Mexico's New Copyright Law:

COPYING AND PASTING USA'S FLAWED COPYRIGHT SYSTEM IS A HUMAN-RIGHTS CATASTROPHE IN THE MAKING

CORY DOCTOROW
EFF Special Advisor

Appendix by KIT WALSH
EFF Senior Staff Attorney

July, 2020

ELECTRONIC FRONTIER FOUNDATION

Author: Cory Doctorow, Appendix by Kit Walsh

A publication of the Electronic Frontier Foundation, 2020.

View this report online:

https://eff.org/mexican-copyright-jul-2020.pdf

Table of Contents

Introduction

In a rushed process without meaningful consultation or debate, Mexico's Congress has adopted a new copyright law modeled on the U.S. system, without taking any account of the well-publicized, widely acknowledged problems with American copyright law. The new law was passed as part of a package of legal reforms accompanying the United States-Mexico-Canada Agreement (USMCA), Donald Trump's 2020 successor to 1989's North American Free Trade Agreement (NAFTA).

However, Mexico's implementation of this Made-in-America copyright system imposes far more restrictions than either the USMCA demands or that Canada or the USA have imposed on themselves. This new copyright regime places undue burdens on Mexican firms and the Mexican people, conferring a permanent trade advantage on the richer, more developed nations of the USA and Canada, while undermining the fundamental rights of Mexicans guaranteed by the Mexican Constitution and the American Convention on Human Rights.

The opposition that sprang up after the swift passage of the new Mexican copyright law faces many barriers, but among the most serious ones is a disinformation campaign that (predictably) characterizes the claims about U.S. copyright law as "fake news". The EFF has more experience with the defects of U.S. copyright law than anyone, and in the sections below we will use it to explain in detail how Mexico's copyright law repeats and magnifies the errors that American lawmakers committed in 1998.

In 1998, the U.S. adopted the Digital Millennium Copyright Act (DMCA), a law whose problems the US government has documented in exquisite detail in the decades since. By the U.S. government's own account, the DMCA presents serious barriers to:

- free expression;
- national resiliency;
- economic self-determination;
- the rights of people with disabilities;
- cybersecurity;
- independent repair;
- education;
- archiving;
- access to knowledge; and
- competition.

Despite these manifest defects, the U.S. government successfully pressured Canada into adopting substantially similar legislation in 2011 with the passage of Canada's Bill C-11. In a series analyses below, we elucidate the ways in which the Mexican copyright bill imposes undue and unique burdens on Mexico, Mexican people, and Mexican industry, and what lessons Mexico *should* have learned from the U.S. and Canadian experience with this one-sided, overreaching version of copyright for the digital world.

In 1998, the US tragically failed to see the import of getting the rules for the Internet right, passing a copyright law that treated the Internet as a glorified entertainment medium. When Canada adopted its law in 2011, it had no excuse for missing the fact that the Internet had become the world's digital nervous system, a medium where we transact our civics and politics; our personal, familial and romantic lives; our commerce and employment; our health and our education.

But these failings pale in comparison to the dereliction of Mexican lawmakers in importing this system to Mexico. The pandemic and its lockdown made it clear that everything we do not only involves the Internet: it *requires* the Internet. In today's world, it is absolutely inexcusable for a lawmaker to regulate the net as though it were nothing more than a glorified video-on-demand service.

Mexico's prosperity depends on getting this right. Even more: the human rights of the Mexican people require that the Congress of Mexico or the Mexican Court get this right.

Free expression

Mexico's Constitution has admirable, far-reaching protections for the free expression rights of its people. Mexico's Congress is not merely prohibited from censoring its peoples' speech -- it is also banned from making laws that would cause others to censor Mexicans' speech.

Mexico's Supreme Court has ruled that Mexican authorities and laws must recognize both Mexican constitutional rights law and international human rights law as the law of the land. This means that the human rights recognized in the Constitution and international human rights treaties such as the American Convention on Human Rights, including their interpretation by the authorized bodies, make up a "parameter of constitutional consistency," except that where they clash, the most speech-protecting rule wins. Article 13 of the American Convention bans prior restraint (censorship prior to publication) and indirect restrictions on expression.

As we will see, Mexico's new copyright law falls very far from this mark, exposing Mexicans to grave risks to their fundamental human right to free expression.

Filters

While the largest tech companies in America have voluntarily adopted algorithmic copyright filters, Article 114 Octies of the new Mexican law says that "measures must be taken to prevent the same content that is claimed to be infringing from being uploaded to the system or network controlled and operated by the Internet Service Provider after the removal notice." This makes it clear that any online service in Mexico will have to run algorithms that intercept everything posted by a user, compare it to a database of forbidden sounds, words, pictures, and moving images, and, if it finds a match, it will have to block this material from public view or face potential fines.

Requiring these filters is an unlawful restriction on freedom of expression. "At no time can an ex ante measure be put in place to block the circulation of any content that can be assumed to be protected. Content filtering systems put in place by governments or commercial service providers that are not controlled by the end-user constitute a form of prior censorship and do not represent a justifiable restriction on freedom of expression." Moreover, they are routinely wrong. Filters often mistake users own creative works for copyrighted works controlled by large corporations and block them at the source. For example, classical pianists who post their own performances of public domain music by Beethoven, Bach, and Mozart find their work removed in an eyeblink by an algorithm that accuses them of stealing from Sony Music, which has registered its own performances of the same works.

To make this worse, these filters amplify absurd claims about copyright — for example, the company Rumblefish has claimed copyright in many recordings of ambient birdsong, with the effect that videos of people walking around outdoors get taken down by filters because a bird was singing in the background. More recently, humanitarian efforts to document war-crimes fell afoul of automated filtering.

Filters can't tell when a copyrighted work is incidental to a user's material or central to it. For example, if your seven-hour scholarly conference's livestream captures some background music playing during the lunch break, YouTube's filters will wipe out all seven hours' worth of audio, destroying the only record of the scientific discussions during the rest of the day.

For many years, people have toyed with the idea of preventing their ideological opponents' demonstrations and rallies from showing up online by playing copyrighted music in the background, causing all video-clips from the event to be filtered away before the message could spread.

This isn't a fanciful strategy: footage from US Black Lives Matter demonstrations is vanishing from the Internet because the demonstrators played amplified music during their protests.

No one is safe from filters: last week, CBS's own livestreamed San Diego Comic-Con presentation was shut down due to an erroneous copyright claim by itself.

Filters can only tell you if a work matches or doesn't match something in their database — they can't tell if that match constitutes a copyright violation. Mexican copyright contains "limitations and exceptions" for a variety of purposes. While this is narrower than the US's fair use law, it nevertheless serves as a vital escape valve for Mexicans' free expression. A filter can't tell if a match means that you are a critic quoting a work for a legitimate purpose or an infringer breaking the law.

As if all this wasn't bad enough: the Mexican filter rule does not allow firms to ignore those with a history of making false copyright claims. This means that if a fraudster sent Twitter or Facebook — or a Made-In-Mexico alternative — claims to own the works of Shakespeare, Cervantes, or Juana Inés de la Cruz, the companies could ignore those particular claims if their lawyers figured out that the sender did not own the copyright,

but would have to continue evaluating each new claim from this known bad actor. If a fraudster included just one real copyright claim amidst the torrent of fraud, the online service provider would be required to detect that single valid claim and honor it.

This isn't a hypothetical risk: "copyfraud" is a growing form of extortion, in which scammers claim to own artists' copyrights, then coerce the artists with threats of copyright complaints.

Algorithms work at the speed of data, but their mistakes are corrected in human time (if at all). If an algorithm is correct an incredible, unrealistic 99 percent of the time, that means it is wrong one percent of the time. Platforms like YouTube, Facebook and TikTok receive hundreds of millions of videos, pictures and comments every day — one percent of one hundred million is one million. That's one million judgments that have to be reviewed by the company's employees to decide whether the content should be reinstated.

