Policy Analysis

CATO INSTITUTE

January 25, 2017 | Number 809

Stingray

A New Frontier in Police Surveillance

By Adam Bates

EXECUTIVE SUMMARY

Police agencies around the United States are using a powerful surveillance tool to mimic cell phone signals to tap into the cellular phones of unsuspecting citizens, track the physical locations of those phones, and perhaps even intercept the content of their communications.

The device is known as a stingray, and it is being used in at least 23 states and the District of Columbia. Originally designed for use on the foreign battlefields of the War on Terror, "cell-site simulator" devices have found a home in the arsenals of dozens of federal, state, and local law enforcement agencies.

In addition, police agencies have gone to incredible lengths to keep information about stingray use from defense attorneys, judges, and the public. Through the use of extensive nondisclosure agreements, the federal government prevents state and local law enforcement from disclosing even the most elementary details of stingray capability and use. That information embargo even applies to criminal trials, and allows the federal government to order evidence withheld or entire cases dropped to protect the secrecy of the surveillance device.

The controversy around police stingray surveillance challenges our antiquated Fourth Amendment jurisprudence, undermines our cherished principles of federalism and separation of powers, exposes a lack of accountability and transparency among our law enforcement agencies, and raises serious questions about the security of our individual rights as the government's technological capability rapidly advances.

Adam Bates is a policy analyst with the Cato Institute's Project on Criminal Justice.

> "What the War on Drugs has done for police militarization, the War on Terror is now doing for police intelligence gathering, and the privacy of millions of Americans is at risk."

BACKGROUND

In 2013, three men set up a drug deal in a Tallahassee parking lot. When the drug dealer arrived, the men pulled out a weapon and robbed the dealer of the drugs and his cell phone.[1] Police arrested the robbers a few days later, in possession of the drugs and the phone, and charged them with armed robbery with a deadly weapon, which carries a mandatory minimum sentence of nearly three years in prison under Florida law and allows sentences of up to 30 years. Prosecutors had the men dead to rights.

But the case took a bizarre turn when defense attorneys began wondering how the police managed to find their clients so quickly. The police and prosecution refused to say. Finally, the judge demanded answers. Rather than reveal the method by which police were able to find the suspects, the prosecution offered the men a plea deal: probation with no jail time.[2] Why would prosecutors drop such a "slam dunk" case?

The case came apart due to the government's use of a surveillance device it refused to disclose to the court. Across the United States, federal and state law enforcement agencies are sweeping up cell phone and location data from American citizens using a device colloquially referred to as a "stingray."[3] Stingray surveillance devices are cellular site simulators—they mimic the signal of a cell phone tower in order to force cell phones in the area to connect. Once a phone connects, the officer can download information from the phone or track its location.

Originally designed for military and national security use, the surveillance devices made their way into local law enforcement officers' hands, in coordination with the federal government, through a variety of transfer and grant programs—such as the Urban Areas Security Initiative—as well as through local funding sources—such as civil asset forfeiture funds. Police agencies in 23 states and the District of Columbia, as well as federal agencies including the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the National Security Administration (NSA), and the Department of Homeland Security, are known to be using the devices.[4] Because of the difficulties of discovering law enforcement use of the technology, it is reasonable to assume that police agencies in many more states are also using the devices in secret.

While events like the 2014 unrest in Ferguson, Missouri, and repeated stories of botched Special Weapons and Tactics (SWAT) raids have laid bare many of the problems involved in an increasingly militarized domestic police force, mission creep has not been limited to weapons and tactics.[5] What the War on Drugs has done for police militarization, the War on Terror is now doing for police intelligence gathering, and the privacy of millions of Americans is at risk.

Much remains unknown about these devices. More troubling still is that the lack of public knowledge is by design. Through the use of nondisclosure agreements, a refusal to honor freedom of information requests, and deceit toward courts and the public, the full capabilities of these devices, the extent of their use by law enforcement, and the existence of policies to govern their use remain secret. But interested defense lawyers and civil liberties advocates have uncovered evidence that the use of stingray devices by domestic law enforcement agencies poses a litany of legal and ethical questions. The purpose of this paper is to illuminate those issues and to suggest some possible legislative and judicial remedies.

The paper will detail the history of the devices and their use by local law enforcement, the known and alleged extent of their capabilities, and why this technology renders millions of innocent Americans at risk of having their personal data and communications information swept up in law enforcement fishing expeditions.

In recent years, stingrays have moved from military and national security uses to routine police use. Surveillance technology, designed for use on battlefields or in antagonistic states where constitutional concerns are minimal, has increasingly found its way into the hands of local law enforcement, often without any discernible effort to adapt the equipment or the policies governing its tactical use to the home front, where targets are citizens with constitutional rights rather than battlefield combatants.

Further exacerbating the problems with stingray transfers are the efforts of the Harris Corporation (the Florida-based manufacturer of the devices) and the federal agencies responsible for licensing and coordinating the transfers of these devices to state and local law enforcement agencies to hide the technology. The administrative regime that the federal government and the Harris Corporation have built requires law enforcement agencies to keep the capabilities, uses, and often, the very existence of stingrays secret from citizens, legislators, and courts.

In defense of this veil of secrecy, government agencies have offered several justifications. Advocates of domestic stingray use insist that the devices are essential tools for law enforcement and that public revelation of their technological capabilities will compromise the efficacy of surveillance. They point to instances where stingray surveillance facilitated a positive outcome, and they highlight the need for law enforcement technology to keep up with advances in the technology of the criminal world.

While stingray technology indeed gives law enforcement officers an added advantage over their surveillance targets, the advantage does not justify secrecy or answer constitutional concerns. The claims that these devices are essential for preventing terrorist attacks and bringing down drug kingpins do not, as this paper will show, fit with the data thus far uncovered, which details stingray use by local law enforcement. Terrorists and drug kingpins long ago concluded that their cell phones were liabilities, and the reports detailing local stingray use support that conclusion. Several data releases compelled by state freedom of information litigation have uncovered little evidence that stingrays are being used to foil terrorists. The releases have, however, revealed thousands of warrantless stingray uses across the country for entirely routine law enforcement actions. Rather than bringing down terrorists and cartels, the government is using stingray surveillance to sidestep the Fourth Amendment's warrant requirement.

Meanwhile, the overly restrictive terms of the nondisclosure agreement, upon which both the Harris Corporation and the FBI condition the local use of stingrays, have compromised prosecutions of people suspected of serious violent crimes. In other words, the ostensibly hypothetical prosecutions of terrorists and drug kingpins are crowding out actual prosecutions of criminals when police and prosecutors are forbidden from disclosing stingray use to the courts.

This phenomenon is not an accident; the terms of the agreement make such crowding out inevitable. The government plainly views sacrificing individual prosecutions, even for serious crimes, as an acceptable price for concealing the nature of stingray surveillance. The FBI's nondisclosure agreement is clear: in exchange for permission to use stingray devices, state and local officials must surrender prosecutorial discretion to the federal government.

Few jurisdictions have willingly admitted to deploying stingray devices. Even fewer have offered any semblance of a publicly available policy on their use. The Department of Justice, which has deployed stingrays for years, only recently announced an initial stingray policy for Justice Department agencies, and it leaves much to be desired. The use of stingray surveillance devices in the absence of a warrant from a fully informed judge and without any legislative or public oversight undermines the separation of powers necessary to hold the government accountable.

