BRENNAN CENTER FOR JUSTICE

at New York University School of Law

Cellphones, Law Enforcement, and the Right to Privacy

HOW THE GOVERNMENT IS COLLECTING AND USING YOUR LOCATION DATA

by Rachel Levinson-Waldman

Cell phones are ubiquitous. As of 2017, there were more cell phones than people in the United States. Nearly 70 percent of those were smartphones, with 94 percent of millennials carrying a smart device.[1] Cell phones go nearly everywhere, and users are increasingly dependent on smartphone applications for daily activities, such as texting, email, and location-assisted direction services.[2]

Cellular technology also allows service providers to collect a wealth of information about a user's whereabouts.[3] Cellular service providers automatically record the location of cell phones at regular intervals, transforming them into personal tracking devices.[4] One court described them as the "easiest means to gather the most comprehensive data about a person's public — and *private* — movements."[5] Cell phone location data is collected in such high volume that it offers a nearly inexhaustible source of granular information, including when and where someone goes, with whom, and even for what purpose.[6]

This white paper surveys the landscape of government acquisition of location data about cell phone users — from cellular providers' collection of location information to the use of technologies that pinpoint where individuals and cell phones are located. It describes how cell phones operate, how that location information is accrued and disseminated, and the technologies that can be used to establish where a phone is, where it has been, and what other users have been in proximity.

The paper then analyzes both the legal and policy landscape: how courts have ruled on these issues, how they can be expected to rule in the future, and how agencies have addressed these issues internally, if at all. It adds to concerns that cell phone-based monitoring could violate the constitutional privacy rights of millions of ordinary Americans — and that people of color are disproportionally affected. Finally, it concludes with a set of recommendations to enhance transparency and accountability around the use of cell phone location data and to ensure constitutional protections for users who are affected.

How is cell phone location data collected?

A cell phone's location information can be collected in several ways. First, a cell phone accesses its network through signals transmitted by cell towers.[7] The cell phone searches for the strongest signal and continually connects to a cell tower as the user moves within the network, whether or not a call is underway.[8] When it connects to a cell tower, the phone transmits identifying information to the service provider.[9] This enables the provider to "track the phone, discontinue service, or blacklist it from a network."[10] The density and proliferation of cell towers make it increasingly possible to locate an individual phone to within a few feet of its position.[11]

Service providers collect and store this location data, called cell site location information (CSLI), at least temporarily; some providers keep the data for up to seven years.[12] Police officers can obtain stored CSLI if they satisfy certain legal requirements. Prior to 2018, law enforcement agents generally obtained CSLI with a court order under the Stored Communications Act, which has a lower standard than a warrant.[13] However, the Supreme Court recently held in *U.S. v. Carpenter* (2018) that the police must get a warrant to obtain seven days or more of CSLI.[14] Police may also request information about *every* device connected to a single tower during a particular interval, potentially netting historical location information from thousands of phones; this technique is colloquially known as a "cell tower dump."[15] For instance, in 2010, the FBI received over 150,000 numbers in a single dump in an effort to determine if a suspect had been near several banks that had been robbed.[16] Verizon had more than 14,000 cell tower dump requests in both 2016 and 2017 and is on track for even more in 2018.[17]

In addition, service providers can use the data transmitted by cell phones to monitor a phone's location in real time and provide that information to the police, allowing law enforcement to track someone's movements as they happen.[18] In addition to requesting prospective — that is, real-time — CSLI from providers, police can also request that providers "ping" phones to force them into revealing their location. This technique relies on Enhanced 911 (E911) data, which allows law enforcement to pinpoint the location of cell phones that have placed 911 calls; a provider can also make a reverse 911 call, allowing the police to invisibly track a target's cell phone in real time.[19] Courts are split on whether a probable cause warrant is required to obtain real-time cell phone location information or if a lower standard is required, though a consensus appears to be emerging in favor of a warrant requirement.[20]