The line to have your case heard is long. How long? Jamie Zawinski, a nightclub owner in San Francisco, posted an announcement of an upcoming performance by a band at his club in 2018, only to have it erroneously removed by Instagram. Zawinski appealed. *28 months later*, Instagram reversed its algorithm's determination and reinstated his announcement — more than two years after the event had taken place.

This kind of automated censorship is not limited to nightclubs. Your contribution to your community's online discussion of an upcoming election is just as likely to be caught in a filter as Zawinski's talking about a band. When (and if) the platform decides to let your work out of content jail, the vote will have passed, and with it, your chance to be part of your community's political deliberations.

As terrible as filters are, they are also very expensive. YouTube's "Content ID" filter has cost the company more than $100,000,000, and this flawed and limited filter accomplishes only a narrow slice of the filtering required under the new Mexican law. Few companies have an extra $100,000,000 to spend on filtering technology, and while the law says these measures "should not impose substantial burdens" on implementers, it also requires them to find a way to achieve permanent removal of material following a notification of copyright infringement. Filter laws mean even fewer competitors in the already monopolized online world, giving the Mexican people fewer places where they may communicate with one another.

Technical Protection Measures

Section 1201 of America's Digital Millennium Copyright Act (DMCA) is one of the most catastrophic copyright laws in history. It provides harsh penalties for anyone who tampers with or disables a "technical protection measure" (TPM): massive fines or, in some cases, prison sentences. These TPMs — including what is commonly known as "Digital Rights Management" or DRM — are the familiar, dreaded locks that stop you from refilling your printer's ink cartridge, using an unofficial App Store with your phone or game console, or watching a DVD from overseas in your home DVD player.

You may have noticed that none of these things violate copyright — and yet, because you must remove a digital lock in order to do them, you could be sued in the name of copyright law. DMCA 1201 does not provide the clear, unambiguous protection that would be needed to protect free expression. One appellate court in the United States has explicitly held that you can be liable for a violation of Section 1201 even if you're making a fair use, and that is the position adopted by the U.S. Copyright Office. Other courts disagree, but the net effect is that you engage in these non-infringing uses and expressions at your peril. The US Congress has failed to clarify this law and tie liability for bypassing a TPM to an actual act of copyright infringement — "you may not remove the TPM from a Netflix video to record it and put it on the public Internet (a copyright infringement), but if you do so in order to make a copy for personal use (not a copyright infringement), that's fine."

The failure to clearly tie DMCA 1201 liability to infringement has had wide-ranging effects for repair, cybersecurity and competition that we will explore below. Today, we want to focus on how TPMs undermine free expression.

TPMs give unlimited power to manufacturers. An ever-widening constellation of devices are designed so that any modifications require bypassing a TPM and incurring liability. This allows companies to sell you a product but dictate how you must use it — preventing you from installing your own apps or other code to make it work the way *you* want it to.

The first speech casualty of TPM rules is the software author. This person can write code — a form of speech — but they cannot run it on their devices without permission from the manufacturer, nor can they give the code to others to run on their devices.

Why might a software author want to change how their device works? Perhaps because it is interfering with their ability to read literature, watch films, hear music or see images. TPMs such as the global DVB CPCM standard enforce a policy called the "Authorized Domain" that defines what is — and is not — a family. Authorized Domain devices owned by a standards compliant family can all share creative works among them, allowing parents and children to share among themselves.

But an "Authorized Domain family" is not the same as an *actual* family. The Authorized Domain was designed by rich people from the global north working for multinational corporations, whose families are far from typical. The Authorized Domain will let you share videos between your boat, your summer home, and your SUV — but it won't let you share videos between a family whose daughter works as a domestic worker in another country, whose son is a laborer in another state, and whose parents are migrant workers who are often separated (there are far more families in this situation than there are families with yachts and second homes!).

Even if your family meets with the approval of an algorithm designed in a distant board-room by strangers who have never lived a life like yours, you still may find yourself unable to partake in culture that you are entitled to. TPMs typically require a remote server to function, and when your Internet goes down, your books or movies can be rendered unviewable.

It's not just Internet problems that can cause the art and culture you own to vanish: last year, Microsoft became the latest in a long list of companies who switched off their DRM servers because they decided they no longer wanted to be a bookstore. Everyone who ever bought a book from Microsoft lost their books.

Forever.

Mexico's Congress did nothing to rebalance its version of America's TPM rules. Indeed, Mexico's rules are *worse* than America's. Under DMCA 1201, the US Copyright Office holds hearings every three years to grant exemptions to the TPM rule, granting people the right to remove or bypass TPMs for legitimate purposes. America's copyright regulator has granted a very long list of these exemptions, having found that TPMs were interfering with Americans in unfair, unjust, and even unsafe ways. Of course, that process is far from perfect: it's slow, skewed heavily in favor of rightsholders, and illegally restricts free expression by forcing would-be speakers to ask the government in advance for permission through an arbitrary process.

Mexico's new copyright law mentions a possible equivalent proceeding but leaves it maddeningly undefined — and certainly does nothing to remedy the defects in the US process. Recall that USMCA is a trade agreement, supposedly designed to put all three countries on equal footing — but Americans have the benefit of more than two decades' worth of exemptions to this terrible rule, while Mexicans will have to labor under its full weight until (and unless) they can use this undefined process to secure a comparable list of exemptions. And even then, they won't have the flexibility offered by fair use under US law.

Notice and Takedown

Section 512 of the US DMCA created a "notice and takedown" rule that allows rightsholders or their representatives to demand the removal of works without any showing of evidence or finding of fact that their copyrights were infringed. This has been a catastrophe for free expression, allowing the removal of material without due care or even through malicious, fraudulent acts (the author of this article had his *New York Times* bestselling novel improperly removed from the Internet by careless lawyers for Fox Entertainment, who mistook it for an episode of a TV show of the same name).

As bad as America's notice and takedown system is, Mexico's is now worse.
In America, online services that honor notice and takedown get a "safe harbor" — meaning that they are not considered liable for their users' copyright infringements. However, online services in the US that believe a user's content is noninfringing may ignore it, and they are only liable at all if they meet the tests for "secondary liability" for copyright infringement, something that is far from automatic. If the rightsholder sues, the service may end up in court alongside their user, but the service can still rely on the safe harbor in relation to other works published by other users, provided they remove them upon notice of infringement.

The Mexican law makes it a strict requirement to remove content. Under Article 232 Quinquies (II), providers must honor *all* takedown demands by copyright owners, even obviously overreaching ones, or they face fines of UMA1,000-20,000.

Further, Article 232 Quinquies (III) of the Mexican law allows anyone claiming to be an infringed-upon rightsholder to obtain the personal information of the alleged infringer. This means that gangsters, thin-skinned public officials, stalkers, and others can use fraudulent copyright claims to unmask their critics. Who will complain about corrupt police, abusive employers, or local crime-lords when their personal information can be retrieved with such ease? We recently defended the anonymity of a person who questioned their religious community, when the religious organization tried to use the corresponding part of the DMCA to identify them. In the name of copyright, the law gives new tools to anyone with power to stifle dissent and criticism.

This isn't the only "chilling effect" in the Mexican law. Under Article 114 Octies (II), a platform must comply with takedown requests for mere links to a Web-page that is allegedly infringing. Linking, by itself, is not an infringement in the United States or Canada, and its legal status is contested in Mexico. There are good reasons why linking is not infringement: It's important to be able to talk about speech elsewhere on the Internet and to share facts, which may include the availability of copyrighted works whose license or infringement status is unknown. Besides that, Web-pages change all the time: if you link to a page that is outside of your control and it is later updated in a way that infringes copyright, *you* could be the target of a takedown request.

Cybersecurity

Central to the cybersecurity issue is Article 114 Bis, which establishes a new kind of protection for "Technical Protection Measures" (TPMs) this includes rightsholder technologies commonly known as Digital Rights Management (DRM), but it also includes basic encryption and other security measures that prevent access to copyrighted software. These are the familiar, dreaded locks that stop you from refilling your printer's ink cartridge, using an unofficial App Store with your phone or game console, or watching a DVD from overseas in your home DVD player. Sometimes there is a legitimate security purpose to restricting the ability to modify the software in a device, but when you as the owner of the device aren't allowed to do so, serious problems arise and you become *less* able to ensure your device security.