The relationship between the federal government, Harris, and state and local law enforcement agencies also represents a threat to American federalist principles. The federal government's terms of use amount to a demand that state and local officials abrogate their authority to prosecute cases when the federal government would rather maintain secrecy. These conditions undermine the police powers of the states, as does the mandate that agencies conceal their surveillance tactics from judges in cases before them.

This threat to federalism was apparent when, in 2014, U.S. Marshals literally raided the Sarasota Police Department and seized stingray documentation in order to prevent the department from complying with a state-level freedom of information request.[6] The Florida chapter of the American Civil Liberties Union (ACLU)

"The government plainly views sacrificing individual prosecutions, even for serious crimes, as an acceptable price for concealing the nature of stingray surveillance."

"When state and local law enforcement are beholden to the federal government for funding, equipment, and tactics, state law enforcement priorities are inevitably altered."

had recently secured an order requiring the Sarasota police to turn over documents pertaining to stingray use. To prevent that information from being turned over to the ACLU and the public, the U.S. Marshals Service launched a pre-dawn raid on the police department to take possession of the information. The federal government has also urged local law enforcement agencies to deceive state judges, and continues to exert pressure in favor of secrecy rather than public disclosure and oversight.[7]

Ultimately, the increasing militarization of police through federal equipment transfers and grant programs unavoidably risks the subversion of local law enforcement priorities in favor of federal ones. When state and local law enforcement are beholden to the federal government for funding, equipment, and tactics, state law enforcement priorities are inevitably altered.

Stingray use presents several novel legal issues as well. The Fourth Amendment provides that people have a right to "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[8] Over the years, the Supreme Court has adopted methods of analyzing Fourth Amendment claims, such as the reasonable expectation of privacy[9] test and third-party doctrine.[10]

In the absence of guidance from the courts, many law enforcement agencies settle for the use of what are known as "pen register" or "trap and trace" orders, which generally require less evidence of wrongdoing than a proper warrant would.[11] As the names suggest—both were originally methods of obtaining information from telegraph machines—these legal standards were created at a time when today's technological infrastructure could scarcely be imagined.

What it means to "be secure" from unreasonable searches is also the source of renewed interest among Fourth Amendment scholars, who argue that the phrase's meaning has been historically misconstrued. This paper will explore that argument and whether it contains the answer to the problem of mass surveillance under our constitutional framework.

As the private details of our lives are increasingly susceptible to digital hacking and surveillance, the government's technological capabilities have far outpaced legal standards created to regulate much older and less invasive technology. It is incumbent upon legislatures and courts to close the growing gap.

Finally, this paper will explore possible reforms, including efforts at both the state and federal level that are already underway. Several state legislatures have already undertaken efforts to oversee the use of these devices, several courts have now revised their rules for dealing with stingray evidence, and there is a realistic potential for public policy to vastly improve the protection of our constitutional rights in the face of warrantless surveillance by law enforcement. While law enforcement's crime-fighting capabilities must keep pace with advances in technology, stingray supporters' argument that complete secrecy is the only means of effecting such advances requires scrutiny.

HOW DO STINGRAYS WORK?

Although the precise extent of stingray use remains shrouded in secrecy, defense lawyers and civil liberties advocates, working through trial discovery efforts and freedom of information litigation, have uncovered a great deal about the capabilities of the devices.

Historically, police have tracked cellular phones through the use of cell tower data collected from, and in coordination with, third-party cell signal carriers. Through the use of pen register or trap and trace orders, police compel carriers to disclose phone records that allow law enforcement agents to locate particular cellular phones. The records allow police to use the carrier's cell towers to triangulate the position of the suspect's phone at any given time.[12]

Stingrays, on the other hand, give government agents the capability to circumvent that process by locating cell phones without the assistance of cell carriers, potentially enabling law enforcement to avoid seeking any judicial authorization first.

Stingrays are cellular-site simulators. They operate by mimicking the signal of a cell phone

tower in order to force all cell phones within a given area to connect to the stingray device.

Cell phones are designed to automatically connect to the cell tower that is broadcasting the strongest signal. A typical cell phone could connect and reconnect dozens of times in a given day in order to achieve the strongest signal as the user travels. Stingray devices produce a boosted signal that muscles out the signals from legitimate cell towers and becomes the preferred signal source for the cell phone. All of this can transpire without the knowledge of, or any input from, the cell phone user or the network carrier. Once the phones are connected to the device, the stingray operator can locate the phone, interfere with its signal, and even retrieve personal data from the device.

A phone's location can be triangulated using its international mobile subscriber identity (IMSI), which is a unique number that phones use to communicate with the cellular network. There are two methods of using the IMSI to locate a phone: the government can either ask the third-party carrier to voluntarily reveal the IMSI of a particular phone or compel the carrier under a court order. As the stingray forces cell phones in a target area to connect to it, the operator can screen the incoming "ripped" IMSI numbers against the known IMSI number he or she is trying to track. Once the suspect IMSI pings the stingray, the precise location of the phone can be triangulated.

Alternatively, if the IMSI number of the target is unknown, the stingray can collect the IMSI numbers of every phone in the target location.[13] Law enforcement can then visually survey the scene while collecting cell data in order to isolate the IMSI number of an individual suspect's phone. As police follow the suspect out of range of the other phones, his unique IMSI will eventually become apparent to the stingray operator. This tactic can be combined with the previously discussed pinging tactic in a way that cuts the network carrier entirely out of the process and allows police to both derive and surveil a given IMSI number on their own.

The location data produced by the stingray and its accompanying software is remarkably precise. Law enforcement officials have testified that stingray devices have allowed them to locate cell phones to within six feet and to identify a phone in a particular section of an apartment in a large apartment complex.[14] The precision of this data raises constitutional questions regarding warrantless searches of private domiciles, a practice the Supreme Court has historically viewed with immense skepticism.

The full extent of the stingray data-ripping capability is unknown, but there is substantial reason to believe that even user content, such as browser activity, SMS text messages, and the content of phone calls can be intercepted. The Department of Justice's own Electronic Surveillance Manual is vague but certainly leaves the door open to widespread personal data collection:

> If the cellular telephone is used to make or receive a call, the screen of the [cell-site simulator] would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected)... [Cell site simulators] and similar devices *may be capable of intercepting the contents of communications* [emphasis added].[15]

The Department of Justice recently articulated publicly, for the first time, a written policy for Department of Justice stingray use, but that policy does little to allay concerns about the possibility of excessive data collection. Rather than claim that current stingray devices lack the ability to take content, the policy states that devices are not "configured" to do so and that to take content in that manner would violate federal law:

> Cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. 3127(3).[16]

"The full extent of the stingray data-ripping capability is unknown, but there is substantial reason to believe that even user content, such as browser activity, SMS text messages, and the content of phone calls can be intercepted."

“Stingray devices are capable of collecting a tremendous amount of personal data, and not just from suspected criminals.”

The implication is clear: the federal government denies using stingray devices to take user content in the domestic law enforcement context, but nothing in the Department of Justice policy refutes that the devices indeed possess such a capability.

