 billion per U.S. dollar. See BuddeComm, "Zimbabwe—Telecoms, Mobile, Broadband and Forecasts: Executive Summary," http://www.budde.com.au/Research/Zimbabwe-Telecoms-Mobile-Broadband-and-Forecasts.html.
[2] The Interception of Communications Act is available at http://www.kubatana.net/docs/legisl/ica_070803.pdf.

behalf,[3] but no concrete evidence of systematic internet filtering has been reported.[4] Nevertheless, with the spread of mobile phones and use of text messages to disseminate information critical of President Robert Mugabe and his Zimbabwean African National Union–Patriotic Front (ZANU-PF) supporters, the authorities have imposed some content restrictions and registration requirements related to these technologies. Under Mugabe, the regime has committed rampant human rights abuses and exercised strict control over the traditional media, and with the presidential election expected to take place in 2012 or 2013, it is anticipated that the government's control of various ICTs will continue to grow.

OBSTACLES TO ACCESS

Internet access has expanded rapidly in Zimbabwe, from a penetration rate of 0.3 percent in 2000 to 15.7 percent by the end of 2011.[5] The mushrooming of cybercafes in most of the country's urban centers, coupled with the forced migration of many Zimbabweans to South Africa, the United Kingdom, Australia, and other countries as a result of the political and economic crisis, created a favorable environment for increased internet usage, as the new expatriates sought to stay in touch with friends and family in Zimbabwe. High prices and limited infrastructure put access to the internet beyond the reach of most of the population, particularly in rural areas. However, for those who want to communicate with friends and relatives abroad, the internet represents a faster, easier, and cheaper alternative to telephony and postal services. Furthermore, the restrictive traditional media environment, which is dominated by state-owned outlets, has made the internet popular among citizens seeking alternative information.

There is a vast divide between urban and rural areas with respect to internet penetration. Most rural communities are geographically isolated and economically disadvantaged and have consequently failed to attract the interest of commercial service providers. Telephone penetration in rural areas is minimal, with lack of electricity representing a major challenge; radio remains the main communication medium in such regions. Many rural telephone connections are still shared or "party" lines, leading to poor or unreliable transmission quality, slow connection speeds, and difficulty initiating dial-up internet connections.[6]

[3] Nqobizitha Khumlo, "Zim Internet Service Providers Struggle to Buy Spying Equipment," Kubatana.net, August 10, 2007, http://www.kubatana.net/html/archive/inftec/070810zol1.asp?spec_code=060426commdex&sector=INFTEC&year=0&range_start=1&intMainYear=0&intTodayYear=2010.

[4] "Country Profile: Zimbabwe," Open Net Initiative, September 30, 2009, http://opennet.net/research/profiles/zimbabwe.

[5] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[6] Zimbabwe has one fixed-line telephone operator, the publicly owned TelOne (formerly the Posts and Telecommunications Corporation, or PTC), which has failed to provide universal access. TelOne boasts just 386,000 subscribers, 50 percent of whom are in the capital, Harare. Only 17 percent of the lines are in rural areas, and 92 percent of the total lines have been digitalized.

Even in urban areas, electricity is regularly rationed, and the penetration of both the internet and mobile phones is uneven. In practice, internet access is limited largely to the few Zimbabweans with formal employment or positions in institutions of higher learning. There is little, if any, internet penetration in the poor townships surrounding cities, where much of the population lives, as few township residents can afford it. Internet penetration is highest in the central business districts of the country's two major cities, Bulawayo and Harare. A Zimbabwe All Media Products and Services Survey (ZAMPS) released in February 2011 found that 24 percent of adults living in urban centers are using the internet, with 83 percent of users accessing the web at least once a month.[7] The survey also found Facebook to be the most popular website among Zimbabwean internet users.[8]

The prices for internet access in Zimbabwe are set by owners of cybercafes and internet service providers (ISPs), and the state has so far not interfered on this issue. Individual ISPs submit their tariff proposals to the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), which approves proposals on per case basis. However, with the majority of Zimbabweans surviving on wages of around US$250 per month and the cost of most home internet packages costing US$50 per month not including installation fees, internet subscriptions are mainly for the affluent.[9] Further, the cost of a modem is US$60,[10] and an average computer costs a minimum of US$600.

Fast and reliable satellite connections to the internet are also very expensive. Even those who have access to the internet at work can only use it for a limited amount of time, as companies seek to contain the high monthly fees they pay for broadband. Increased competition is projected to significantly reduce the price of internet in the coming years. In 2010, only the ISP PowerTel[11] offered unlimited broadband at US$50 per month. By the end of 2011, other ISPs had introduced much cheaper internet bundle packages, ranging from US$70 connecting at 512 Kbps for the first gigabyte (and best effort thereafter) to US$18 for one gigabyte of usage. The price per megabyte of mobile broadband services for the country's operators was also reduced in 2011, compelling ISPs to push their prices further downwards.[12]

See "An Overview of Zimbabwe's Telecommunications—Potraz Presentation Download," *Technology Zimbabwe* (blog), March 5, 2010, http://www.techzim.co.zw/2010/03/zimbabwe-telecoms-overview/.

[7] "Zimbabweans look to the Internet for truth and freedom," The Zimbabwe Mail, March 14, 2012, http://www.thezimbabwemail.com/zimbabwe/7436.html.

[8] Ibid.

[9] "Zimbabwe – Telecoms, Mobile and Broadband," BuddeComm, August 2011, http://www.budde.com.au/Research/Zimbabwe-Telecoms-Mobile-Broadband-and-Forecasts.html.

[10] L.S.M Kabweza, "Review: PowerTel Mobile Broadband," TechZim, February 23, 2011, http://www.techzim.co.zw/2011/02/review-powertel-mobile-broadband/.

[11] PowerTel is a subsdiary of the state-owned national power company, Zimbabwe Electricity Supply Authority (ZESA).

[12] L.S.M Kabweza, "How much the price of internet connectivity can reduce in one year," Technology Zimbabwe, January 30, 2012, http://www.techzim.co.zw/2012/01/how-much-the-price-of-internet-connectivity-can-in-one-year/.

Voice over Internet Protocol (VoIP) is now also offered by a number of internet access providers and telephone companies, including Econet (through its broadband division), Gigatel, Telco, PowerTel, Africom, TelOne, Brodacom.[13] Consisting mainly of direct satellite connections through VSAT, other broadband access technologies include GSM, WiMAX, and fiber-optic or copper-wire ADSL.