Under the US system, it is an offense to bypass these TPMs when they control access to a copyrighted work, even when no copyright infringement takes place. If you have to remove a TPM to modify your printer to accept third-party ink or your car to accept a new engine part, you do not violate copyright — but you still violate this extension of copyright *law*.

Unsurprisingly, manufacturers have aggressively adopted TPMs because these allow them to control both their customers and their competitors. A company whose phone or game console is locked to a single, official App Store can monopolize the market for software for their products, skimming a percentage from every app sold to every owner of that device.

Customers cannot lawfully remove the TPM to use a third-party app-store, and competitors can't offer them the tools to unlock their devices. "Trafficking" in these tools is a crime in the USA, punishable by a five-year prison sentence and a $500,000 fine.

But the temptation to use a TPM isn't limited to controlling customers and competitors: companies that use TPMs also get to decide who can reveal the defects in their products. Computer programs inevitably have bugs, and some of these bugs present terrible cybersecurity risks. Security defects allow hackers to remotely take over your car and drive it off the road, alter the ballot counts in elections, wirelessly direct your medical implants to kill you, or stalk and terrorize people.

The only reliable way to discover these defects before they can be weaponized is to subject products and systems to independent scrutiny. As the renowned security expert Bruce Schneier says, "Anyone can design a security system that works so well they can't think of a way to defeat it. That doesn't mean it works, that just means it works against people stupider than them."

Independent security research is incompatible with laws protecting TPMs. In order to investigate systems and report on their defects, security researchers must be free to bypass TPMs, extract the software from the device, and subject it to testing and analysis. When security researchers *do* discover defects, it's common for companies to deny that they exist, or that they are important, painting the matter as a "he said/she said" dispute.

But these disputes have a simple resolution: security researchers routinely publish "proof of concept" code that allows anyone to independently verify their findings. This is simple scientific best practice: since the Enlightenment, scientists have published their findings and invited others to replicate them, a process that is at the core of the Scientific Method.

Section 1201 of the US Digital Millennium Copyright Act (DMCA 1201) defines a process for resolving disputes between TPMs and fundamental human rights. Every three years, the US Copyright Office hears petitions from people whose fundamental rights have been compromised by the TPM law, and grants exemptions to it.

The US government has repeatedly acknowledged that TPMs interfere with security research and granted explicit exemptions to the TPM rule for security research. These exemptions are weak (the US statute does not give the Copyright Office authority to authorize security researchers to publish proof-of-concept code), but it still provides much-needed surety for researchers attempting to warn us that we are in danger from our devices. When powerful corporations threaten security researchers in attempts to silence them, the Copyright Office's exemptions can give them the courage to publish anyway, protecting all of us.

The US exemptions process is weak and inadequate. The Mexican version of this process is even weaker, and even more inadequate (the law doesn't even bother to define how it will work, and merely suggests that some process will be created in the future).

Article 114 Quater (I) of Mexico's law does contain a vague offer of protection for security research, similar to an equally vague assurance in the DMCA. The DMCA has been US law for 22 years, and in all that time, no one has ever used this clause to defend themselves.

To understand why, it is useful to examine the text of the Mexican law. Under the Mexican law, security researchers are only protected if their "sole purpose" is "testing, investigating or correcting the security of that computer, computer system or network." It is rare for a security researcher to have only one purpose: they want to provide the knowledge they glean to the necessary parties so that security flaws do not harm any of the users of similar technology. They may also want to protect the privacy and autonomy of users of a computer, system, or network in ways that conflict with what the manufacturer would view as the security of the device.

Likewise, the Mexican law requires that security researchers be operating in "good faith," creating unquantifiable risk. Researchers often disagree with manufacturers about the appropriate way to investigate and disclose security vulnerabilities. The vague statutory provision for security testing in the United States was far too unreliable to successfully foster essential security research, something that even the US Copyright Office has now repeatedly acknowledged.

The bottom line: our devices cannot be made more secure if independent researchers are prohibited from auditing them. The Mexican law will deter this activity. It will make Mexicans less secure.

Cybersecurity is intimately bound up with human rights. Insecure voting machines can compromise elections, and even when they are not hacked, the presence of insecurities robs elections of legitimacy, leading to civic chaos.

Civil society groups engaged in democratic political activity around the world have been attacked by commercial malware that uses security defects to invade their devices, subjecting them to illegal surveillance, kidnapping, torture, and even murder.

One such product, the NSO Group's Pegasus malware, was implicated in the murder of Jamal Khashoggi. That same tool was used to target Mexican investigative journalists, human rights defenders, even Mexican children whose parents were investigative journalists.

Defects in our devices expose us to politically motivated surveillance, but they also expose us to risk from organized criminals, for example, "stalkerware" can enable human traffickers to monitor their victims.

Digital rights are human rights. Without the ability to secure our devices, we cannot fully enjoy our familiar, civic, political, or social lives.

Self-determination

The Mexican law contains three troubling provisions:

I. Copyright filters: these automated censorship systems remove content from the Internet without human review and are a form of "prior restraint" ("prior censorship" in the Mexican legal parlance), which is illegal under Article 13 of the American Convention on Human Rights, which Mexico's Supreme Court has affirmed is part of Mexican free speech law (Mexico has an outstanding set of constitutional protections for free expression).
II. Technical Protection Measures: "TPMs" (including "digital rights management" or "DRM") are the digital locks that manufacturers use to constrain how owners of their products may use them, and to create legal barriers to competing products and embarrassing disclosures of security defects in their products. As with the US copyright system, Mexico's system does not create reliable exemptions for lawful conduct.
III. Notice and Takedown: A system allowing anyone purporting to be a copyright holder to have material swiftly removed from the Internet, without any judicial oversight or even presentation of evidence. The new Mexican law can easily be abused by criminals and corrupt officials who can use copyright to force online service providers to turn over the sensitive personal details of their critics, simply by pretending to be the victims of copyright infringement.

This system has grave implications for Mexicans' human rights, beyond free expression and cybersecurity.

Implicated in this new system are Mexicans' rights to education, repair, and adaptation for persons with disability.

Unfit for purpose

The new law *does* contain language that seems to protect these activities, but that language is deceptive, as the law demands that Mexicans satisfy unattainable conditions and subject themselves to vague promises, with dire consequences for getting it wrong. There are four ways in which these exemptions are unfit for purpose:

1. **Sole Purpose.** The exemptions specify that one must act for the "sole purpose" of the exempted activity — a security researcher must be investigating a device for the sole purpose of fixing its defects, but arguably not to advance the state of security research in general, or to protect the privacy and autonomy of users of a computer, system, or network in ways that conflict with what the manufacturer would view as the security of the device.
2. **Noncommercial.** The exemptions also frequently cover only "noncommercial" actors, implying that you can only modify a system if you can do so yourself, or if you can find someone else to do it for free. If you are blind and want to convert an ebook so that you can read it with your screenreader, you have to write the code yourself or find a volunteer who'll do it for you — you can't pay someone else to do the work.
3. **Good faith.** The exemptions frequently require that anyone who uses them must be acting in "good faith," an imprecise term that can be a matter of opinion when corporate interests conflict with those of researchers. If a judge doesn't belief you were acting in good faith, you could face both fines and criminal sanctions.
4. **No tools.** Even if you are confident that you are acting for the sole purpose of exercising an exemption and doing so non commercially and in good faith, you are still stuck. Because while the statute recognizes in general terms that there could be a process to create further exemptions for people who bypass digital locks, it does *not* provide a similar process for those who make tools for those purposes.

The defects in the Mexican law are largely present in the US law from which they were copied. It's telling that no US defendant has *ever* successfully used any of the statutory exemptions, not in 22 years. Indeed, the US Copyright Office has repeatedly affirmed that these exemptions do not adequately protect legitimate conduct with the clarity that would be required for them to be effective.