Even insofar as the policy requires the use of warrants and forbids the collection and retention of private data, it is only administrative guidance rather than statutory law. Further, as the Department of Justice policy applies only to the federal agencies under the jurisdiction of the Department of Justice, there remains a substantial danger that other federal, state, and local law enforcement agencies do not impose similar restraints.[17]

Stingray devices are capable of collecting a tremendous amount of personal data, and not just from suspected criminals. The stingray device doesn't discriminate between target cell phones and other phones in the area. It can interfere with signals, record telephony metadata, pinpoint locations, and potentially intercept the content of calls and text messages. Despite this intrusive capability, many jurisdictions have no publicly available policy guidelines at all, due in large part to the way stingrays came into the possession of domestic law enforcement agencies in the first place.

DOMESTICATION OF STINGRAY SURVEILLANCE

The cell-site simulators used by law enforcement are primarily manufactured by the Florida-based Harris Corporation. Originally used exclusively by the federal government, the proliferation of cell-simulator software for purely state and local law enforcement use has rapidly accelerated.[18]

The technology is currently in use by the Federal Bureau of Investigation; the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the Department of Homeland Security (DHS); Immigrations and Customs Enforcement (ICE); the U.S. Marshals Service; and the Drug Enforcement Administration; as well as the Army, Navy, Marine Corps, National Guard, and the National Security Agency. Even the Internal Revenue Service possesses stingray devices.[19] Freedom of Information Act (FOIA) requests, along with litigation and media investigation, have revealed state or local law enforcement use of the technology in 23 states and the District of Columbia as of October 2016.[20]

By 2010 the Harris Corporation had entered into negotiations with the Federal Communications Commission (FCC), which regulates the sale and use of all radio-emitting devices, to begin licensing stingray equipment to state and local law enforcement.[21] Harris requested, and the FCC assented to, a provision of the licensing agreement that would require law enforcement agencies that wish to employ stingray devices to coordinate their acquisition and use with the FBI.[22]

In exercising its coordination authority, the FBI requires state and local law enforcement agencies to accept a comprehensive nondisclosure agreement before being allowed to acquire stingray devices. Law enforcement officials have interpreted the nondisclosure agreement as preventing even the disclosure of the agreement itself, and until recently, lawyers and civil libertarians could only speculate about its terms.

However, in March 2015, a Supreme Court of New York[23] ruling in favor of the New York Civil Liberties Union against the Erie County Sheriff's Office finally led to the disclosure of an unredacted copy of the FBI's coordination agreement.[24] The Erie County agreement imposes 11 conditions on the agency's use of stingray devices, on issues ranging from training requirements to a mandate that agencies keep the devices secret from public information requests.

The most remarkable of these provisions grants the FBI plenary power to compel state and local authorities to drop criminal cases, regardless of the severity of the offense, if the secrecy of the stingray device would be compromised by moving forward with the prosecution. The provision also bars law enforcement agencies and prosecutors from disclosing any revealing information about the devices at any stage of criminal or civil proceedings.

The "drop prosecution" condition of the FBI nondisclosure agreement with Erie County reads in full:

> In addition, the Erie County Sheriff's Office will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (beyond the evidentiary results obtained through the use of the equipment/technology), if using or providing such information would potentially or actually compromise the equipment/technology. This point supposes that the agency has some control or influence over the prosecutorial process. Where such is not the case, or is limited so as to be inconsequential, it is the FBI's expectation that the law enforcement agency identify the applicable prosecuting agency, or agencies, for inclusion in this agreement.[25]

The "no information" provision states:

> The Erie County Sheriff's Office shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology [. . .] including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in the testimony in any phase of civil of criminal trial, without the prior written approval of the FBI.[26]

In other words, if defense attorneys ask the right questions, they can force the prosecution to choose between dropping the case (or at least the evidence gleaned from the use of a stingray) and violating the terms of the nondisclosure agreement and risking the ire of the federal government.

This situation is not hypothetical. Evidence from numerous jurisdictions shows state and local prosecutors doing precisely what the nondisclosure agreement ostensibly demands: dropping evidence or even entire prosecutions against criminal suspects when their defense attorneys suspect that stingrays were used in the investigations of their clients and demand to see the devices in court.

Shortly after the unredacted nondisclosure terms were revealed, the FBI issued a statement denying that it had ever invoked the authority to compel prosecutors or police to refuse to participate in prosecutions built upon stingray evidence.[27] The statement did not, however, disclose whether or how often the FBI has authorized disclosure of stingray data to courts or defendants pursuant to the "no information" clause of the agreement. The FCC, for its part, has denied any responsibility for both the terms of the FBI's nondisclosure agreement and the requirement that state and local law enforcement agencies agree to it in the first place.[28] Notwithstanding these statements, state and local law enforcement agencies around the country have, rightly or wrongly, interpreted the agreement to mean that they are not allowed to disclose the nature of stingray surveillance devices to courts or defense attorneys.

Over time, stingrays have moved from military and national security tools to routine law enforcement devices. National security and military agencies may occasionally have a need for such extensive secrecy mandates, but what justifications can state and local police agencies offer to defend material omissions to judges, attorneys, criminal defendants, and the public at large?

JUSTIFICATIONS FOR STINGRAY USE

Law enforcement agencies have offered a variety of justifications for stingray use and for the lack of transparency accompanying it. The primary justification for stingray use is that cell-site simulator surveillance is a powerful tool

"National security and military agencies may occasionally have a need for such extensive secrecy mandates, but what justifications can state and local police agencies offer to defend material omissions to judges, attorneys, criminal defendants, and the public at large?"

"In Baltimore, stingray devices have been used, by one detective's estimate, more than 4,300 times in routine law enforcement activities in the city."

for law enforcement, and of this, there is little doubt. Stingrays have been deployed in thousands of investigations around the country and have helped to locate violent suspects accused of heinous crimes.

The ability to surreptitiously track a suspect's movements in real time, to locate a suspect within a specific room of a larger building, or to identify a suspect in a large crowd is of obvious value to law enforcement.[29] Insofar as government officials have disclosed information—often at the order of a court—regarding stingray use, it's clear that many criminal investigations have been in some way assisted by the use of cell-simulator technology.

But whether stingray technology is a valuable asset for law enforcement isn't the end of the inquiry. Investigative ease is not the sole element to consider. The U.S. Constitution restricts the ability of the government to perform unreasonable searches and seizures. The Fourth Amendment's warrant requirement makes it clear that investigative power must be balanced against an individual's right to be secure in his person and property. Separation of powers and checks and balances frustrate government efficiency in order to prevent abuse.

In order to assess the stated justifications for stingray use and secrecy, the utility to law enforcement must be weighed against established legal principles, such as privacy rights, the separation of powers, and due process. The efficiency of law enforcement is only a legitimate interest insofar as law enforcement stays within the bounds of the Constitution.

The two most commonly asserted justifications for stingray use and secrecy relate to the War on Terror and the War on Drugs. Law enforcement advocates of stingray devices consider the ability to surreptitiously track the cell phones of drug traffickers and would-be terrorists an essential tool for maintaining drug prohibition and combating terrorism.