Although the cost for broadband internet access has gone down due to competition, effective broadband for home and individual users has not been realized due to the poor infrastructure of the state-owned fixed-line operator, TelOne. Nonetheless, there have been efforts to expand coverage to other parts of the country. In December 2010, Econet (through its fiber subsidiary, Liquid Telecom) completed building a fiber link between the capital city Harare and the southern town of Beitbridge, which is connected to South Africa's fiber cable system. Other licensed data carriers are also starting to roll out fiber-optic networks across the country and establish links to international undersea cables.[14]

While broadband is available in major urban areas, particularly Harare and Bulawayo, the majority of Zimbabwean internet users still go online through a dial-up connection. The annual local telephone charges for dial-up access are between US$150 and $208.[15] The number of cybercafes in most of the country's urban centers grew dramatically between 2009 and 2010 due political stability and the dollarization of the economy; however, a number of internet cafes began to close down in 2011 as a result of high costs for both providers and users. For instance, in January 2011, one of the country's largest chains of internet cafes, Quick & Easy, was closed down by a Messenger of the Court for failing to repay a loan amounting to more than US$10,000.[16]

Mobile phone penetration in the country has continued to expand, increasing from 6.8 percent in 2006 to 72.1 percent by the end of 2011,[17] though this figure could be misleading since many people own more than one SIM card. Zimbabwe, like most countries in Africa, has seen an influx of low-cost imitation mobile phones from Asia that are internet-enabled. With the introduction of services like 3G and 4G technology in July 2009 and May 2010,

[13] "Econent Wireless launches VoiP," TeleGeography, January 26, 2012, http://www.telegeography.com/products/commsupdate/articles/2012/01/26/econet-wireless-launches-voip/.
[14] BuddeComm, "Zimbabwe."
[15] ZOL dialup internet price webpage: http://www.zol.co.zw/index.php?option=com_content&view=article&id=99&Itemid=209; YoAfrica dialup price webpage: http://www.yoafrica.com/viewinfo.cfm?linkcategoryid=2&siteid=1.
[16] "Quick and Easy Internet Cafes shut by Messenger of Court," The Zimbabwean, January 17, 2011, http://www.thezimbabwean.co.uk/news/36771/quick-a-easy-internet-cafes-shut-by-messenger-of-court.html.
[17] International Telecommunication Union (ITU),"Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#; A country's teledensity figure measures the number of active mobile phone SIM cards and landlines as percentage of the country's total figure. However, since many people own more than one SIM card, the real mobile phone penetration might be lower than 72.1 percent.

respectively, and Enhanced Data rates for GSM Evolution (EDGE) on mobile networks, internet access has increased as more people connect through their mobile phones.

Given the monthly subscription fee of US$25, the 3G service is still only affordable for the few who are still gainfully employed in a country where the jobless rate is estimated at 94 percent.[18] In fact, some observers fear that rather than enhancing access to the internet for the general public, advanced mobile phone service may sharpen the digital divide by improving access for the few who already have it. Because of inadequate infrastructural development, the current 3G internet is frustratingly slow, and 4G mobile internet access is even more expensive. A 3G monthly subscription costs US$40 per month through the state-owned mobile operator NetOne. It joins rivals Econet and Telecel Zimbabwe in offering 3G service. The rate for pre-paid mobile web access for Telecel, Econet and NetOne is US$0.11, $0.15 and $0.10 per megabyte respectively, making NetOne the cheapest.[19] All three mobile companies have rolled out a mix of 3G, EDGE and GPRS.[20]

There are currently 15 licensed Internet Access Providers (IAPs)[21] and 128 ISPs in Zimbabwe.[22] In Zimbabwe, IAPs offer only internet access, while ISPs may provide additional services, although ISPs must connect through the limited IAP infrastructure. Only two of the IAPs, CommIT[23] and Aptics, have a Class B license, which entitles them to offer internet-based voice services in addition to the normal services that the rest provide.[24] The Class B license fee as set by POTRAZ is US$2 million. Before the IAPs can install their equipment, it must be vetted and approved by the regulator. In addition, the Post and Telecommunications Act of 2000 requires ISPs to renew contracts with TelOne for access to its fixed-line network. There are no stringent regulations that hinder the establishment of cybercafes. According to POTRAZ, Zimbabwe currently has five international gateways for internet and voice traffic. There are also two trunk switches for the TelOne fixed network, and nine mobile switching centres setup by the country's three mobile operators.[25]

[18] UN Central Emergency Response Fund, "CERF Allocates $5 Million for Protracted Relief and Recovery Operation in Zimbabwe," news release, January 14, 2010, http://ochaonline.un.org/CERFaroundtheWorld/Zimbabwe2010/tabid/6430/language/en-US/Default.aspx.
[19] Alfonce Mbizwo, "NetOne 3G ready for launch," BizTech Africa, October 14, 2011, http://www.biztechafrica.com/article/netone-3g-ready-launch/1278/.
[20] "Zimbabwe: NetOne opens mobile broadband to prepaid subscribers," Balancing Act, January 6, 2012, http://www.balancingact-africa.com/news/en/issue-no-586/internet/zimbabwe-netone-open/en.
[21] Interview by L.S.M Kabweza with POTRAZ official in Networks Department, Bonnie B Mtengwa (cited in L.S.M Kabweza (2011) ICT Policy and New Media Cultures in Southern Africa – Zimbabwe Report, Internal report for the Department of Media Studies, University of the Witwatersrand, South Africa.
[22] Zimbabwe Internet Service Providers Association membership list, http://www.zispa.org.zw/members.html.
[23] L.S.M Kabweza, "POTRAZ Calls ICT Providers to Help Define IAP/ISP Roles," Technology Zimbabwe, May 6, 2010, http://www.techzim.co.zw/2010/05/potraz-iap-isp-roles/.
[24] L.S.M Kabweza, "Aptics enters market with promise of affordable broadband and VoIP," TechZim, March 5, 2012, http://www.techzim.co.zw/2012/03/aptics-comes-to-market-with-broadband-internet-and-voip/.
[25] An Overview of Zimbabwe's Telecommunications—Potraz Presentation Download," *Technology Zimbabwe* (blog), March 5, 2010, http://www.techzim.co.zw/2010/03/zimbabwe-telecoms-overview/.

In February 2012, the Transport and Communications Minister Nicholas Goche announced that the government had stopped Econet Wireless from installing a fiber-optic cable linking Zimbabwe to high-speed undersea cables in Mozambique to preserve the monopoly of the service by the state-owned fixed telephone operator, TelOne. The Minister stated that service providers must not compete for the provision of infrastructure, only on services, and highlighted the government policy that infrastructure such as the national backbone should be provided by the public sector. The Minister of Information and Technology,[26] from the Movement for Democratic Change (MDC) opposition party, challenged the government move by arguing that there is no such agreed policy that bans service providers from installing fiber-optic cable.[27] This incident demonstrates continued efforts by government, particularly by ZANU-PF officials, to control Zimbabwe's flow of information.

ISPs and mobile phone companies are licensed and regulated by the telecommunications regulatory body, POTRAZ, whose leaders are appointed by the president in consultation with the Minister of Transport and Communication. POTRAZ has been widely accused of partisanship and making politicized decisions, such as the cancellation of TeleAccess's operating license in 2005.[28] The regulator has not directly blocked the establishment of ISPs, but the exorbitant application fees it charges have hindered the proliferation of such businesses. The fees for IAPs and ISPs range from US$2-4 million, depending on the type of service to be provided. This is in addition to the 3.5 percent of annual gross income that the provider must pay to POTRAZ.[29] Application fees for operating a mobile phone service are equally steep.

LIMITS ON CONTENT

Despite reports of continued human rights abuses and government control over the traditional media, there has been no concrete evidence of systematic internet filtering in Zimbabwe, though some instances of surveillance and censorship have been reported. For example, in previous years, email messages to central bank employees were allegedly blocked if they contained references to the main opposition party, MDC, or its leader,

[26] In April 2009, President Robert Mugabe announced a unilateral decision to reassign the ministerial administration of Acts of Parliament, which saw MDC ministers being stripped of much of their responsibilities, without consulting the other party of the Government of National Unity (GNU). The administration of the Posts and Telecommunications Act was formally reassigned to the Ministry of Transport and Infrastructure Development, under ZANU-PF. The MDC-aligned Minister of Information & Communications, Nelson Chamisa's control over parastatals such as Tel One, Net One, Transmedia and Zimpost and the regulator POTRAZ was taken away.