Education

The US experience reveals the ways that badly drafted copyright law can interfere with education:

- Educational materials are removed from the Internet due to incorrect or fraudulent copyright claims, without warning, leaving teachers who relied on those materials with holes in their curriculum;

- Educational materials are automatically removed from the Internet due to copyright filter errors, also stranding teachers with missing curricular materials; and
- Educators cannot make lawful use of the materials purchased for their students because they are blocked by TPMs that they are legally prohibited from bypassing.

Right to Repair

Increasingly, dominant firms have used control over repairs as sources of undeserved, monopoly profits. By controlling repair, firms can not only force customers to pay higher prices for repairs and to use more expensive, more profitable original parts — they can also force customers to discard their devices and buy new ones, by declaring them to be beyond repair.

Enacting legal penalties for bypassing TPMs is a gift to any company seeking to control repairs. Companies use TPMs so that even after the correct part is installed, the device refuses to work unless a company technician inputs an unlock code.

Disturbingly, this conduct has spread to the world of medical devices, where multinational corporations use TPMs to prevent repairs to ventilators.

At the forefront of the Right to Repair movement are farmers, whose must contend with both a remote location (far from the authorized technicians) and urgent timescales (you need to get your crop in *before* the storm hits, even if the authorized technician can't make it out before then).

During the global pandemic, many of us are living under conditions familiar to farmers, dangling at the end of a long, slow, unreliable supply chain and confronted by urgent needs.

Technology is primarily designed in the global north by engineers and product specialists whose lives are very different from people in the global south. Mexican people have long relied on their own ingenuity and technical mastery to modify, repair and adapt systems built by distant people in foreign lands to suit their own lived experience in their own land.

Mexican law does not provide any clear protection for repairs that require access to or use of copyrighted works.

Repair is a vital part of self-determination, and the Mexican copyright law puts the interests of monopolistic, rent-seeking foreign companies ahead of the rights of Mexican people to decide how they will use their own property.

Adaptation and Disability

Nowhere is the need for technological self-determination more keenly felt than when it involves people with disabilities.

A rallying cry of the disability movement is "nothing about us without us" -- meaning, among other things, that each person with a disability should have the final say about how their technology works.

The creation of assistive adaptations by and with people with disabilities has been a boon for everyone: the principle of "universal design" — design that enables every body and every mind to participate fully in life — means that all of us benefit, whether that's using closed captions to watch a video in a noisy environment or to learn a foreign language; or using screen magnifiers to read small or low-contrast text.

Digital technology holds the promise of incredible advances in universal design: automated caption-generation and scene description, adaptive systems that anticipate a user's intention based on statistical analysis of their historic usage, predictive text input, and more. Some of these adaptations will come from original manufacturers, but many will come from the community of those using the technology.

People with disabilities should face *no* conditions as to how they adapt their technology or who they chose to work with to make adaptations on their behalf. None. Period.

People with disabilities do not each necessarily have the technical knowledge to modify their own devices, by themselves, to suit their needs. This is why the exemption for people with disabilities in the Mexican law is wholly inadequate. It precludes hiring someone else to effect a modification (that would be "commercial activity") and it

forecloses on general-purpose research that helps with adaptation because no one is allowed to provide technology or services to aid in bypassing TPMs to adapt technology. Under the Mexican law, the way that, say, a blind person is permitted to make a work accessible is to:

1. become a cybersecurity expert;
2. discover a defect in the e-reader software;
3. write a piece of software to liberate the ebook they want to read;

No one is allowed to offer them technical assistance, and they may not share their accomplishment to help others. It would be a joke, if it wasn't so grimly unfunny.

There can be no question that all of this is by intent or extreme negligence. Not only did Mexico's Congress have the benefit of 22 years' worth of documented problems with the US version of this law, they also had an easy remedy to these problems. All they had to do was say, "You are allowed to bypass a TPM provided that you are not violating someone's copyright." That's it. Rather than larding their exemptions with unattainable and vague conditions, Mexico's lawmakers could have articulated a crisp, bright-line rule that anyone could follow: don't bypass TPMs in a way that's connected to copyright infringement, and you're fine.

They didn't.

National Sovereignty

Trade agreements are billed as creating level playing fields between nations to their mutual benefit. But decades of careful scholarship show that poorer nations typically come off worse through these agreements, even when they are subjected to the same rules, because the same rules don't have the same effect on different countries. Besides that, Mexico has now adopted *worse* rules than its trade partners.

To understand how this works, we need only look to the history of the USA's relationship with the copyrights and patents of foreign persons and firms. When the USA was a new, poor, developing nation that imported more copyrights and patents than it exported it did not honor foreigners' copyrights or patents, but rather allowed its people and its businesses to use them without paying, to develop the nation. Once the USA became an industrial and cultural powerhouse, it entered into agreements with other countries for mutual recognition of one another's copyrights and patents in order to extract wealth based on rights to its technology and culture.

But the USA has a short memory for what it once considered just; it has made the foreign enforcement of US copyrights a trade priority for decades, often demanding that its trading partners extend more legal privileges to US copyright holders than they (or anyone else) receive at home in the United States; and preventing local users from benefiting from fair use or other balancing rights available in the United States. The poorer the trading partner, the more the US government and US industry expect it to surrender.

Mexico's copyright is a sad and enervating example of this principle in action. The law imposes restrictions that do not — and could not — exist under US law, because they violate US Constitutional principles (these laws *also* violate Mexican Constitutional principles).

For example, Mexico's copyright law effectively mandates copyright filters, which automatically screen Mexican Internet users' expressive speech and arbitrarily censor some of it based on an algorithm's decision to treat it as a copyright infringement.

Neither the US nor Canada has such a requirement, which puts Mexican online firms at a significant trade disadvantage relative to its "equal partners" under USMCA. These filters can be very costly to develop and maintain. For example, YouTube has invested over $100,000,000 to develop its content filtering systems. Those are costs that Mexican online services will have to shoulder if they compete with Canadian and US firms, while their counterparts in the USA and Canada face no such requirement.

Just as dangerous to Mexico's prosperity are its new rules on TPMs (including "Digital Rights Management" or DRM). The US version of these rules, Section 1201 of the Digital Millennium Copyright Act (DMCA 1201), sets out a procedure for granting exemptions to the ban on bypassing digital locks. The Mexican version holds out the possibility of creating such a process but does not describe it.

Even if the Mexican government eventually develops an equivalent procedure, people and businesses in the USA will still enjoy more flexibility than their Mexican counterparts: that's because the US system has produced a long, extensive list of exemptions that Mexico will have to develop on its own, through whatever process it eventually creates (if it ever does).

These rules interfere with many key activities, including accessibility adaptations for people with disabilities, education, and repair, including repair of agricultural and medical equipment, most of which come from US firms, who can charge Mexican consumers and the Mexican health-care system arbitrarily high prices for repairs, without having to fear competition from Mexican repair shops. They can also unilaterally declare equipment to be "beyond repair" and insist that it be replaced at full cost.

All of this happened even as the US government is facing a legal challenge to its ban on circumventing access controls that might see the law struck down in the USA, but still in force in Mexico.

Mexico's new copyright law also includes a much narrower set of limitations and exceptions than either the US ("fair use") or Canadian ("fair dealing") systems provide for. That means that Mexican consumers must pay US and Canadian firms for activities that people in the USA and Canada can undertake for free.

This is especially dangerous when coupled with Mexico's new Notice and Takedown system, which allows anyone to have content removed from the Internet simply by claiming to be the victim of copyright infringement. Under the US system, companies that do not act on these notices are only penalized if they actually commit indirect copyright infringement. But Mexico's version of these rules (Article 232 Quinquies (II)) forces compliance with a copyright owner's takedown demands even if the platform believes the content is a noninfringing use.

That means that US firms and individuals can remove material — for example, negative reviews quoting a book or warnings about defective software — from Mexican online services, while such a tactic could be ignored by US online services.

This asymmetry is not new. It is a recurring feature of US-Mexico trade relations, something that was already present under NAFTA, but which USMCA expands to the digital realm through this outrageous copyright law.