The argument in support of the secrecy surrounding stingrays builds upon the same foundation. If terrorists and drug runners get wind of what stingrays are and how they operate, as the argument goes, then suspects will be able to neutralize the surveillance by changing their behavior.[30]

Law enforcement officials often refer to the War on Terror in their efforts to procure stingray devices. Indeed, much of the funding for these devices comes to state and local law enforcement through federal homeland security and defense grants, such as the Urban Areas Security Initiative (UASI).[31] Competition for this grant money invariably skews law enforcement priorities away from investigating and preventing typical crimes and toward national security functions. By signing onto these federal initiatives, state and local police are essentially pledging to take on federal law enforcement responsibilities in exchange for being allowed to acquire federal resources.

For instance, in their application for stingray equipment in 2006, officials from the Michigan State Police stated that the technology would be vital in allowing "the State to track the physical location of a suspected terrorist who is using wireless communications as part of their communication."[32] In Tacoma, Washington, the police cited the threat of improvised explosive devices (IEDs) in their application for the technology.[33] Perhaps needless to say, in the time since the grant was approved, there is no evidence that stingray surveillance has been used to avert improvised explosive device attacks in Tacoma.

While police departments have been reluctant to reveal details about their use of stingray devices unless forced to by court orders, the data thus far suggests that cases–such as the ones in Michigan and Tacoma, Washington–represent a trend. Departments around the country cite terrorism to justify the grant money and the licensing of the equipment but ultimately use the devices for nonterrorism purposes. In Baltimore, stingray devices have been used, by one detective's estimate, more than 4,300 times in routine law enforcement activities in the city.[34] A Freedom of Information Act release from the Tallahassee Police Department shows hundreds of routine uses, without a single terrorism investigation.[35]

When government officials attempt to jus-

tify the acquisition of military-grade equipment, appeals to bizarre and outlandish threats are common, but occasionally officials are candid about their motivations. When Keene, New Hampshire, applied to the federal government for funding for a BearCat tactical vehicle by citing a terrorist threat to the annual town pumpkin festival, one city council member allowed:

> Our application talked about the danger of domestic terrorism, but that's just something you put in the grant application to get the money. What red-blooded American cop isn't going to be excited about getting a toy like this? That's what it comes down to.[36]

Terrorist attacks are simply not that common, generating few opportunities for police to deploy stingrays in terrorism investigations.[37] Or perhaps terrorists, like drug traffickers before them, long ago concluded that cell phones were a potential surveillance liability and altered their communications. Regardless, the fact is that there is little evidence at the state or local level that stingray surveillance is being used to further the government's interest in combating terrorism.

But even if it could be shown that stingray devices were being used by state and local law enforcement to combat terrorism, the secrecy regime could not be justified.

Whatever tactical advantage the government gained by hiding the use and capabilities of cell-site simulators in years past has been eroded by years of compelled revelations as a result of FOIA requests and court proceedings. Even if we assume that keeping these capabilities secret at one time justified a regime of immense secrecy, the secret is out now.[38] While it is conceivable that less sophisticated would-be terrorists are not keeping tabs on law enforcement's technological capabilities, the types of highly sophisticated terror and drug organizations about whom the FBI's nondisclosure agreement worries will have learned what they need to by now.

FEDERALISM AND SEPARATION OF POWERS

When federal–state partnerships preclude executive officers of state and local agencies from informing judges, legislators, or the general public about their capabilities (or even the fact that they've partnered with the federal government in the first place), separation of powers questions arise. These questions are especially acute in jurisdictions where the stingray equipment was purchased through federal security grant programs or using funds taken from private individuals through civil asset forfeiture.[39] In such cases, it's entirely possible that the legislature is never consulted at all, as no local appropriation is necessary. When state and local law enforcement agencies depend on federal funding for their equipment and cut their local legislatures and courts out of the process, state and local control of law enforcement is threatened.[40]

Similarly, insofar as the FBI's nondisclosure agreement prohibits law enforcement agents and prosecutors from disclosing stingray uses or evidence to judges, or from accurately describing the devices in applications for warrants or pen/trap orders, the role of the judiciary in overseeing and ensuring constitutional compliance by law enforcement has been seriously compromised.

Perhaps most importantly, the secrecy around these devices and the surreptitious means utilized by law enforcement to deploy them are having a deleterious effect on the criminal justice system. When judges find out that they've been misled into authorizing cell-site simulators, or when prosecutors are pressured to drop charges or dismiss evidence rather than reveal stingray use, entire criminal cases fall apart.[41] Dangerous criminals are put back on the street or given overly favorable plea bargains by prosecutors merely to protect an increasingly ill-kept secret, and to defend a law enforcement tactic that serves as an end-around traditional due process and separation of powers barriers. The traditional institutions keeping the abuse of such tools in check have been sidelined, and actual prosecutions of

"'Our application talked about the danger of domestic terrorism, but that's just something you put in the grant application to get the money.' — Keene, New Hampshire, city councilor"

> "The complete lack of transparency regarding government use of stingray technology guarantees that bad actors are not being held accountable and that guidelines, where they exist at all, are not always being followed."

criminals have been abandoned in the name of pursuing a hypothetical enemy.

The FBI has also encouraged constitutionally dubious practices at the state and local level. In April 2016, a government watchdog organization in Oklahoma revealed an agreement between the FBI and the Oklahoma City Police Department for the acquisition of a stingray device.[42] The FBI memo explains that, due to exigent circumstances, the use of a full nondisclosure agreement would be inappropriate and that the memo would serve in that capacity instead.

One provision of the memo states:

> Information obtained through use of the equipment is FOR LEAD PURPOSES ONLY, and may not be used as primary evidence in any affidavits, hearings or trials. This equipment provides general location information about a cellular device, and your agency understands it is required to use additional and independent investigative means and methods, such as historical cellular analysis, that would be admissible at trial to corroborate information concerning the location of the target obtained through use of this equipment.[43]

This technique, known as parallel construction, allows law enforcement to obscure evidence sources to prevent their disclosure in court.[44] The tactic is used to protect the identities of confidential informants, but it can also be used to hide evidence from judges or defendants.

When utilizing parallel construction, law enforcement uses some surreptitious and, perhaps, constitutionally dubious tactics to generate a piece of evidence. In order to obscure the source of that evidence, police will use the new information as a lead to gather information from which they construct a case that appears to have been cracked using routine police work. The police then represent to the court and to the defendant that the routine tactics led to the break in the case. The secret evidence or technique is not revealed.

While legislatures and courts have been unable to provide oversight or accountability due to the secrecy of law enforcement and the federal government, the stingray-utilizing agencies themselves have in many cases done next to nothing to ensure the appropriate and constitutional use of these devices.

A LACK OF ACCOUNTABILITY

The complete lack of transparency regarding government use of stingray technology guarantees that bad actors are not being held accountable and that guidelines, where they exist at all, are not always being followed.

The federal government does not reveal which departments own or lease the devices; which departments are actively deploying them and how often; what, if any, guidelines govern them; or what mechanisms, if any, are in place to ensure the devices are used properly. Even if guidelines were to be put in place, the lack of transparency with which these devices have been used suggests a dire need for strict and independently enforced accountability mechanisms.

In October 2015, following several remarkable revelations regarding stingray surveillance, both the Department of Homeland Security and the Department of Justice publicly outlined their stingray policies for the first time.