[27] Alfonce Mbizwo, "Why Zim blocked Econet line," BiztechAfrica, February 19, 2012, http://www.biztechafrica.com/article/why-zim-blocked-econet-line/2036/.

[28] "Potraz Just Playing Dirty Politics—Shumba," Zimbabwe Independent, November 18, 2005, http://www.theindependent.co.zw/business/13372.html.

[29] The POTRAZ website can be found at http://www.potraz.gov.zw/.

Morgan Tsvangirai. There have also been cases in which the authorities apparently traced antigovernment email content to its source and arrested suspected senders.[30]

Although online sources of information are not overtly manipulated by government or partisan interests, the government has from time to time exhibited a desire to control mobile phone communications, for instance by warning operators not to let subscribers use their networks for political purposes, especially during elections or in other potentially volatile situations. The authorities issued such a warning in response to the mass circulation of text messages castigating the ruling ZANU-PF party during its December 2009 party congress. Econet in turn warned all its subscribers that their service would be cut off if they sent political messages.[31] In June 2010, just days after a column in the government-controlled *Herald* newspaper threatened Econet with the loss of its operating license, the company complained to the MDC about its use of the network for political purposes and announced that it was installing software that would identify and block problematic messages.

A few months prior to this incident, in March 2010, the Broadcasting Authority of Zimbabwe (BAZ) tried to stop the Kubatana Freedom Fone's Interactive Voice Response (IVR) service from operating, citing that because IVR was a form of broadcasting, Econet was facilitating unlicensed broadcasting from Kubatana on their platform. Econet subsequently suspended the Kubatana service while their legal department was investigating the matter. The issue was settled a week later after Econet and Kubatana successfully argued that POTRAZ regulates the mobile phone industry, not BAZ, and "that Econet sells lines to individuals and organisations on a non-discriminatory basis, and has no control over their subscribers use of their lines."[32] Thus, Econet could not disconnect Kubatana's phone lines on this basis, leading BAZ to drop the matter.

Overseas-based independent news websites and other digital media have emerged as an important source of alternative information for those able to access them. Sites such as Newszimbabwe.com and Zimonline.co.ca publish independent information often obtained from stringers or other contacts based inside Zimbabwe, at times generating news later picked up by mainstream media outlets. There is no evidence of the government influencing or manipulating online content.

[30] Open Net Initiative, "Country Profile: Zimbabwe," 2009, http://opennet.net/research/profiles/zimbabwe.
[31] "Zanu PF Texts Sent from Sweden: Econet," New Zimbabwe, December 17, 2009, http://www.newzimbabwe.com/news-1491-Zanu+PF+texts+sent+from+Sweden/news.aspx.
[32] Margaret Atwood and Bev Clarke, "New Media, Same Regime Politics: Resisting the Repression of Media Freedom in Zimbabwe," *New Media, Alternative Politics* Working Papers, No 1, December 2010.

In early February 2012, the Zimbabwe Media Commission, created by the country's power-sharing government in 2009 to lead media reforms, announced that it was enlisting the services of the police to bar unlicensed foreign newspapers from being distributed in the country.[33] Several newspapers would be affected should the ban become operational,[34] though it will not affect online versions of newspapers from being accessed by Zimbabweans with access to the internet.

While various social media platforms are available in Zimbabwe, low penetration limits the utility of the internet as a means of mass mobilization. Even within the fraction of the population that accesses the medium regularly, there is no coordinated use of social-networking sites to build support for political change. Nevertheless, during the hotly contested 2008 elections, Zimbabweans used mobile phone text messages and blogs to disseminate oppositionist and independent versions of events that were not addressed in the severely restricted traditional media. Civic organizations such as Kubatana, an online community of Zimbabwean activists and NGOs, have been using specialized software to disseminate bulk political text messages to their subscribers and receive feedback from them.[35] With the use of ICTs, Kubataba is growing as a platform for e-activism and self-expression. In March 2012, during the sentencing trial of six human rights activists who were arrested in February 2011 for watching a video about the uprisings in Egypt and Tunisia, social media were used to inform people of the progress of the trial and gather people at the courthouse. It is believed that the massive public turnout deterred the court from giving prison sentences to the six activists.[36]

In general, sites like Facebook are mainly used for friendly chats and renewing social contacts, as the lack of anonymity on such sites and fear of repercussions limit politically-oriented statements which can traced back to those expressing them. Although many journalists contribute to online news platforms, quite a number of them use pseudonyms when writing on sensitive issues for fear of harassment.[37] Debates on the country's political and socioeconomic issues and reactions to internet stories on Zimbabwe are mostly confined

[33] Trevor Neethling, "Zimbabwe threatens to ban South African newspapers," Business Day, February 3, 2012, http://www.businessday.co.za/articles/Content.aspx?id=164155.
[34] Titles that could be affected include the *Sunday Times*, *Mail and Guardian*, *Business Day* and *Financial Mail* which are published in South Africa as well as *The Zimbabwean* which is published in the United Kingdom.
[35] Ken Banks, "Mobile Phones Play Role in Zimbabwe," PCWorld, April 14, 2008, http://www.pcworld.com/businesscenter/article/144535/mobile_phones_play_role_in_zimbabwe.html.
[36] Discussion with Zimbabwean media freedom activist and consultant, Rashweat Mukundu, March 23, 2012, Johannesburg.
[37] "What online news means for Zimbabwe," The Zimbabwe Mail, April 5, 2011, http://www.thezimbabwemail.com/opinion/7745.html; Tendai Chari, "Ethical challenges facing Zimbabwean media in the context of the Internet," *Global Media Journal - Africa Edition*, Zimbabwe, 2009, Vol 3 (1), globalmedia.journals.ac.za/pub/article/download/19/51; Committee to Protect Journalists, "Sweeping Surveillance Law to Target 'Imperialist-Sponsored Journalists,'" press release, August 9, 2007, http://allafrica.com/stories/200708090943.html; Barbara Borst, "African Journalists Struggle to Find their Role in Building Democracies," *Perspectives on Global Issues*, Volume 2, Issue 2, spring 2008, http://www.perspectivesonglobalissues.com/0301/borst.htm.

to chat rooms and feedback sections of online news sites. Even in those cases, the base of contributors is fairly narrow, and the quality of the discussion is often limited.

Due to the restrictive communicative space in the country, the number of blogs have grown and become critically important in Zimbabwe as an alternative platform for debate. Blogging has offered community organizations, minorities, individuals and online journalists the opportunity to express their views, although some bloggers use pseudonyms for fear of reprisals. Many new blogs hosted by Blogspot and WordPress appeared in 2011.

VIOLATIONS OF USER RIGHTS

Zimbabwe's constitution provides for freedom of expression, including freedom from interference with personal correspondence. However, Section 20(2) of the constitution places a number of limitations on these rights in the interests of national defense, public safety, public order, public morality, public health, and town or country planning.[38] Currently, there are no laws that specifically protect online modes of communication, and bloggers are not recognized as eligible for accreditation as journalists. Judicial independence is compromised by an appointment process that allows for high levels of executive interference. While, the judiciary has sometimes demonstrated a degree of autonomy through rulings that are not necessarily favorable to the state, including on freedom of expression, the government often ignores such decisions.