Under NAFTA, US exports of corn syrup to Mexico surged, and Mexican anti-obesity campaigners who tried to stem the tide were rebuffed by the rules of the trade agreement.

As a result, Mexico's obesity epidemic is among the worst in the region, as is Mexican consumption of processed food. Julio Berdegué, a regional representative of the Food and Agriculture Organization of the United Nations, said "Unfortunately, Mexico is one of the leading countries in obesity, both in men and women and children. It is a very serious problem." Mexico's export sector has also shifted, with much of the fresh fruits and vegetables that once made up the country's dietary staples now being exported to the USA.

Mexico's new copyright law only exacerbates this problem. Mexico's TPM rules hamper the security research that is the country's best hope to secure its people's digital devices. During Mexico's "sugar wars," activists were hacked with weapons sold by the cyber-arms dealer NSO Group, as part of an illegal campaign to neutralize their opposition to the powerful US sugar industry. That attack exploited a vulnerability in the activists' mobile apps, and Mexico's new copyright law impedes the work of those who would reveal those vulnerabilities.

The history of Latin America is filled with shameful instances of US interference to improve its prosperity at the expense of its southern neighbors.

The passage of the Mexican copyright law, rushed through in the middle of the pandemic without adequate consultation or debate, continues this denial of dignity and sovereignty. Lobbyists for just laws don't fear public scrutiny, after all. The only reason to undertake a lawmaking exercise like this under the shroud of haste and obscurity is to sneak it through before the public knows what's going on and can organize in opposition to it.

Appendix: Detailed legislative analysis

By Kit Walsh, Senior Staff Attorney

Mexico has just adopted a terrible new copyright law, thanks to pressure from the United States (and specifically from the copyright maximalists that hold outsized influence on US foreign policy).

This law closely resembles the Digital Millennium Copyright Act enacted in the US 1998, with a few differences that make it much, much worse.

We'll start with a quick overview, and then dig deeper.

"Anti-Circumvention" Provision

The Digital Millennium Copyright Act included two very significant provisions. One is DMCA 1201, the ban on circumventing technology that restricts access to or use of copyrighted works (or sharing such technology). Congress was thinking about people ripping DVDs to infringe movies or descrambling cable channels without paying, but the law it passed goes much, much farther. In fact, some US courts have interpreted it to effectively eliminate fair use if a technological restriction must be bypassed.

In the past 22 years, we've seen DMCA 1201 interfere with media education, remix videos, security research, privacy auditing, archival efforts, innovation, access to books for people with print disabilities, unlocking phones to work on a new carrier or to install software, and even the repair and reverse engineering of cars and tractors. It turns out that there are a lot of legitimate and important things that people do with culture and

with software. Giving copyright owners the power to control those things is a disaster for human rights and for innovation.

The law is sneaky. It includes exemptions that sound good on casual reading, but are far narrower than you would imagine if you look at them carefully or in the context of 22 years of history. For instance, for the first 16 years under DMCA 1201, we tracked dozens of instances where it was abused to suppress security research, interoperability, free expression, and other noninfringing uses of copyrighted works.

It's a terrible, unconstitutional law, which is why EFF is challenging it in court.

Unfortunately, Mexico's version is even worse. Important cultural and practical activities are blocked by the law entirely. In the US, we and our allies have used Section 1201's exemption process to obtain accommodations for documentary filmmaking, teachers to use video clips in the classroom, for fans to make noncommercial remix videos, to unlock or jailbreak your phone, to repair and modify cars and tractors, to use competing cartridges in 3D printers, and for archival preservation of certain works. Beyond those, we and our allies have been fighting for decades now to protect the full scope of noninfringing activities that require circumvention, so that journalism, dissent, innovation, and free expression do not take a back seat to an overbroad copyright law. Mexico's version has an exemption process as well, but it is far more limited, in part because Mexico doesn't have our robust fair use doctrine as a backstop.

This is not a niche issue. The U.S. Copyright Office received nearly 40,000 comments in the 2015 rulemaking. In response to a petition signed by 114,000 people, the U.S. Congress stepped in to correct the rulemaking authorities when they allowed the protection for unlocking phones to lapse in 2012.

"Notice-and-Takedown" Provision

In order to avoid the uncertainty and cost of litigation (which would have bankrupted every online platform and deprived the public of important opportunities to speak and connect), Congress enacted Section 512, which provides a "safe harbor" for various Internet-related activities. To stay in the safeharbor, service providers must comply with several conditions, including "notice and takedown" procedures that give copyright holders a quick and easy way to disable access to allegedly infringing content. Section 512 also contains provisions allowing users to challenge improper takedowns. Without these protections, the risk of potential copyright liability would prevent many online intermediaries from providing services such as hosting and transmitting user-generated content. Thus the safe harbors have been essential to the growth of the Internet as an engine for innovation and free expression.

But Section 512 is far from perfect, and again, the Mexican version is worse.

First of all, a platform can be fined simply for failing to abide by takedown requests — even if the takedown is spurious and the targeted material does not infringe. In the US, if they opted out of the safe harbor, they would still only be liable if someone sued them and proved secondary liability. Platforms are already incentivized to take down content

on a hair trigger to avoid potential liability, and the Mexican law provides new penalties if they don't.

Second, we have long catalogued the many problems that arise when you provide the public a way to get material removed from the public sphere without any judicial involvement. It is sometimes deployed maliciously, to suppress dissent or criticism, while other times it is deployed with lazy indifference about whether it is suppressing speech that isn't actually infringing.

Third, by requiring that platforms prevent material from reappearing after it is taken down, the Mexican law goes far beyond DMCA 512 by essentially mandating automatic filters. We have repeatedly written about the disastrous consequences of this kind of automated censorship.

So that's the short version. For more detail, read on. But if you are in Mexico, consider first exercising your power to fight back against this law.

In-depth legislative analysis and commentary

The text of the law is presented in full in blockquotes. EFF's analysis has been inserted following the relevant provisions.

Provisions on Technical Protection Measures

> Article 114 Bis.- In the protection of copyright and related neighboring rights, effective technological protection measures may be implemented and information on rights management. For these purposes:
>
> I. An effective technological protection measure is any technology, device or component that, in the normal course of its operation, protects copyright, the right of the performer or the right of the producer of the phonogram, or that controls access to a work, to a performance, or to a phonogram. Nothing in this section shall be compulsory for persons engaged in the production of devices or components, including their parts and their selection, for electronic, telecommunication or computer products, provided that said products are not destined to carry Unlawful conduct, and

This provision adopts a broad definition of 'technological protection measure' or TPM, so that a wide range of encryption and authentication technologies will trigger this provision. The reference to copyright is almost atmospheric, since the law is not substantively restricted to penalizing those who bypass TPMs for infringing purposes.

> II. The information on rights management are the data, notice or codes and, in general, the information that identifies the work, its author, the interpretation, the performer, the phonogram, the producer of the phonogram, and to the holder of any right over them, or information about the terms and conditions of use of the work, interpretation or execution,

> and phonogram, and any number or code that represents such information, when any of these information elements is attached to a copy or appear in relation to the communication to the public of the same.
>
> In the event of controversies related to both fractions, the authors, performers or producers of the phonogram, or holders of respective rights, may exercise civil actions and repair the damage, in accordance with the provisions of articles 213 and 216 bis. of this Law, independently to the penal and administrative actions that proceed.
>
> Article 114 Ter.- It does not constitute a violation of effective technological protection measures when the evasion or circumvention is about works, performances or executions, or phonograms whose term of protection granted by this Law has expired.

In other words, the law doesn't prohibit circumvention to access works that have entered the public domain. This is small comfort: Mexico has one of the longest copyright terms in the world.

> Article 114 Quater.- Actions of circumvention or evasion of an effective technological protection measure protection that controls access to a work, performance or execution, or phonogram protected by this Law, shall not be considered a violation of this Law, when:

This provision lays out some limited exceptions to the general rule of liability. But those exceptions won't work. After more than two decades of experience with the DMCA in the United States, it is clear that when regulators can't protect fundamental rights by attempting to imagine in advance and authorize particular forms of cultural and technological innovation. Furthermore, several of these exemptions are modeled off of stale US exemptions that have proven completely inadequate in practice. The US Congress could plead ignorance in the 90s; legislators have no excuse today.