The policies include a requirement that federal law enforcement officials seek warrants for stingray use except under certain exigent circumstances, a requirement that data be disposed of routinely and when it is no longer needed for a specific investigation, and a requirement that government agencies be open with courts about the use of the technology in criminal investigations.[45]

It is important to note, however, that while these policies represent a step toward transparency on the part of the federal government, they are merely internal administrative policies. They do not carry the force of law, and enforcement of these guidelines is left entirely up to the executive agencies deploying the devices.

These guidelines also appear to apply only to devices being used by the federal government and have no bearing on the use of stingray devices that are in the hands of state and local

police, who remain free to set up their own guidelines and accountability policies.

Without a full accounting of the capabilities of stingray devices and public acknowledgment of their use by each law enforcement agency, any hope of imbuing the process with accountability for misuse is fleeting. A reliance on executive agency self-policing and the assurances of police agencies that they are not abusing their technology is inadequate protection in lieu of constitutional safeguards. The judicial and legislative branches, tasked by our system with checking the power of the executive branch, have important roles to play in limiting the abuses of stingray surveillance and thus far have failed to do so.

LEGAL STATUS OF WARRANTLESS STINGRAY SURVEILLANCE

Understanding the issues raised by warrantless stingray surveillance requires some background on the Supreme Court precedents that inform our current Fourth Amendment jurisprudence.

In the 1967 case *Katz v. United States*, the Supreme Court ruled that a police wiretap of a phone booth was a search within the meaning of the Fourth Amendment and required a warrant because of the attempt of the defendant to keep the conversation private.[46] Justice Harlan, in a concurring opinion, laid out his understanding of the court's ruling and included a reasonable expectation of privacy test, which has since become the standard test in Fourth Amendment privacy jurisprudence.

Roughly a decade later, in *United States v. Miller*[47] and *Smith v. Maryland*,[48] the Court articulated what has come to be known as the third-party doctrine. Under third-party doctrine analysis, the expectation of privacy disappears where the individual voluntarily conveys information to third parties. But *Miller* and *Smith* involved microfilms of bank deposits and a list of dialed phone numbers, respectively. In the modern context, the third-party doctrine can, as the government argues, be applied much more broadly, as almost all of the data emanating from cell-phones and other Web-connected mobile devices is constantly being sent to third-party service providers. With so much of our daily activity being sent to third-party Internet and telephone service providers, the level of constitutional protection afforded to such data becomes a much more significant question than it was decades ago.

By the early 2000s, the Supreme Court was wrestling with advances in police technology that allowed officers to peer through walls and into the privacy of the home. In 2001, the Court decided *Kyllo v. United States*, in which agents from the Department of the Interior utilized infrared heat imagers to look inside a private home in search of the hallmark heat signatures of a marijuana-growing operation.[49] The Court ruled that using "sense-enhancing technology" to peer into private homes was a search within the meaning of the Fourth Amendment and therefore required a warrant based upon probable cause.

A decade later, some members of the Court had begun to question the applicability of the expectation of privacy test in light of modern technology. In 2012 the Supreme Court decided *U.S. v. Jones*.[50] Police and FBI agents, without a warrant, snuck onto Jones's property and placed a global positioning system (GPS) tracker on his car. The Court ruled that the physical trespass onto Jones's property represented a search. Perhaps the most notable aspect of the *Jones* case was the concurring opinion by Justice Sonia Sotomayor, who finally raised the specter of rethinking the expectation of privacy test and doing away with the third-party doctrine:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail

"The judicial and legislative branches, tasked by our system with checking the power of the executive branch, have important roles to play in limiting the abuses of stingray surveillance and thus far have failed to do so."

"How many criminal suspects are going to turn down a favorable plea deal just to have their Fourth Amendment rights analyzed by a judge who could send them to prison?"

> addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as JUSTICE ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not.
>
> I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[51]

While Sotomayor's analysis did not receive the support of a Court majority, it at least stands as a signal that some on the Court are ready to revisit an outdated privacy test in light of the centrality of third-party data sharing to virtually every aspect of our private lives in the 21st century.

Chief Justice Roberts, writing for a unanimous court, made a similar observation about the centrality of cell phones to our private lives just two years later in a case called *Riley v. California*:

> These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy. A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones.[52]

Federal and state courts have not yet had much opportunity to apply these principles. That's in large part because the courts have often been competing against a stacked deck when it comes to policing cell-site simulators. Between the explicit provisions of the FBI nondisclosure agreement and federal encouragement to keep relevant information from courts, most judges have not had occasion to analyze the legal issues raised by stingray use.

The FBI wields considerable control over whether a particular case reaches a verdict, and therefore whether it is likely to result in a clear ruling from a judge on the constitutionality of stingray use. Judges have a difficult time assessing the legality of police practices when the cases are routinely removed from court through plea bargains or dropped charges. How many criminal suspects are going to turn down a favorable plea deal just to have their Fourth Amendment rights analyzed by a judge who could send them to prison?

Despite this pervasive secrecy regime, in several criminal cases vigilant defense attorneys who questioned how the police found their clients stumbled onto stingray investigations. What they managed to find suggests a widespread pattern of obfuscation and occasional deceit by the FBI and local law enforcement agencies to obscure their behavior from the courts and from criminal defendants.

In one 2014 Arizona case, the City of Tucson cited both "Harris corporation's legal obligations under federal law and its contractual obligations to the Federal Bureau of Investigation regarding this technology" to attempt to avoid responding to a state freedom of information request.[53] The city further asserted that the redactions from the freedom of information response were made at the behest of both Harris Corporation and the FBI, contradicting the FBI's statements that its nondisclosure agreement does not require such secrecy.[54] The city did, however, acknowledge that when using its stingray devices, the Tucson police sought neither warrants nor pen register orders, meaning that the Tucson Police Department was using the technology without judicial authorization or oversight.[55]

In a 2015 Baltimore case, a criminal defendant received a favorable plea deal after the city re-

fused to disclose stingray material "because the Department of Justice prohibits the access and disclosure of these items." The judge threatened a detective with contempt proceedings after citing the nondisclosure agreement from the stand. "You don't have a non-disclosure agreement with the court," Judge Barry Williams told him.[56]

The cross-examination of a police officer from another Maryland case transcript reveals the position in which judges find themselves in court.

> **Judge:** It's a simple question. Why was he stopped? What was the, it was a warrantless arrest. Why was he stopped? That's the question she's asked. He can answer the question. Why did you stop him?
>
> **Police Officer:** This kind of goes into Homeland Security issues, Your Honor.
>
> **Judge:** Okay, if it goes into Homeland Security issues, then the phone doesn't come in. Okay. Step down, thank you. I mean this is simple. *You can't just stop someone and not give me a reason, State, and you know that.* (emphasis added).[57]

But these revelations only arose in situations where defendants and their lawyers chose to go to trial in the first place and in trials where the defense attorney's suspicions about surreptitious police surveillance paid off. It stands to reason, then, that the vast majority of criminal cases in which stingray evidence is used, like the vast majority of criminal cases generally, are pled out before going to trial and often before defense counsel has an opportunity to raise such questions. In a country where more than 9 out of every 10 criminal defendants waive their right to trial, potentially inadmissible stingray evidence can be used to put pressure on defendants without any risk of being revealed to the court.