While most of the charges against journalists in the past few years have either been withdrawn or resulted in acquittals, continuous harassment of journalists by the authorities has often induced self-censorship, even among those writing for online publications. The country's civil and criminal defamation laws, the Interception of Communications Act (ICA), and the Criminal Law Codification and Reform Act (CODE) all apply equally to online journalists and reporters for traditional media. The CODE punishes anyone who publicly undermines the authority of or insults the president in any printed or electronic medium with up to 20 years in prison.[39] In one case, business executive John Norman Alfred Rusthon was arrested in March 2010 for allegedly circulating an email message with photographs purporting to show the lavish interior of the president's house. He was charged with undermining the office of the president under Section 33(2) (a)(i) of the CODE and was released on US$200 bail several days later.[40] The case never went to court.

[38] The text of the constitution is available at http://www.parlzim.gov.zw/cms/UsefulResourses/ZimbabweConstitution.pdf.
[39] The law is available at http://www.kubatana.net/docs/legisl/criminal_law_code_050603.pdf.
[40] "Manager Arrested for Insulting the President," Herald (Zimbabwe), March 2, 2010, http://allafrica.com/stories/201003020057.html.

The ICA in conjunction with the Criminal Evidence Act was also used in July 2011 when the police (from the Criminal Investigations Department's Serious Fraud Squad) approached Econet for the call history details of Minister of Finance Tendai Biti, who is also the secretary-general of the MDC. The police requested this information as part of their investigation into suspected fraud against the minister who allegedly authorized several foreign trips for a female economist in the ministry and gave her travel and subsistence allowances at special rates.[41] The Minister applied for an injunction to bar the police from obtaining details of his cellphone records, and Econet stated that it would not release the Minister's records until the issue was finalized at the High Court. At the time of writing, the matter was still pending.

In March 2011, a man from Bulawayo, Zimbabwe's second largest city, became the first person in the country to be arrested over a comment he made on Facebook. Vikas Mavhudzi was charged "with subverting a constitutional government" after he posted a message on a Facebook page allegedly belonging to opposition leader and Prime Minister Morgan Tsvangirai that referenced the uprisings in Egypt.[42] The man was arrested on February 24, 2011, apparently after receiving an anonymous call that claimed he had sent a "security threat" via his mobile phone. The prosecutor Jeremiah Mutsindikwa accused Mavhudzi of "advocating or attempting to take-over government by unconstitutional means."[43] He spent more than a month in jail before being granted bail on March 31, 2011, and his case collapsed after no evidence of the message could be found.[44]

Mavhudzi's arrest coincided with the imprisonment of 45 individuals on February 19, 2011 who were charged with treason for discussing the Arab Spring events in North Africa. The group had been watching a video about the uprisings in Egypt and Tunisia when the police raided the closed-door meeting, arrested the group members—who included trade union leaders, students, and human rights activists—and confiscated computers and other equipment.[45] Although 39 individuals from the group were freed, the remaining six were imprisoned and tortured before being released on bail. On February 15, 2012, the court dismissed an acquittal application for the six individuals, and on March 21, 2012, the court

[41] "Biti asks High Court to invalidate police phone records warrant," The Zimbabwe Reporter, July 12, 2011, http://zimbabwereporter.com/politics/3425.html; Tendai Kamhungira, "Econet won't release Biti's phone records," Daily News, July 14, 2011, http://www.dailynews.co.zw/index.php/news/34-news/3278-econet-wont-release-bitis-phone-records.html.

[42] The message read: "I am overwhelmed. I don't want to say Mr. or PM what has happened in Egypt is sending shockwaves to dictators around the world. No weapon but unity of purpose worth emulating, hey."

[43] Tererai Karimakwenda, "Bulawayo man arrested over Facebook message," SW Radio Africa News, March 4, 2011, http://www.swradioafrica.com/news040311/byoman040311.htm.

[44] "Zimbabwe Facebook subversion trial collapses," BBC News, Africa, September 21, 2011, http://www.bbc.co.uk/news/world-africa-15004244.

[45] "Activists arrested for watching video on Middle East unrest," IFEX, March 2, 2011, http://www.ifex.org/zimbabwe/2011/03/02/46_arrested/.

handed the activists a two-year suspended prison sentence, a US$500 fine, and 420 hours of community service.[46]

There have been no known cases of physical attacks against bloggers and online journalists, but there is concern that this could change as the country gears for elections in 2012 or 2013.

Website owners, bloggers, and internet users in general are not required to register with the government, though mobile phone users are required to register their SIM cards by submitting their personal identity details to the mobile operator, ostensibly to combat crime and stem threatening or obscene communications.[47] POTRAZ reported that around two million subscribers were disconnected in mid-2011 as a result of non-compliance.[48]

In September 2011, POTRAZ announced a ban of the popular BlackBerry messenger service (BBM) that enables users to send free messages. The ban was reportedly enacted for security reasons, blaming BBM for the mass uprisings in the Arab world at the beginning of 2011 and the violent protests in England in August 2011.[49] Moreover, the POTRAZ director-general announced in mid-2011 that the telecommunications authority was examining the impact of BlackBerry's Research in Motion (RIM) encryption technology and its compliance with the Interception of Communications Act (ICA), which requires that all telecommunication services should have the capability of being intercepted.[50] The ban came after POTRAZ clashed with Econet Wireless Zimbabwe over its subscribers' use of BlackBerry's heavily-encrypted services without prior licensing.[51]

The Post and Telecommunications Act of 2000 allows the government to monitor email usage and requires ISPs to supply information to government officials when requested in addition to report any email with "offensive or dangerous" content. The Interception of Communications Act of 2007 (ICA) enabled the establishment of a monitoring center to

[46] Human Rights Watch, "Zimbabwe: Six Sentenced for Watching Arab Spring Video: Charges in Politically Motivated Case Should be Dropped," news release, March 21, 2012, http://www.hrw.org/news/2012/03/21/zimbabwe-six-sentenced-watching-arab-spring-video.

[47] "POTRAZ issues mobile phone registration reminder," Technology Zimbabwe, January 31, 2011, http://www.techzim.co.zw/2011/01/potraz-registration-reminder/.

[48] Tawinda Musarurwa, "Zimbabwe: Tele-Density Rate takes Dip," The Herald, May 10, 2011, http://allafrica.com/stories/201105110010.html, cited in L.S.M Kabweza, "ICT Policy and New Media Cultures in Southern Africa – Zimbabwe Report, Internal report for the Department of Media Studies" (South Africa: University of the Witwatersrand, 2011).

[49] "Mugabe vetoes Blackberry service," The Zimbabwean, September 28, 2011, http://www.thezimbabwean.co.uk/news/zimbabwe/53208/mugabe-vetoes-blackberry.html.

[50] Section 12 (1) (a) of the Act reads: (1) Notwithstanding any other law, a telecommunication service provider shall – (a) provide a telecommunication service which has the capacity to be intercepted.