It gets worse: because Mexico does not have a general fair use rule, innovators would be entirely dependent on these limited exemptions.

> I. Non-infringing reverse engineering processes carried out in good faith with respect to the copy that has been legally obtained of a computer program that effectively controls access in relation to the particular elements of said computer programs that have not been readily available to the person involved in that activity, with the sole purpose of achieving the interoperability of an independently created computer program with other programs;

If your eyes glazed over at "reverse engineering" and you assumed this covered reverse engineering generally, you would be in good company. This exemption is sharply limited, however. The reverse engineering is only authorized for the "computer program that effectively controls access" and is limited to "elements of said computer programs that have not been readily available." It does not mention reverse engineering of

computer programs that are subject to access controls – in part because the US Congress was thinking about DVD encryption and cable TV channel scrambling, not about software. If you circumvent to confirm that the software is the software claimed, do you lose access to this exemption because the program was already readily available to you? Even if you had no way to verify that claim without circumvention? Likewise, your "sole purpose" has to be achieving interoperability of an independently created computer program with other programs. It's not clear what "independently" means, and this is not a translation error – the US law is similarly vague. Finally, the "good faith" limitation is a trap for the unwary or unpopular. It does not give adequate notice to a researcher whether their work will be considered to be done in "good faith." Is reverse engineering for competitive advantage a permitted activity or not? Why should any non-infringing activity be a violation of copyright-related law, regardless of intent?

If you approach this provision as if it authorizes "reverse engineering" or "interoperability" generally you are imagining an exemption that is far more reasonable than what the text provides.

In the US, for example, companies have pursued litigation over interoperable garage door openers and printer cartridges all the way to appellate courts. It has never been this provision that protected interoperators. The Copyright Office has recognized this in granting exemptions to 1201 for activities like jailbreaking your phone to work with other software.

> II. The inclusion of a component or part thereof, with the sole purpose of preventing minors from accessing inappropriate content, online, in a technology, product, service or device that itself is not prohibited;

It's difficult to imagine something having this as the 'sole purpose.' In any event, this is far too vague to be useful for many.

> III. Activities carried out by a person in good faith with the authorization of the owner of a computer, computer system or network, performed for the sole purpose of testing, investigating or correcting the security of that computer, computer system or network;

Again, if you skim this provision and believe it protects "computer security," you are giving it too much credit. Most security researchers do not have the "sole purpose" of fixing the particular device they are investigating; they want to provide that knowledge to the necessary parties so that security flaws do not harm any of the users of similar technology. They want to advance the state of understanding of secure technology. They may also want to protect the privacy and autonomy of users of a computer, system, or network in ways that conflict with what the manufacturer would view as the security of the device. The "good faith" exemption again creates legal risk for any security researcher trying to stay on the right side of the law. Researchers often disagree with manufacturers about the appropriate way to investigate and disclose security vulnerabilities. The vague statutory provision for security testing in the United States was far too unreliable to successfully foster essential security research, something that even the US Copyright Office has now acknowledged. Restrictions on engaging in and

sharing security research are also part of our active lawsuit seeking to invalidate Section 1201 as a violation of free expression.

> IV. Access by the staff of a library, archive, or an educational or research institution, whose activities are non-profit, to a work, performance, or phonogram to which they would not otherwise have access, for the sole purpose to decide if copies of the work, interpretation or execution, or phonogram are acquired;

This exemption too must be read carefully. It is not a general exemption for noninfringing archival or educational uses. It is instead an extremely narrow exemption for deciding whether to purchase a work. When archivists want to break TPMs to archive an obsolete format, when educators want to take excerpts from films to discuss in class, when researchers want to run analytical algorithms on video data to measure bias or enhance accessibility, this exemption does nothing to help them. Several of these uses have been acknowledged as legitimate and impaired by the US Copyright Office.

> V. Non-infringing activities whose sole purpose is to identify and disable the ability to compile or disseminate undisclosed personal identification data information, reflecting the online activities of a natural person, in a way that it does not to affect the ability of any person to gain access to a work, performance, or phonogram;

This section provides a vanishingly narrow exception, one that can be rendered null if manufacturers use TPMs in such a way that you cannot protect your privacy without bypassing the same TPM that prevents access to a copyrighted work. And rightsholders have repeatedly taken this very position in the United States. Besides that, the wording is tremendously outdated; you may want to modify the software in your child's doll so that it doesn't record their voice and send it back to the manufacturer; that is not clearly "online activities" – they're simply playing with a doll at home. In the US, "personally identifiable information" also has a meaning that is narrower than you might expect.

> VI. The activities carried out by persons legally authorized in terms of the applicable legislation, for the purposes of law enforcement and to safeguard national security;

This would be a good model for a general exemption: you can circumvent to do noninfringing things. Lawmakers have recognized, with this provision, that the ban on circumventing TPMs could interfere with legitimate activities that have nothing to do with copyright law, and provided a broad and general assurance that these noninfringing activities will not give rise to liability under the new regime.

> VII. Non-infringing activities carried out by an investigator who has legally obtained a copy or sample of a work, performance or performance not fixed or sample of a work, performance or execution, or phonogram with the sole purpose of identifying and analyzing flaws in technologies for encoding and decoding information;

This exemption again is limited to identifying flaws in the TPM itself, as opposed to analyzing the software subject to the TPM.

> VIII. Non-profit activities carried out by a person for the purpose of making accessible a work, performance, or phonogram, in languages, systems, and other special means and formats, for persons with disabilities, in terms of the provisions in articles 148, section VIII and 209, section VI of this Law, as long as it is made from a legally obtained copy, and

Why does accessibility have to be nonprofit? This means that companies trying to serve the needs of the disabled will be unable to interoperate with works encumbered by TPMs.

> IX. Any other exception or limitation for a particular class of works, performances, or phonograms, when so determined by the Institute at the request of the interested party based on evidence.

It is improper to create a licensing regime that presumptively bans speech and the exercise of fundamental rights, and then requires the proponents of those rights to prove their rights to the government in advance of exercising them. We have sued the US government over its regime and the case is pending.

> Article 114 Quinquies.- The conduct sanctioned in article 232 bis shall not be considered as a violation of this Law:

These are the exemptions to the ban on providing technology capable of circumvention, as opposed to the act of circumventing oneself. They have the same flaws as the corresponding exemptions above, and they don't even include the option to establish new, necessary exemptions over time. This limitation is present in the US regime, as well, and has sharply curtailed the practical utility of the exemptions obtained via subsequent rulemaking. They also do not include the very narrow privacy and library/archive exemptions, meaning that it is unlawful to give people the tools to take advantage of those rights.

> I. When it is carried out in relation to effective technological protection measures that control access to a work, interpretation or execution, or phonogram and by virtue of the following functions:
>
> a) The activities carried out by a non-profit person, in order to make an accessible format of a work, performance or execution, or a phonogram, in languages, systems and other modes , means and special formats for a person with a disability, in terms of the provisions of articles 148, section VIII and 209, section VI of this Law, as long as it is made from a copy legally obtained;
>
> b) Non-infringing reverse engineering processes carried out in good faith with respect to the copy that has been legally obtained of a computer program that effectively controls access in relation to the particular elements of said computer programs that have not been readily available to

the person involved in that activity, with the sole purpose of achieving the interoperability of an independently created computer program with other programs;

c) Non-infringing activities carried out by an investigator who has legally obtained a copy or sample of a work, performance or performance not fixed or sample of a work, performance or execution, or phonogram with the sole purpose of identifying and analyzing flaws in technologies for encoding and decoding information;

d) The inclusion of a component or part thereof, with the sole purpose of preventing minors from accessing inappropriate content, online, in a technology, product, service or device that itself is not prohibited;

e) Non-infringing activities carried out in good faith with the authorization of the owner of a computer, computer system or network, carried out for the sole purpose of testing, investigating or correcting the security of that computer, computer system or network, and

f) The activities carried out by persons legally authorized in terms of the applicable legislation, for the purposes of law enforcement and to safeguard national security.