In addition to stingray abuses that never make it in front of a judge, police have, sometimes under express federal guidance, willfully misled courts regarding the nature of cell-site simulator technology and the capabilities of stingray devices.[58] Utilizing common terms of art for court orders, police will, for instance, refer to "confidential informants," or "data from telephone service providers" to justify applications for pen registers or warrants. These terms have traditional meanings in the legal system that convey none of the novelty or magnitude of stingray surveillance. Judges, in other words, are sometimes authorizing stingray devices without knowing it.[59] This deception makes it extremely difficult for judges to function in an oversight role when it comes to stingray use.

The problem has become so pervasive that defense attorney organizations are now offering explicit guidance to defense lawyers in order to ferret out stingray uses by police in criminal proceedings.[60]

The consequence of the secrecy, especially the dropping of evidence or entire cases when called out on questionable stingray use, is a general dearth of case law on the constitutional issues that stingrays present. As more has been revealed and the breadth of stingray use has become more widely known, it is fair to anticipate that the amount of judicial analysis will increase.

A few courts have been able to weigh in on the constitutional implications of warrantless stingray use already. In 2013 a federal district court in Arizona upheld the use of a stingray device in a tax fraud prosecution against a defendant on the grounds that the police were sufficiently descriptive in their warrant application to satisfy Fourth Amendment requirements.[61] Another federal district court, this time in Maryland, found that stingrays relied only on information that had been voluntarily conveyed to third parties and thus did not constitute a search within the meaning of the Fourth Amendment.[62]

At least one state-level appellate court has disagreed with those federal rulings. In an opinion released in March 2016, the Court of Special Appeals of Maryland held that using a stingray to locate a phone inside a home constitutes a search within the meaning of the Fourth Amendment and requires a warrant.[63]

In that case, defendant Kerron Andrews was suspected of shooting three people. Police

"In a country where more than 9 out of every 10 criminal defendants waive their right to trial, potentially inadmissible stingray evidence can be used to put pressure on defendants without any risk of being revealed to the court."

> "Legislators have an obligation to protect their citizens' privacy, and they don't need to wait for the courts to do that job for them."

sought and received a court order to use a pen/trap device to surveil Andrews' phone. The police, however, actually deployed a cell-site simulator—in this case a newer-generation device with the trade name HailStorm—in order to track the physical location of Andrews' phone in real time. The police were able to track Andrews to a specific home in Baltimore.

Citing *Kyllo*, the court held that the use of a cell-site simulator to track a person's location inside a home violates a person's reasonable expectation of privacy. The court also held that the data being beamed from a person's phone to a cell tower is not being "voluntarily conveyed," thus the third-party doctrine is inapplicable and the data retains its constitutional protection.

The court also found that police had misled the judge by requesting a pen/trap order without explaining the full capabilities of the device. Insofar as the FBI's nondisclosure agreement contributed to that decision by law enforcement, the court questioned the constitutionality of the agreement itself.

> We perceive the State's actions in this case to protect the Hailstorm technology, driven by a nondisclosure agreement to which it bound itself, as detrimental to its position and inimical to the constitutional principles we revere.[64]

The few instances of courts assessing the legality of stingray use have come to different conclusions, citing different precedents, and it could be years before these splits in Fourth Amendment interpretations are resolved.

Even if courts are not ready to do away with the third-party doctrine entirely, the *Kyllo* precedent represents an interesting potential conflict with the third-party line of reasoning in cell phone tracking cases. Indeed, stingrays do collect data from cell phone users, but ostensibly the primary use of that data is to triangulate the precise location of the phone rather than to analyze the content of the data itself. This tracking capability inevitably includes the inside of homes and other areas traditionally considered beyond the reach of warrantless searches. Any location capable of receiving a cell tower signal is fair game to the stingray and indistinguishable from public areas with little to no expectation of privacy.

Stingray surveillance, then, represents a potential flashpoint between two previously disparate Fourth Amendment doctrines. As the primary purpose of the devices is to track locations through a technique that is obviously not within the traditional sensory suite of a human police officer, it is possible that the Supreme Court would find that the "sense-enhancing technology" precedent of *Kyllo* is the more appropriate analytical framework than the third-party doctrine, even if Justice Sotomayor stands alone in her desire to revisit the third-party doctrine itself.

REMEDIES FOR WARRANTLESS STINGRAY SURVEILLANCE

If judges do take on a more active role in stingray oversight, that by itself may still be insufficient to protect the rights of individuals. Suppression of evidence gained in violation of a person's Fourth Amendment rights is not guaranteed to deter police misconduct, and courts have been hesitant to take more punitive measures against the state or its agents when they fail the existing Fourth Amendment tests.

Legislators have an obligation to protect their citizens' privacy, and, as Justice Alito pointed out in his concurrence in *Riley*, they don't need to wait for the courts to do that job for them:

> Many forms of modern technology are making it easier and easier for both government and private entities to amass a wealth of information about the lives of ordinary Americans, and at the same time, many ordinary Americans are choosing to make public much information that was seldom revealed to outsiders just a few decades ago.
>
> In light of these developments, it would be very unfortunate if privacy protection in the 21st century were left pri-

> marily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.[65]

The courts establish a floor that privacy protections cannot fall below, but legislators are free to raise that floor on their own initiative, and there has been some progress on that front.

At the federal level, Rep. Jason Chaffetz (R-UT) has introduced a bill that would make the use of a stingray without a warrant a criminal offence, except in some limited exigent circumstances. The Stingray Protection Act goes well beyond merely suppressing tainted evidence. It would impose criminal liability, up to 10 years' imprisonment, for anyone who improperly deploys a stingray device.[66] The bill has an arduous path to becoming law but clearly demonstrates that years of press and court revelations have put stingray abuse squarely on the agenda of some legislators.

Additionally, several states have taken steps to curb warrantless stingray use. The California state legislature recently passed a bill imposing a warrant requirement on state and local stingray use in California,[67] while states such as New York and Missouri are considering similar legislation.[68]

These efforts affirm the traditional constitutional responsibility of state governments for law enforcement. State legislatures have the power to correct many of the problems raised by secretive stingray use, whether through forbidding state and local law enforcement to participate in federal militarization or transfer programs or imposing strict requirements on the use of surveillance devices.

CONCLUSION

Technological advancements in law enforcement are inevitable. The government's ability to surreptitiously monitor the private communications of Americans will develop as quickly as the means of communication themselves. In that sense, it is likely a fool's errand to argue for an outright ban on police use of cell-simulator technology. It's possible to imagine a legitimate role for this technology in law enforcement's arsenal. But the efforts at secrecy, the lack of accountability, and the twisted incentives created by federal meddling in state and local law enforcement beg for reform.

At the executive level, federal and state agencies should be forthright and transparent in their possession and use of stingray surveillance devices, both with the relevant courts and the general public. Even if one accepts the argument that extreme secrecy produced an advantage for law enforcement over terrorists and drug cartels, that advantage has long since evaporated as criminal syndicates have altered their methods and the veil of secrecy has been stripped from the technology.