[51] Kudakwashe Gwabanayi, "Potraz stops Econet project," Zimpapers, June 18, 2011, http://zimpapers.co.zw/index.php?option=com_content&view=article&id=3793:potraz-stops-econet-project&catid=41:business&Itemid=133.

oversee, among other things, traffic in all telecommunications and postal services.[52] In addition, the law requires telecommunications operators and ISPs to install the necessary technology at their own expense. Failure to comply can be punished with a fine of up to three years in prison. Furthermore, there have been unconfirmed reports that the government has received surveillance technology and training from China.[53]

Warrants allowing the monitoring and interception of communications are issued by the Minister of Information at his discretion, meaning there is no substantial judicial oversight or other independent safeguards against abuse. The frequency and extent of monitoring in practice remains uncertain. There are also reports that the government's Central Intelligence Organization (CIO) monitors all networks connected to the IP world's routing system through the Interception of Communications Unit, which is administered by a top ZANU-PF politician.[54]

The government has reportedly used Chinese assistance to hack into websites, although this cannot be confirmed. In December 2011, the website of the *Daily News*, one of the private newspapers in the country, experienced a series of attacks on its website. Although there is no concrete proof, the *Daily News's* information technology department blamed Chinese hackers working with some Zimbabweans for the hacking.[55] In February 2012, the website of the Finance Ministry (www.zimtreasurey.org) was hacked by a group calling themselves Absolution.[56] This followed a similar hacking of other government websites in December 2010 by a group of supporters working with Wikileaks.

[52] The law is available at http://kubatana.net/docs/legisl/icb_070508.pdf.
[53] Lance Guma, "Too Much to Monitor for Snooping Squads," SW Radio Africa, August 7, 2007, http://www.swradioafrica.com/news070807/snoop070807.htm; Reporters Without Borders, "All Communications Can Now Be Intercepted under New Law Signed by Mugabe," news release, August 6, 2007, http://en.rsf.org/zimbabwe-all-communications-can-now-be-06-08-2007,17623.html.
[54] "Mugabe vetoes Blackberry service," The Zimbabwean, September 28, 2011, http://www.thezimbabwean.co.uk/news/zimbabwe/53208/mugabe-vetoes-blackberry.html.
[55] "Chinese cyber spooks intensify Zimbabwe media attacks, The Zimbabwe Mail targeted," The Zimbabwe Mail, December 30, 2011, http://www.thezimbabwemail.com/zimbabwe/10042-chinese-linked-ip-tries-to-hack-daily-news-website-attacks-on-th.html
[56] L.S.M Kabweza, "Zimbabwe finance ministry website taken down after hacking," Technology Zimbabwe, February 10, 2012, http://www.techzim.co.zw/2012/02/zim-finance-ministry-taken-down-after-hacking/.

METHODOLOGY

This third edition of *Freedom on the Net* provides analytical reports and numerical ratings for 47 countries worldwide. The countries were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom. The ratings and reports included in this study particularly focus on developments that took place between January 1, 2011 and May 1, 2012.

WHAT WE MEASURE

The *Freedom on the Net* index aims to measure each country's level of internet and digital media freedom based on a set of methodology questions described below (see "Checklist of Questions"). Given increasing technological convergence, the index also measures access and openness of other digital means of transmitting information, particularly mobile phones and text messaging services.

Freedom House does not maintain a culture-bound view of freedom. The project methodology is grounded in basic standards of free expression, derived in large measure from Article 19 of the Universal Declaration of Human Rights:

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers."*

This standard applies to all countries and territories, irrespective of geographical location, ethnic or religious composition, or level of economic development.

The project particularly focuses on the transmission and exchange of news and other politically relevant communications, as well as the protection of users' rights to privacy and freedom from both legal and extralegal repercussions arising from their online activities. At the same time, the index acknowledges that in some instances freedom of expression and access to information may be legitimately restricted. The standard for such restrictions applied in this index is that they be implemented only in narrowly defined circumstances and in line with international human rights standards, the rule of law, and the principles of necessity and proportionality. As much as possible, censorship and surveillance policies and procedures should be transparent and include avenues for appeal available to those affected.

The index does not rate governments or government performance per se, but rather the real-world rights and freedoms enjoyed by individuals within each country. While digital media freedom may be primarily affected by state actions, pressures and attacks by nonstate actors, including the criminal underworld, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental, including private corporations.

THE SCORING PROCESS

The index aims to capture the entire "enabling environment" for internet freedom within each country through a set of 21 methodology questions, divided into three subcategories, which are intended to highlight the vast array of relevant issues. Each individual question is scored on a varying range of points. Assigning numerical points allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. Countries are given a total score from 0 (best) to 100 (worst) as well as a score for each subcategory. Countries scoring between 0 to 30 points overall are regarded as having a "Free" internet and digital media environment; 31 to 60, "Partly Free"; and 61 to 100, "Not Free." An accompanying country report provides narrative detail on the points covered by the methodology questions.

The methodology examines the level of internet freedom through a set of 21 questions and nearly 100 accompanying sub-points, organized into three groupings:

A. **Obstacles to Access**—including infrastructural and economic barriers to access; governmental efforts to block specific applications or technologies; legal and ownership control over internet and mobile phone access providers.
B. **Limits on Content**—including filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.
C. **Violations of User Rights**—including legal protections and restrictions on online activity; surveillance and limits on privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.

The purpose of the sub-points is to guide analysts regarding the factors they should consider while evaluating and assigning the score for each methodology question. After researchers submitted their draft scores, Freedom House convened three regional review meetings and several international conference calls, attended by Freedom House staff and a range of local experts, scholars, and civil society representatives from the countries under study. During the meetings, participants reviewed, critiqued, and adjusted the draft scores through careful consideration of events, laws, and practices relevant to each item. After completing the regional and country consultations, Freedom House staff did a final review of all scores to ensure their comparative reliability and integrity.

CHECKLIST OF QUESTIONS

- Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- A combined score of 0-30=Free, 31-60=Partly Free, 61-100=Not Free.
- Under each question, **a lower number of points is allotted for a more free situation, while a higher number of points is allotted for a less free environment.**
- Unless otherwise indicated, the sub-questions listed are meant to provide guidance as to what issues should be addressed under each methodology question, though not all will apply to every country.

A. OBSTACLES TO ACCESS (0-25 POINTS)

1. **To what extent do infrastructural limitations restrict access to the internet and other ICTs? (0-6 points)**
   - *Does poor infrastructure (electricity, telecommunications, etc) limit citizens' ability to receive internet in their homes and businesses?*
   - *To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?*
   - *To what extent is there internet and mobile phone access, including via 3G networks or satellite?*
   - *Is there a significant difference between internet and mobile-phone penetration and access in rural versus urban areas or across other geographical divisions?*
   - *To what extent are broadband services widely available in addition to dial-up?*
2. **Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)**
   - *In countries where the state sets the price of internet access, is it prohibitively high?*
   - *Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?*
   - *Do low literacy rates (linguistic and "computer literacy") limit citizens' ability to use the internet?*
   - *Is there a significant difference between internet penetration and access across ethnic or socio-economic societal divisions?*
   - *To what extent are online software, news, and other information available in the main local languages spoken in the country?*

3. **Does the government impose restrictions on ICT connectivity and access to particular Web 2.0 applications permanently or during specific events? (0-6 points)**
   - *Does the government place limits on the amount of bandwidth that access providers can supply?*
   - *Does the government use control over internet infrastructure (routers, switches, etc.) to limit connectivity, permanently or during specific events?*
   - *Does the government centralize telecommunications infrastructure in a manner that could facilitate control of content and surveillance?*
   - *Does the government block protocols and tools that allow for instant, person-to-person communication (VOIP, instant messaging, text messaging, etc.), particularly those based outside the country (i.e. YouTube, Facebook, Skype, etc.)?*
   - *Does the government block protocols and Web 2.0 applications that allow for information sharing or building online communities (video-sharing, social-networking sites, comment features, blogging platforms, etc.) permanently or during specific events?*
   - *Is there blocking of certain tools that enable circumvention of online filters and censors?*