II. When it is carried out in relation to effective technological measures that protect any copyright or related right protected in this Law and by virtue of the following functions:

a) Non-infringing reverse engineering processes carried out in good faith with respect to the copy that has been legally obtained of a computer program that effectively controls access in relation to the particular elements of said computer programs that have not been readily available to the person involved in that activity, with the sole purpose of achieving the interoperability of an independently created computer program with other programs, and

b) The activities carried out by persons legally authorized in terms of the applicable legislation, for the purposes of law enforcement and to safeguard national security.

Article 114 Sexies.- It is not violation of rights management information, the suspension, alteration, modification or omission of said information, when it is carried out in the performance of their functions by persons legally authorized in terms of the applicable legislation, for the effects of law enforcement and safeguarding national security.

Article 232 Bis.- A fine of 1,000 UMA to 20,000 UMA will be imposed on whoever produces, reproduces, manufactures, distributes, imports, markets, leases, stores, transports, offers or makes available to the public,

> offer to the public or provide services or carry out any other act that allows having devices, mechanisms, products, components or systems that:

Again, it's damaging to culture and innovation to ban non-infringing activities and technologies simply because they circumvent access controls.

> I. Are promoted, published or marketed with the purpose of circumventing effective technological protection measure;
>
> II. Are used predominantly to circumvent any effective technological protection measure, or

This seems to suggest that a technologist who makes a technology with noninfringing uses can be liable because others, independently, have used it unlawfully.

> III. Are designed, produced or executed with the purpose of avoiding any effective technological protection measure.
>
> Article 232 Ter.- A fine of 1,000 UMA to 10,000 UMA will be imposed, to those who circumvent an effective technological protection measure that controls access to a work, performance, or phonogram protected by this Law.
>
> Article 232 Quáter.- A fine of 1,000 UMA to 20,000 UMA will be imposed on those who, without the respective authorization:
>
> I. Delete or alter rights management information;

This kind of vague prohibition invites nuisance litigation. There are many harmless ways to 'alter' rights management information – for accessibility, convenience, or even clarity. In addition, when modern cameras take pictures, they often automatically apply information that identifies the author. This creates privacy concerns, and it is a common social media practice to strip that identifying information in order to protect users. While large platforms can obtain a form of authorization via their terms of service, it should not be unlawful to remove identifying information in order to protect the privacy of persons involved in the creation of a photograph (for instance, those attending a protest or religious event).

> II. Distribute or import for distribution, rights management information knowing that this information has been deleted, altered, modified or omitted without authorization, or
>
> III. Produce, reproduce, publish, edit, fix, communicate, transmit, distribute, import, market, lease, store, transport, disclose or make available to the public copies of works, performances, or phonograms, knowing that the rights management information has been deleted, altered, modified or omitted without authorization.

Federal Criminal Code

> Article 424 bis.- A prison sentence of three to ten years and two thousand to twenty thousand days fine will be imposed:
>
> I. Whoever produces, reproduces, enters the country, stores, transports, distributes, sells or leases copies of works, phonograms, videograms or books, protected by the Federal Law on Copyright, intentionally, for the purpose of commercial speculation and without the authorization that must be granted by the copyright or related rightsholder according to said law.
>
> The same penalty shall be imposed on those who knowingly contribute or provide in any way raw materials or supplies intended for the production or reproduction of works, phonograms, videograms or books referred to in the preceding paragraph;

This is ridiculously harsh and broad, even in the most generous reading. And the chilling effect of this criminal prohibition will go even further. If one "knows" they are providing paper to someone but do not know that person is using it to print illicit copies, there should be complete legal clarity that they are not liable, let alone criminally liable.

> II. Whoever manufactures, for profit, a device or system whose purpose is to deactivate the electronic protection devices of a computer program, or

As discussed, there are many legitimate and essential reasons for deactivating TPMs.

> III. Whoever records, transmits or makes a total or partial copy of a protected cinematographic work, exhibited in a movie theater or places that substitute for it, without the authorization of the copyright or related rightsholder.

Jail time for filming any part of a movie in a theater is absurdly draconian and disproportionate.

> Article 424 ter.- A prison sentence of six months to six years and five thousand to thirty thousand days fine will be imposed on whoever that sells to any final consumer on the roads or in public places, intentionally, for the purpose of commercial speculation, copies of works, phonograms, videograms or books, referred to in section I of the previous article.
>
> If the sale is made in commercial establishments, or in an organized or permanent manner, the provisions of article 424 Bis of this Code will be applied.

Again, jail for such a violation is extremely disproportionate. The same comment applies to many of the following provisions.

Article 425.- A prison sentence of six months to two years or three hundred to three thousand days fine will be imposed on anyone who knowingly and without right exploits an interpretation or an execution for profit.

Article 426.- A prison term of six months to four years and a fine of three to three thousand days will be imposed, in the following cases:

I. Whoever manufactures, modifies, imports, distributes, sells or leases a device or system to decipher an encrypted satellite signal, carrier of programs, without authorization of the legitimate distributor of said signal;

II. Whoever performs, for profit, any act with the purpose of deciphering an encrypted satellite signal, carrier of programs, without authorization from the legitimate distributor of said signal;

III. Whoever manufactures or distributes equipment intended to receive an encrypted cable signal carrying programs, without authorization from the legitimate distributor of said signal, or

IV. Whoever receives or assists another to receive an encrypted cable signal carrying programs without the authorization of the legitimate distributor of said signal.

Article 427 Bis.- Who, knowingly and for profit, circumvents without authorization any effective technological protection measure used by producers of phonograms, artists, performers, or authors of any work protected by copyright or related rights, it will be punished with a prison sentence of six months to six years and a fine of five hundred to one thousand days.

Article 427 Ter.- To who, for profit, manufactures, imports, distributes, rents or in any way markets devices, products or components intended to circumvent an effective technological protection measure used by phonogram producers, artists or performers, as well as the authors of any work protected by copyright or related rights, will be imposed from six months to six years of prison and from five hundred to one thousand days fine.

Article 427 Quater.- To those who, for profit, provide or offer services to the public intended mainly to avoid an effective technological protection measure used by phonogram producers, artists, performers, or performers, as well as the authors of any protected work. by copyright or related right, it will be imposed from six months to six years in prison and from five hundred to a thousand days fine.

Article 427 Quinquies.- Anyone who knowingly, without authorization and for profit, deletes or alters, by himself or through another person, any rights

management information, will be imposed from six months to six years in prison and five hundred to one thousand days fine.

The same penalty will be imposed on who for profit:

I. Distribute or import for its distribution rights management information, knowing that it has been deleted or altered without authorization, or

II. Distribute, import for distribution, transmit, communicate, or make available to the public copies of works, performances, or phonograms, knowing that rights management information has been removed or altered without authorization.

Notice and takedown provisions

Article 114 Septies.- The following are considered Internet Service Providers:

I. Internet Access Provider is the person who transmits, routes or provides connections for digital online communications without modification of their content, between or among points specified by a user, of material of the user's choosing, or that makes the intermediate and transient storage of that material done automatically in the course of a transmission, routing or provision of connections for digital online communications.

II. Online Service Provider is a person who performs any of the following functions:

a) Caching carried out through an automated process;

b) Storage, at the request of a user, of material that is hosted in a system or network controlled or operated by or for an Internet Service Provider, or

c) Referring or linking users to an online location by using information location tools, including hyperlinks and directories.

Article 114 Octies.- The Internet Service Providers will not be responsible for the damages caused to copyright holders, related rights and other holders of any intellectual property right protected by this Law, for the copyright or related rights infringements that occur in their networks or online systems, as long as they do not control, initiate or direct the infringing behavior, even if it takes place through systems or networks controlled or operated by them or on their behalf, in accordance with the following:

I. The Internet Access Providers will not be responsible for the infringement, as well as the data, information, materials and contents that are transmitted or stored in their systems or networks controlled or operated by them or on their behalf when:

For clarity: this is the section that applies to those who provide your Internet subscription, as opposed to the websites and services you reach over the Internet.