The FBI should disavow any suggestion that hiding evidence from judges or defendants is a condition of stingray acquisition. It should also cease pressuring prosecutors to drop cases in order to protect the existence and capabilities of cell-site simulators.

At the judicial level, Fourth Amendment jurisprudence governing the privacy protections of cell phone data is in desperate need of Supreme Court analysis. Lower courts seem confused about which analytical framework to apply to stingray cases and how the technology should be assessed within those frameworks. Courts at all levels should reject state secrecy arguments that deny judges and defense teams access to information about stingray capabilities and usage.

State legislative bodies should be wary of federal encroachment into a role traditionally occupied by state and local governments. The use of federal security grants to equip state and local law enforcement, the use of federal nondisclosure agreements to hide the behavior of state and local agents from judicial and legislative oversight, and the inevitable twisting of law enforcement priorities that accompanies such incentive programs are all reasons for caution in allowing agencies to participate in these federal programs. Legislatures should

"The efforts at secrecy, the lack of accountability, and the twisted incentives created by federal meddling in state and local law enforcement beg for reform."

require law enforcement agencies to publish stingray policies that detail the circumstances under which stingray use is authorized, to publish data retention guidelines, and to resolve to seek a warrant or a probable cause analogue before deploying stingrays.

Stingray surveillance raises many novel political and legal issues, yet cell phone trackers are only the vanguard. Police technology will continue to become more expansive and powerful, and the longer it takes legislatures and courts to produce a legal framework capable of keeping up with technology and ensuring that constitutional rights are protected, the more threatening the surveillance state will become.

NOTES

1. The gun turned out to be a BB gun, but for purposes of armed robbery statutes it is treated as a firearm.

2. Ellen Nakashima, "Secrecy around Police Surveillance Equipment Proves a Case's Undoing," *Washington Post*, February 22, 2015, https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html.

3. The term "stingray" is often used as an umbrella term to refer to an entire family of cell phone surveillance devices that may go by other trade names, such as "KingFish," "HailStorm," or "Loggerhead."

4. American Civil Liberties Union, "Stingray Tracking Devices: Who's Got Them?" ACLU.org., https://www.aclu.org/map/stingray-tracking-devices-whos-got-them.

5. American Civil Liberties Union, "War Comes Home: The Excessive Militarization of American Policing," ACLU.org, June 2014, https://www.aclu.org/sites/default/files/assets/jus14-warcomeshome-report-web-rel1.pdf, p. 26.

6. Kim Zetter, "U.S. Marshals Seize Cops' Spying Records to Keep Them from the ACLU," *Wired*, June 3, 2014, https://www.wired.com/2014/06/feds-seize-stingray-documents/.

7. Kim Zetter, "Emails Show Feds Asking Florida Cops to Deceive Judges," *Wired*, June 19, 2014, https://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray/.

8. U.S. Const. amend. IV.

9. See *Katz v. United States*, 389 U.S. 347 (1967).

10. See *Smith v. Maryland*, 442 U.S. 735 (1979).

11. 18 U.S.C. 3123 describes the relevant legal standards for use of pen registers or trap and trace devices.

12. For more detail on the technical capabilities of Stingray devices, see Stephanie K. Pell and Christopher Soghoian, "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy," *Harvard Journal of Law & Technology* 28, no. 1 (Fall 2014): 8–19; see also, Sam Biddle, "Long-Secret Stingray Manuals Detail How Police Can Spy on Phones," *The Intercept*, September 12, 2016, https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/.

13. For instance, if law enforcement is using the stingray to monitor a demonstration in which no individual is suspected of any wrongdoing sufficient to justify a pen register, a stingray would allow law enforcement to learn the identity and phone information of the attendees, which could be used to facilitate further surveillance.

14. *United States v. Rigmaiden*, 844 F. Supp.2d 982, 996 (D. Ariz. 2012).

15. Department of Justice Electronic Surveillance Manual (Jan. 2, 2008), p. 17.

16. "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology," United States Department of Justice, Office of Public Affairs, http://www.justice.gov/opa/file/767321/download.

17. Including the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Department of Homeland Security (DHS); the Federal Bureau of Investigation (FBI); and the U.S. Marshals Service, but excluding agencies under the Department of Homeland Security, such as the U.S. Immigration and Customs Enforcement (ICE), the U.S. Secret Service, and the Transportation Security Administration (TSA).

18. FBI response to Freedom of Information request by Electronic Privacy Information Center, February 2013, https://epic.org/foia/fbi/stingray/FBI-FOIA-Release-02072013-OCR.pdf.

19. Nicky Woolf and William Green, "IRS Possessed Stingray Cellphone Surveillance Gear, Documents Reveal," *Guardian* (London), October 26, 2015, http://www.theguardian.com/world/2015/oct/26/stingray-surveillance-technology-irs-cell phone-tower.

20. American Civil Liberties Union, "Stingray Tracking Devices: Who's Got Them?"

21. Nathan Freed Wessler, "Documents Suggest Maker of Controversial Surveillance Tool Misled the FCC," American Civil Liberties Union, September 17, 2014, https://www.aclu.org/blog/documents-suggest-maker-controversial-surveillance-tool-misled-fcc?redirect=blog/national-security/documents-suggest-maker-controversial-surveil lance-tool-misled-fcc.

22. Federal Communications Commission, "Grant of Equipment Authorization to Harris Corporation," March 2, 2012. "(1) The marketing and sale of these devices shall be limited to federal, state, local public safety and law enforcement officials only; and (2) State and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization."

23. A point of clarity: in the New York court system, a supreme court is not the highest court. That distinction belongs to the New York State Court of Appeals.

24. *New York Civil Liberties Union v. Erie County Sheriff's Office*, State of New York Supreme Court, Index No. 2014/000206, March 17, 2015, http://www.nyclu.org/files/releases/ErieCoStingray Win_3.17.15.pdf.

25. Agreement between FBI and Scott R. Patronik, Chief of Erie County Sheriff's Office, June 29, 2012, http://nyclu.org/files/20120629-renondisclsure-obligations(Harris-ECSO).pdf.

26. Ibid.

27. Ellen Nakashima, "FBI Clarifies Rules on Secretive Cellphone-Tracking Devices," *Washington Post*, May 14, 2015, https://www.washingtonpost.com/world/national-security/fbi-clarifies-rules-on-secretive-cellphone-tracking-devices/2015/05/14/655b4696-f914-11e4-a13c-193b1241d51a_story.html.

28. FCC letter to Phil Mocek of MuckRock News, October 2, 2014, https://www.muckrock.com/news/archives/2014/oct/08/fcc-fbi-cant-agree-stingray-nda/. "We do not require that state and local law enforcement agencies have to complete one or more non-disclosure agreements with the Federal Bureau of Investigation prior to acquisition and/or use of the authorized equipment."

29. See Testimony of Elana Tyrangiel, Principal Deputy Assistant Attorney General at the Department of Justice and Seth M. Stodder of the Department of Homeland Security before House Subcommittee on Interior, October 21, 2015.

30. The concern is explicitly mentioned in the nondisclosure agreement itself, which states that disclosure would empower surveillance targets to "employ countermeasures to avoid detection." Supra, note 24.