4. **Are there legal, regulatory, or economic obstacles that prevent the existence of diverse business entities providing access to digital technologies? (0-6 points)**

   Note: Each of the following access providers are scored separately:

   1a. Internet-service providers (ISPs) and other backbone internet providers (0-2 points)
   1b. Cybercafes and other businesses that allow public internet access (0-2 points)
   1c. Mobile phone companies (0-2 points)

   - *Is there a legal or de facto monopoly over access providers or do users have a choice of access provider, including ones privately owned?*
   - *Is it legally possible to establish a private access provider or does the state place extensive legal or regulatory controls over the establishment of providers?*
   - *Are registration requirements (e.g. bureaucratic "red tape") for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?*
   - *Does the state place prohibitively high fees on the establishment and operation of access providers?*

5. **To what extent do national regulatory bodies overseeing digital technology operate in a free, fair, and independent manner? (0-4 points)**
   - *Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?*
   - *Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' interests?*
   - *Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?*
   - *Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?*

- *Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?*

B. LIMITS ON CONTENT (0-35 POINTS)

1. **To what extent does the state or other actors block or filter internet and other ICT content, particularly on political and social issues? (0-6 points)**
   - *Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?*
   - *Is there significant filtering of text messages or other content transmitted via mobile phones?*
   - *Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of e-mail or text messages, etc?*
   - *Are methods such as deep-packet inspection used for the purposes of preventing users from accessing certain content or for altering the content of communications en route to the recipient, particularly with regards to political and social topics?*
2. **To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? (0-4 points)**
   - *To what extent are non-technical measures—judicial or extra-legal—used to order the deletion of content from the internet, either prior to or after its publication?*
   - *To what degree does the government or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?*
   - *Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?*
   - *Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?*
3. **To what extent are restrictions on internet and ICT content transparent, proportional to the stated aims, and accompanied by an independent appeals process? (0-4 points)**
   - *Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?*
   - *Are state authorities transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?*
   - *Do state authorities block more types of content than they publicly declare?*
   - *Do independent avenues of appeal exist for those who find content they produced to have been subjected to censorship?*

4. **Do online journalists, commentators, and ordinary users practice self-censorship? (0-4 points)**
   - *Is there widespread self-censorship by online journalists, commentators, and ordinary users in state-run online media, privately run websites, or social media applications?*
   - *Are there unspoken "rules" that prevent an online journalist or user from expressing certain opinions in ICT communication?*
   - *Is there avoidance of subjects that can clearly lead to harm to the author or result in almost certain censorship?*

5. **To what extent is the content of online sources of information determined or manipulated by the government or a particular partisan interest? (0-4 points)**
   - *To what degree do the government or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?*
   - *Do authorities issue official guidelines or directives on coverage to online media outlets, blogs, etc., including instructions to marginalize or amplify certain comments or topics for discussion?*
   - *Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?*
   - *Does the government employ, or encourage content providers to employ, individuals to post pro-government remarks in online bulletin boards and chat rooms?*
   - *Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?*

6. **Are there economic constraints that negatively impact users' ability to publish content online or online media outlets' ability to remain financially sustainable? (0-3 points)**
   - *Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, e-mail applications, blog hosting platforms, etc.) to be economically viable?*
   - *Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?*
   - *Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?*
   - *To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect "net neutrality" with regard to content)?*
   - *To what extent do users have access to free or low-costs blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?*

7. **To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content? (0-4 points)**
   - *Are people able to access a range of local and international news sources via the internet or text messages, despite efforts to restrict the flow of information?*
   - *Does the public have ready access to media outlets or websites that express independent, balanced views?*

- *Does the public have ready access to sources of information that represent a range of political and social viewpoints?*
- *To what extent do online media outlets and blogs represent diverse interests within society, for example through websites run by community organizations or religious, ethnic and other minorities?*
- *To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?*

8. **To what extent have individuals successfully used the internet and other ICTs as tools for mobilization, particularly regarding political and social issues? (0-6 points)**
   - *To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or the behavior of other powerful societal actors?*
   - *To what extent are online communication tools (e.g. Twitter) or social networking sites (e.g. Facebook, Orkut) used as a means to organize politically, including for "real-life" activities?*
   - *Are mobile phones and other ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?*

C. VIOLATIONS OF USER RIGHTS (0-40 POINTS)

1. **To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)**
   - *Does the constitution contain language that provides for freedom of speech and of the press generally?*
   - *Are there laws or legal decisions that specifically protect online modes of expression?*
   - *Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?*
   - *Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?*
   - *Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?*

2. **Are there laws which call for criminal penalties or civil liability for online and ICT activities? (0-4 points)**
   - *Are there specific laws criminalizing online expression and activity such as posting or downloading information, sending an e-mail, or text message, etc.? (Note: this excludes legislation addressing harmful content such as child pornography or activities such as malicious hacking)*
   - *Do laws restrict the type of material that can be communicated in online expression or via text messages, such as communications about ethnic or religious issues, national security, or other sensitive topics?*
   - *Are restrictions of internet freedom closely defined, narrowly circumscribed, and proportional to the legitimate aim?*
   - *Are vaguely worded penal codes or security laws applied to internet-related or ICT activities?*

- *Are there penalties for libeling officials or the state in online content?*
- *Can an online outlet based in another country be sued if its content can be accessed from within the country (i.e. "libel tourism")?*

3. Are individuals detained, prosecuted or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs, particularly on political and social issues? (0-6 points)

- *Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?*
- *Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via e-mail or text messages?*
- *Does the lack of an independent judiciary or other limitations on adherence to the rule of law hinder fair proceedings in ICT-related cases?*
- *Are individuals subject to abduction or arbitrary detention as a result of online activities, including membership in certain online communities?*
- *Are penalties for "irresponsible journalism" or "rumor mongering" applied widely?*
- *Are online journalists, bloggers, or others regularly prosecuted, jailed, or fined for libel or defamation (including in cases of "libel tourism")?*

4. Does the government place restrictions on anonymous communication or require user registration? (0-4 points)

- *Are website owners, bloggers, or users in general required to register with the government?*
- *Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names or register with the government?*
- *Are users prohibited from using encryption software to protect their communications?*
- *Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?*

5. To what extent is there state surveillance of internet and ICT activities without judicial or other independent oversight, including systematic retention of user traffic data? (0-6 points)

- *Do the authorities regularly monitor websites, blogs, and chat rooms, or the content of e-mail and mobile text messages, including via deep-packet inspection?*
- *To what extent are restrictions on the privacy of digital media users transparent, proportional to the stated aims, and accompanied by an independent process for lodging complaints of violations?*
- *Where the judiciary is independent, are there procedures in place for judicial oversight of surveillance and to what extent are these followed?*
- *Where the judiciary lacks independence, is there another independent oversight body in place to guard against abusive use of surveillance technology and to what extent is it able to carry out its responsibilities free of government interference?*

- *Is content intercepted during internet surveillance admissible in court or has it been used to convict users in cases involving free speech?*