> a) Does not initiate the chain of transmission of the materials or content nor select the materials or content of the transmission or its recipients, and
>
> b) Include and do not interfere with effective standard technological measures, which protect or identify material protected by this law, which are developed through an open and voluntary process by a broad consensus of copyright holders and service providers, which are available from in a reasonable and non-discriminatory manner, and that do not impose substantial costs on service providers or substantial burdens on their network systems.

There is no such thing as a standard technological measure, so this is just dormant poison. A provision like this is in the US law and there has never been a technology adopted according to such a broad consensus.

> II. The Online Service Providers will not be responsible for the infringements, as well as the data, information, materials and content that are stored or transmitted or communicated through their systems or networks controlled or operated by them or on their behalf, and in cases that direct or link users to an online site, when:

First, for clarity, this is the provision that applies to the services and websites you interact with online, including sites like YouTube, Dropbox, Cloudflare, and search engines, but also sites of any size like a bulletin-board system or a server you run to host materials for friends and family or for your activist group.

The consequences for linking are alarming. Linking isn't infringing in the US or Canada, and this is an important protection for public discourse. In addition, a linked resource can change from a non-infringing page to an infringing one.

> a) In an expeditious and effective way, they remove, withdraw, eliminate or disable access to materials or content made available, enabled or transmitted without the consent of the copyright or related rights holder, and that are hosted in their systems or networks, once you have certain knowledge of the existence of an alleged infringement in any of the following cases:
>
> 1. When it receives a notice from the copyright or related rights holder or by any person authorized to act on behalf of the owner, in terms of section III of this article, or

It's extremely dangerous to take a mere allegation as "certain knowledge" given how many bad faith or mistaken copyright takedowns are sent.

> 2. When it receives a resolution issued by the competent authority ordering the removal, elimination or disabling of the infringing material or content.
>
> In both cases, reasonable measures must be taken to prevent the same content that is claimed to be infringing from being uploaded to the system or network controlled and operated by the Internet Service Provider after the removal notice or the resolution issued by the competent authority.

This provision effectively mandates filtering of all subsequent uploads, comparing them to a database of everything that has been requested to be taken down. Filtering technologies are overly broad and unreliable, and cannot make infringement determinations. This would be a disaster for speech, and the expense would also be harmful to small competitors or nonprofit online service providers.

> b) If they remove, disable or suspend unilaterally and in good faith, access to a publication, dissemination, public communication and/or exhibition of the material or content, to prevent the violation of applicable legal provisions or to comply with the obligations derived of a contractual or legal relationship, provided they take reasonable steps to notify the person whose material is removed or disabled.
>
> c) They have a policy that provides for the termination of accounts of repeat offenders, which is publicly known by their subscribers;

This vague provision is also often a sword wielded by rightsholders. When the service provider is essential, such as access to the Internet, termination is an extreme measure and should not be routine.

> d) Include and do not interfere with effective standard technological measures that protect or identify material protected by this Law, which are developed through an open and voluntary process by a broad consensus of copyright holders and service providers, which are available in a reasonable and non-discriminatory manner, and that do not impose substantial costs on service providers or substantial burdens on their systems or networks,

Again, there's not yet any technology considered a standard technological measure.

> e) In the case of Online Service Providers referred to in subsections b) and c) of the section II of article 114 Septies, in addition to the provisions of the immediately preceding paragraph, must not receive a financial benefit attributable to the infringing conduct, when the provider has the right and ability to control the infringing conduct.

This is a bit sneaky and could seriously undermine the safe harbor. Platforms do profit from user activity, and do technically have the ability to remove content – if that's enough to trigger liability or to defeat a safe harbor, then the safe harbor is essentially null for any commercial platform.

> III. The notice referred to in subsection a), numeral 1, of the previous section, must be submitted through the forms and systems as indicated in the regulations of the Law, which will establish sufficient information to identify and locate the infringing material or content.
>
> Said notice shall contain as a minimum:
>
> 1. Indicate of the name of the rightsholder or legal representative and the means of contact to receive notifications;
>
> 2. Identify the content of the claimed infringement;
>
> 3. Express the interest or right regarding the copyright, and
>
> 4. Specify the details of the electronic location to which the claimed infringement refers.
>
> The user whose content is removed, deleted or disabled due to probable infringing behavior and who considers that the Online Service Provider is in error, may request the content be restored through a counter-notice, in which he/she must demonstrate the ownership or authorization he/she has for that specific use of the content removed, deleted or disabled, or justify its use according to the limitations or exceptions to the rights protected by this Law.
>
> The Online Service Provider who receives a counter-notice in accordance with the provisions of the preceding paragraph, must report the counter-notice to the person who submitted the original notice, and enable the content subject of the counter-notice, unless the person who submitted the original notice initiates a judicial or administrative procedure, a criminal complaint or an alternative dispute resolution mechanism within a period not exceeding 15 business days since the date the Online Service Provider reported the counter-notice to the person who submitted the original notice.

It should be made clear that the rightsholder is obligated to consider exceptions and limitations before sending a takedown.

> IV. Internet Service Providers will not be obliged to supervise or monitor their systems or networks controlled or operated by them or on their behalf, to actively search for possible violations of copyright or related rights protected by this Law and that occur online.
>
> In accordance with the provisions of the Federal Law on Telecommunications and Broadcasting, Internet Service Providers may carry out proactive monitoring to identify content that violates human dignity, is intended to nullify or impair rights and freedoms, as well as those that stimulate or advocate violence or a crime.

This provision is sneaky. It says "you don't have to filter, but you're allowed to look for content that impairs rights (like copyright) or a crime (like the new crimes in this law)." Given that the law also requires the platform to make sure that users cannot re-upload content that is taken down, it's cold comfort to say here that they don't have to filter proactively. At best, this means that a platform does not need to include works in its filters until it has received a takedown request for the works in question.

> V. The impossibility of an Internet Service Provider to meet the requirements set forth in this article by itself does not generate liability for damages for violations of copyright and related rights protected by this Law.

This provision is unclear. Other provisions seem to indicate liability for failure to enact these procedures. Likely this means that a platform would suffer the fines below, but not liability for copyright infringement, if it is impossible to comply.

> Article 232 Quinquies.- A fine of 1,000 UMA to 20,000 UMA will be imposed when:
>
> I. Anyone who makes a false statement in a notice or counter-notice, affecting any interested party when the Online Service Provider has relied on that notice to remove, delete or disable access to the content protected by this Law or has rehabilitated access to the content derived from said counter-notice;

This is double-edged: it potentially deters both notices and counternotices. It also does not provide a mechanism to prevent censorship; a platform continues to be obligated to act on notices that include falsities.

> II. To the Online Service Provider that does not remove, delete or disable access in an expedited way to the content that has been the subject of a notice by the owner of the copyright or related right or by someone authorized to act on behalf of the holder, or competent authority, without prejudice to the provisions of article 114 Octies of this Law, or

This is a shocking expansion of liability. In the US, the safe harbor provides important clarity, but even without the safe harbor, a platform is only liable if they have actually committed secondary copyright infringement. Under this provision, even a spurious takedown must be complied with to avoid a fine. This will create even worse chilling effects than what we've seen in the US.

> III. To the Internet Service Provider that does not provide expeditiously to the judicial or administrative authority, upon request, the information that is in their possession and that identifies the alleged infringer, in the cases in which said information is required in order to protect or enforce copyright or related rights within a judicial or administrative proceeding.

We have repeatedly seen these kinds of information requests used alongside a pointless copyright claim in order to unmask critics or target people for harassment. Handing out personal information should not be automatic simply because of an allegation of

copyright infringement. In the US, we have fought for and won protections for anonymous speakers when copyright owners seek to unmask them because of their expression of their views. For instance, we recently defended the anonymity of a member of a religious community who questioned a religious organization, when the organization sought to abuse copyright law to learn their identity.