31. The efficacy of programs such as the Urban

Areas Security Initiative (UASI) has been called into question by efficiency hawks such as former Senator Tom Coburn (R-OK), who paints a damning portrait of the program's waste. See Tom Coburn, "Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities," December 2012, https://info.publicintelligence.net/SenatorCoburn-UASI.pdf.

32. Nathan Freed Wessler, "Police Citing 'Terrorism' to Buy Stingrays Used Only for Ordinary Crimes," American Civil Liberties Union, October 23, 2015, https://www.aclu.org/blog/free-future/police-citing-terrorism-buy-stingrays-used-only-ordinary-crimes.

33. Privacy SOS, "Police Are Using a Powerful Surveillance Tool to Fight the War on Drugs, Not Terrorism," October 15, 2014, https://privacysos.org/node/1554.

34. Justin Fenton, "Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases," *Baltimore Sun*, April 9, 2015, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

35. See the master list of stingray deployments by the Tallahassee Police Department, March 27, 2014, *Fusion*, https://fusiondotnet.files.wordpress.com/2015/02/03.27.2014_-_master_ce_log.pdf.

36. American Civil Liberties Union, "War Comes Home: The Excessive Militarization of American Policing," ACLU, June 2014, https://www.aclu.org/report/war-comes-home-excessive-militarization-american-police, p. 26.

37. See John Mueller, "Is There Still a Terrorist Threat? The Myth of the Omnipresent Enemy," *Foreign Affairs*, September/October 2006, https://www.foreignaffairs.com/articles/2006-09-01/there-still-terrorist-threat-myth-omnipresent-enemy.

38. See Pell and Soghoian, "Your Secret Stingray's No Secret Anymore."

39. Joel Handley et al., "Inside the Chicago Police Department's Secret Budget," *Chicago Reader*, September 29, 2016, http://www.chicagoreader.com/chicago/police-department-civil-forfeiture-investigation/Content?oid=23728922.

40. Even when the funding sources are local, as in the case of civil forfeiture funds, the agencies still must coordinate their acquisition and use of stingray equipment with the federal government.

41. Robert Patrick, "Controversial Secret Phone Tracker Figured in Dropped St. Louis Case," *St. Louis Post-Dispatch*, April 19, 2015, http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html; Ellen Nakashima, "Secrecy around Police Surveillance Equipment Proves a Case's Undoing," *Washington Post*, February 22, 2015, https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html; and Justin Fenton, "Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases," *Baltimore Sun*, April 9, 2015, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.

42. Clifton Adcock, "Okla. Authorities Have or Use Controversial Cellphone Tracker," Oklahoma Watch, April 10, 2016, http://oklahomawatch.org/2016/04/10/okla-authorities-have-or-use-controversial-cell-phone-tracker/.

43. "Approved Non-Disclosure Notice," from the FBI to the Oklahoma City Police Department, August 7, 2014, https://assets.documentcloud.org/documents/2825761/OKCPDFBI-MOU.pdf.

44. Or, less charitably, "evidence laundering." In an email response to the revelations, ACLU Staff Attorney Nathan Wessler stated: "This is the first time I have seen language this explicit in an FBI non-disclosure agreement. The typical non-disclosure agreements order local police to hide information from courts and defense attorneys,

which is bad enough, but this goes the outrageous extra step of ordering police to actually engage in evidence laundering. Instead of just hiding the surveillance, the FBI is mandating manufacture of a whole new chain of evidence to throw defense attorneys and judges off the scent. As a result, defendants are denied their right to challenge potentially unconstitutional surveillance and courts are deprived of an opportunity to curb law enforcement abuses." See Jenna McLaughlin, "FBI Told Cops to Recreate Evidence from Secret Cell-Phone Trackers," *The Intercept*, May 5, 2016, https://theintercept.com/2016/05/05/fbi-told-cops-to-recreate-evidence-from-secret-cell-phone-trackers/.

45. See Testimony of Seth M. Stodder, Assistant Secretary, Threat Prevention and Security Policy, Office of Policy, U.S. Department of Homeland Security, testifying before the Committee on Oversight and Government Reform, Subcommittee on Information Technology, October 21, 2015. See also Testimony of Elana Tyrangiel, Principal Deputy Assistant Attorney General Before the Subcommittee on Information Technology, Committee on Oversight and Government Reform, U. S. House of Representatives, October 21, 2015.

46. *Katz v. United States*, 389 U.S. 347 (1967).

47. *United States v. Miller,* 425 U.S. 435 (1976).

48. *Smith v. Maryland*, 442 U.S. 735 (1979).

49. *Kyllo v. United States,* 533 U.S. 27 (2001).

50. *United States v. Jones*, 132 S. Ct. 945 (2012).

51. *United States v. Jones*, 132 S. Ct. 945 (2012).

52. *Riley v. California,* 573 U.S. ___ (2014) at 8.

53. *Hodai v. The City of Tucson*, Superior Court of the State of Arizona, No. C20141225, City's verified answer, p. 2, par. 10.

54. Ibid., p. 4.

55. Ibid., p. 5.

56. Justin Fenton, "Legal Challenge Alleges Authorities Withheld Police Use of Stingray Surveillance," *Baltimore Sun*, September 4, 2015, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-challenge-20150904-story.html/.

57. C. Justin Brown and Kasha M. Lee, "StingRay Devices Usher in a New Fourth Amendment Battleground," *The Champion*, National Association of Criminal Defense Lawyers, June 2015, p. 13.

58. Kim Zetter, "Emails Show Feds Asking Florida Cops to Deceive Judges."

59. As former U.S. Magistrate Judge Brian Owsley explains, pen/trap applications using such vague terminology can deceive judges into believing they are authorizing traditional pen registers or trap and trace devices, when in fact law enforcement plans to use the authorization to deploy much more invasive cell-site simulators. See Larry Greenemeier, "What Is the Big Secret Surrounding Stingray Surveillance?" *Scientific American*, June 25, 2015, http://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/.

60. Brown and Lee, "StingRay Devices Usher in a New Fourth Amendment Battleground," pp. 12–20.

61. United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Arizona 2012).

62. United States v. Graham, 846 F. Supp. 4d 284 (D. Md. 2012).

63. State of Maryland v. Andrews (2015). Court of Special Appeals of Maryland, No. 1496, Sept. Term 2015. Filed March 30, 2016.

64. Ibid., at p. 25.

65. Riley v. California, 573 U.S. ___ (2014) at concurrence p. 6.

66. Nicky Woolf, "Congressman Introduces Bill to

End Warrantless Stingray Surveillance," Guardian (London), Nov. 4, 2015, http://www.theguardian.com/world/2015/nov/04/house-bill-end-warrantless-stingray-surveillance-jason-chaffetz.

67. Cyrus Farivar, "California Cops, Want to Use a Stingray? Get a Warrant, Governor Says," Ars Technica, Oct. 8, 2015, http://arstechnica.com/tech-policy/2015/10/california-governor-signs-new-law-mandating-warrant-for-stingray-use/.

68. Mike Maharrey, "Missouri Bill Would Ban Warrantless Use of Stingray Devices, Hinder Federal Surveillance Program," Tenth Amendment Center, December 18, 2015, http://blog.tenthamendmentcenter.com/2015/12/missouri-bill-would-ban-warrantless-use-of-stingray-devices-hinder-federal-surveillance-program/.