6. To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users? (0-6 points)

Note: Each of the following access providers are scored separately:

1a. Internet-service providers (ISPs) and other backbone internet providers (0-2 points)
1b. Cybercafes and other businesses that allow public internet access (0-2 points)
1c. Mobile phone companies (0-2 points)

- *Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?*
- *Are access providers prosecuted for not doing so?*
- *Does the state attempt to control access providers through less formal methods, such as codes of conduct?*
- *Can the government obtain information about users without a legal process?*

7. Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor? (0-5 points)

- *Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?*
- *Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?*
- *Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?*
- *Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?*

8. Are websites, governmental and private entities, ICT users, or service providers subject to widespread "technical violence," including cyberattacks, hacking, and other malicious threats? (0-3 points)

- *Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks (e.g. cyber espionage, data gathering, DoS attacks), including those originating from outside of the country?*
- *Have websites belonging to opposition or civil society groups within the country's boundaries been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?*
- *Are websites or blogs subject to targeted technical attacks as retribution for posting certain content (e.g. on political and social topics)?*
- *Are laws and policies in place to prevent and protect against cyberattacks (including the launching of systematic attacks by non-state actors from within the country's borders) and are they enforced?*

CONTRIBUTORS

FREEDOM HOUSE RESEARCH TEAM

- Sanja Kelly, Project Director, Freedom House
- Sarah Cook, Senior Research Analyst, Freedom House
- Mai Truong, Staff Editor, Freedom House

REPORT AUTHORS AND ADVISORS

- **Argentina:** Eduardo Bertoni, Director, Center for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law, Argentina; Atilio Grimani, Research Assistant at CELE
- **Australia:** Alana Maurushat, Director, Cyberspace Law and Policy Centre, University of New South Wales
- **Azerbaijan:** Khadija Ismayilova, journalist; Vafa Fati-Zada, independent researcher
- **Brazil:** Omar Kaminski, President, Brazilian Institute of IT Law; Ivar A. M. Hartmann, Researcher, FGV Law School in Rio de Janeiro
- **Burma**: Min Zin, Burmese journalist and columnist for *Foreign Policy's* Transitions blog
- **China** (Advisor)**:** Xiao Qiang, Director of China Internet Project and an adjunct professor, Graduate School of Journalism, University of California, Berkeley
- **Cuba:** Ernesto Hernández Busto, blogger and journalist based in Spain
- **Georgia:** Giorgi (Giga) Paitchadze, blogger, Tbilisi
- **Germany:** Jeanette Hoffman, Director, and Christian Katzenbah, Project Manager for Research, Alexander von Humboldt Institute for Internet and Society, Berlin
- **Hungary:** Sandor Orban, Program Director, South East European Network for Professionalization of Media; Borbála Tóth, independent researcher
- **India:** Ketan Tanna, Feature and Web Editor, *The Free Press Journal*, Mumbai
- **Indonesia:** Enda Nasution, blogger and founder of Salingsilang online portal, Jakarta
- **Iran:** Mahmood Enayat, Director, Iran Media Program, Annenberg School of Communication, University of Pennsylvania
- **Italy:** Giampiero Giacomello, Assistant Professor of International Relations, University of Bologna
- **Jordan:** Yahia Shukkier, journalist at *al-Arab al-Yawm* and lecturer, Media Faculty, Middle East University, Amman

- **Kazakhstan**: Adil Nurmakov, Associate Professor, International IT University, Almaty
- **Kenya:** Grace Githaiga, Associate, Kenya ICT Action Network, Nairobi
- **Kyrgyzstan:** Tattu Mambetalieva, Director, Civil Initiative on Internet Policy (CIIP), Bishkek; Artem Goryainov, IT Programs Director, CIIP
- **Mexico:** Alejandra Ezeta, Director, Ciudadanos en Medios: Democracia e Información
- **Nigeria:** 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria
- **Pakistan:** Bytes for All, Islamabad
- **Philippines:** Jacques D.M. Gimeno, Program Director, Philippines Center for Islam and Democracy; Sheen Gimeno, independent researcher
- **South Africa:** Alex Comninos, independent researcher from South Africa and doctoral student, Department of Geography, Justus-Liebig University, Giessen
- **Southeast Asia** (Advisor): Bridget Welsh, Associate Professor in Political Science, Singapore Management University
- **South Korea:** Yenn Lee, Visiting Scholar, Royal Holloway, University of London
- **Sri Lanka:** Nigel Nugawela, researcher, Center for Policy Alternatives, Colombo (at time of writing)
- **Syria:** Mohammad al-Abdallah, Syrian human rights activist and independent researcher
- **Thailand:** Arthit Suriyawongkul and Thaweeporn Kummetha, Thai Netizen Network
- **Turkey:** Yaman Akdeniz, Professor of Law, Istanbul Bilgi University and founder of Cyber-Rights.org
- **Uganda:** Peter Mwesige, Executive Director, African Centre for Media Excellence (ACME); Grace Natabaalo, Program Associate, ACME; and Ashnah M. Kalemera, Program Officer, Collaboration on International ICT Policy for East and Southern Africa
- **Ukraine:** Tatyana Lokot, doctoral student at the Philip Merrill College of Journalism, University of Maryland; head of new media programs in Kyive-Mohyla Journalism School (at time of writing)
- **United Kingdom**: David Banisar, independent researcher, London
- **United States**: Center for Democracy and Technology, Washington DC
- **Uzbekistan:** Zhanna Hördegen, lawyer and Research Fellow, University Priority Research Program on Asia and Europe, University of Zurich

The analysts for the reports on Bahrain, Belarus, China, Egypt, Estonia, Ethiopia, Libya, Malaysia, Russia, Rwanda, Saudi Arabia, Tunisia, Venezuela, Vietnam and Zimbabwe are independent internet researchers who have requested to remain anonymous.

GLOSSARY

Note: Glossary definitions based on those available from the following sources, as well as additional explanations drawn from other sections of this study: Merriam Webster Online, www.merriam-webster.com and Webopedia: Online Computer Dictionary for Computer and Internet Terms and Definitions, www.webopedia.com.

3G: Third generation of mobile communications technology, which allows high-speed internet access through mobile phones

Blog: short for weblog, an online personal journal with reflections, comments, and often links to other websites or blogs provided by the writer; most blogs allow reader comments and are used to foster discussion surrounding certain topics; while most contain reflections on bloggers' personal lives, increasingly they are being used to comment on social and political issues

Blogosphere: all of the blogs on the internet or within a specific country, e.g. the Tunisian blogosphere

Broadband: a high-speed internet connection in which a single wire can carry many channels at once, allowing a high data-transfer rate; necessary for viewing multimedia content

Bulletin Board System (BBS): an electronic message center; most bulletin boards serve specific interest groups; users can post information or products for sale, and other posters can respond

Chat Room: an online location that allows multiple users to engage in a real-time, text-based conversation or discussion

Cybercafe: a commercial location where patrons can use the in-house computers to access the internet for a specified fee and time; most often used by travelers or those without a home internet connection

Cyberspace: the nonphysical world created by computer systems; the internet, for example, creates a cyberspace within which people can communicate with one another, do research, or simply window shop; like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery

DDOS Attack: Distributed Denial of Service Attack; generally consists of the concerted efforts of a person or persons to prevent an internet site or service from functioning efficiently or at all, either temporarily or indefinitely; this is usually done by overloading the attacked website with so many requests for information that it crashes and cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable; those responsible often infiltrate computers around the world and program them to join in the assault as an automated network, or "botnet"

Dial-up: an internet connection over a standard telephone line, usually with a very slow speed that makes it difficult to access some features, especially multimedia applications

DNS: domain name system; an internet service that translates domain names—the appellations commonly used to identify websites, e.g., www.example.com—into numerical IP addresses; because domain names are alphabetic, they are easier to remember, but the internet is actually based on IP addresses; every time a user enters a domain name, a DNS service must translate the name into the corresponding IP address; for example, the domain name www.example.com might translate to 198.105.232.4

DSL and ADSL: digital subscriber line and asymmetrical digital subscriber line; allow data transmission over the wires of a local telephone network, at a faster speed than dial-up permits; the internet connection can be maintained without obstructing telephone use on the same line; ADSL features a greater flow of data in one direction than in the other, so that download speeds are often much faster than upload speeds

Fiber-Optic Cables: Cables made of glass or plastic fibers, used to transmit data. Fiber optic cables have a much greater bandwidth than metal wires typically used for local telephone networks, can carry more data, and are less susceptible to interference

Firewall: a system designed to prevent unauthorized access to or from a private network; can be implemented in both hardware and software; all messages entering or leaving the protected network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria; while in most countries these are also used by companies to prevent employees from accessing content unrelated to their work, in several countries—most notably China and Iran—firewalls are set up on a national level to prevent citizens from accessing certain content from abroad

Forum: an online discussion group in which participants with common interests can exchange open messages; forums are sometimes called newsgroups

Forum Trolling: the practice of lingering in a chat room or forum and reading the posts instead of contributing to the discussion, often used to denote a "spy" who observes what is being said or discussed and then reports that information to authorities or who attempts to maliciously disrupt conversations or agitate users in a forum or chat room

Hosting Service/Host: a service provider that houses, or hosts, multiple websites on its server computers in exchange for a fee

ICT: information and communications technology, including computers and mobile devices

Instant Messaging/I-Chatting: real-time, text-based communication between individuals in what amounts to a temporary private chat room

IP Address: the numeric address of a computer on the internet; used to identify a computer and network in much the same way as a social security number or national identity number is used to identify a person

ISP: internet-service provider, a company that provides access to the internet for a fee; supplies customers with a software package, a username, a password, and telephone numbers to initiate a connection

IT: information technology, the broad subject concerned with all aspects of managing and processing information

Local Area Network (LAN): A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves

Microblog: A type of blog that allows users to publish short text updates that are disseminated to a large number of followers. Twitter is an example of a microblogging site that allows posts of up to 140 characters

Netizen: citizen of the internet; a person actively involved in the online community

Packet Sniffer: computer software or hardware that can intercept and log traffic passing over a network; often part of a firewall system; can be used to spy on users and collect sensitive information such as passwords

Proxy server: A server, or a computer that sits between a user and a website to intercept requests. Proxy servers have various uses, but in the context of these reports, they typically refer to a tool used to circumvent blocks on accessing certain websites

Real Name Registration: A system by which users who want to post a comment online have to complete a registration form that collects data on the user's real name, ID card number, contact phone or address

Secure Sockets Layer (SSL): a method developed for transmitting private documents and data over the internet; uses two-layer encryption to ensure security; most often used in websites that handle private data, such as credit-card or banking information; denoted by the use of "https" in the URL rather than the standard "http"

SMS/Text Messaging: short-message service; brief text messages of no more than a few hundred characters, sent electronically from one mobile phone to another

Social Networking Site (SNS): a website that enables users to create public profiles and form relationships with the site's other users, e.g., Facebook, MySpace, Orkut

Uniform Resource Locator (URL): the global address of a document or page on the World Wide Web, e.g. http://www.freedomhouse.org/report-types/freedom-net is the URL for *Freedom on the Net*

Universal Serial Bus (USB) Modem: a specific portable USB device that looks similar to a USB flash drive (a data storage device) and can be plugged into any USB port on a computer to allow broadband access to the internet

Value-added Network Service (VANS): a network provider hired to facilitate electronic data interchange or provide other network services; before the arrival of the World Wide Web, some companies formed value-added networks to exchange data with other companies, but contemporary VANS providers focus on offering data translation, encryption, secure e-mail, management reporting, and other services for their customers

Video Sharing: the practice of uploading video clips—including those captured using mobile phones with video features—for viewing by others; some video sharing takes place via paid web-hosting sites, but most occurs on popular free websites such as YouTube

Virtual Private Network (VPN): a way to maintain fast, secure, and reliable communication by using the internet to connect remote sites or users; often explained as tunneling a smaller network through a larger network, a VPN can be established to

circumvent strict internet controls and censorship within a given country; multinational corporations that operate in repressive internet environments often purchase from the government the right to use VPNs to connect to their home offices

VoIP: Voice over Internet Protocol, a category of hardware and software that enables users to make telephone calls via the internet; these calls do not incur a surcharge beyond what the user is paying for internet access, just as users do not pay for sending individual e-mails

Web 2.0: the metaphorical second generation of the World Wide Web; refers to advanced graphical features, multimedia formats, greater interactivity and content production by users, and related online services, including blog hosting, video sharing, and social networking

Wi-Fi: wireless technology that provides an internet or network connection for properly equipped computers, mobile phones, and other such devices within a given physical or geographical area

BOARD OF TRUSTEES

ABOUT FREEDOM HOUSE

Freedom House is an independent private organization supporting the expansion of freedom throughout the world.

Freedom is possible only in democratic political systems in which governments are accountable to their own people, the rule of law prevails, and freedoms of expression, association, and belief are guaranteed. Working directly with courageous men and women around the world to support nonviolent civic initiatives in societies where freedom is threatened, Freedom House functions as a catalyst for change through its unique mix of analysis, advocacy, and action.

- **Analysis:** Freedom House's rigorous research methodology has earned the organization a reputation as the leading source of information on the state of freedom around the globe. Since 1972, Freedom House has published *Freedom in the World*, an annual survey of political rights and civil liberties experienced in every country of the world. The survey is complemented by an annual review of press freedom, an analysis of transitions in the post-communist world, and other publications.
- **Advocacy:** Freedom House seeks to encourage American policymakers, as well as other government and international institutions, to adopt policies that advance human rights and democracy around the world. Freedom House has been instrumental in the founding of the worldwide Community of Democracies, has actively campaigned for a reformed Human Rights Council at the United Nations, and presses the Millennium Challenge Corporation to adhere to high standards of eligibility for recipient countries.
- **Action:** Through exchanges, grants, and technical assistance, Freedom House provides training and support to human rights defenders, civil society organizations, and members of the media in order to strengthen indigenous reform efforts in countries around the globe.

Founded in 1941 by Eleanor Roosevelt, Wendell Willkie, and other Americans concerned with mounting threats to peace and democracy, Freedom House has long been a vigorous proponent of democratic values and a steadfast opponent of dictatorships of the far left and the far right. The organization's diverse Board of Trustees is composed of a bipartisan mix of business and labor leaders, former senior government officials, scholars, and journalists who agree that the promotion of democracy and human rights abroad is vital to America's interests.

1301 Connecticut Avenue, NW, Washington, DC 20036
(202) 296-5101

120 Wall Street, New York, NY 10025
(212) 514-8040