A number of law enforcement agencies also have technology that enables them to circumvent the service provider and gain direct access to real-time cell phone location data.[21] These devices, called cell site simulators, are known colloquially as "Stingrays" after a popular model manufactured by the Harris Corporation.[22] A cell site simulator "masquerades as a cell tower, tricking all nearby cell phones to connect to itself" rather than to a legitimate tower.[23] When deployed — whether by hand, from within a patrol car, or attached to a plane[24] — these simulators gather the real-time geolocation of all phones within range.[25]

Cell site simulators can be used in two ways. First, if an officer already knows the location of a phone down to the radius of several blocks or a neighborhood, he or she can drive around the area with the simulator to pinpoint the precise location.[26] As part of this process, the cell site simulator will "also intercept[] the data of other cell phones in the area, including the phones of people not being investigated."[27] Second, the device can be used to identify all the cell phones (and, by extension, their subscriber information) at a given location, such as a protest.[28] Cell site simulators are generally used in such a way that "[t]he phone's user will not know" they are being tracked, so law enforcement can use the tool for location surveillance without the public's knowledge.[29] As of November 2018, the U.S. Departments of Justice, Homeland Security, and Treasury owned numerous cell site simulators, as did 75 law enforcement agencies in 27 states and the District of Columbia.[30]

Smartphone location data can also be obtained through the phone's use of Wi-Fi, Bluetooth, and GPS. Smartphones continuously send out signals containing identifying information to establish connections with these technologies; in the case of GPS, smartphones receive signals from GPS satellites and perform calculations based on the timing and other features of the signals to determine their location — indeed, a phone can calculate its GPS location, even with no WiFi or cellular connection, because it does not need to broadcast anything to receive the GPS signals.[31] Smartphones store their location history until the user takes affirmative steps to clear the data.[32] Third-party applications running on smartphones can also request and receive geolocation data without any direct action on the part of the user.[33] Law enforcement can request this data directly from these third-party providers like Google and Facebook,[34] often with delayed notice to users.[35]

While users can enable privacy settings that are meant to limit disclosure of much of their location data, phones can bypass these privacy restrictions in various circumstances.[36] A sufficiently determined individual could even ascertain a phone's location through data produced by built-in features that measure the phone's altitude and speed.[37] In other words, short of turning off one's phone, it is nearly impossible to prevent the transmission of location data.

Why does this matter?

First, cell phone location information reveals a user's movements with ever-increasing precision, potentially exposing intimate details of someone's life.[38] As the federal appeals court for the District of Columbia explained, "[a] person who knows all of another's travels can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts."[39] This information could be used to target a political opponent — for instance, an undocumented activist — and could chill the exercise of First Amendment-protected activities like protests and other gatherings. Even limited location data, whether from CSLI or a cell site simulator, may

reveal whether a person is inside a home or another private space protected by the Fourth Amendment, information that has traditionally required a warrant to obtain.[40]

Second, there is significant distrust around law enforcement's use of cell site simulators. There is now some public knowledge about the use and capabilities of these tools. However, states and local agencies buying the devices were long required to sign restrictive nondisclosure agreements with the FBI before purchase, often preventing the disclosure of critical information to the courts and defense counsel.[41] Even now, there are concerns that cell site simulators could at some point begin intercepting "user content such as browser activity, SMS text messages, and the content of phone calls."[42] This technological capability does not yet appear to have been deployed by local or state law enforcement. But the government's tendency to obscure the capabilities and use of surveillance technologies hinders oversight, trust, and public debate.

Location surveillance also has a disproportionate impact on communities of color. Law enforcement agencies have historically focused their power and resources on communities of color, and this disparity persists today.[43] New technologies that extend the power and reach of law enforcement are likely to exacerbate existing biases in policing and add more surveillance to communities that are already extensively policed.[44] In 2016, following on a formal complaint from civil rights groups to the Federal Communications Commission, a coalition of senators sent a letter to the FCC raising concerns that cell site simulators were more frequently used in minority neighborhoods and asking the agency to provide additional information.[45]

What does the law say?

HISTORICAL CELL SITE INFORMATION

The Fourth Amendment to the U.S. Constitution guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[46] Until the middle of the last century, that language was understood to mean that only a physical search violated the Constitution and therefore required a warrant. Thus, the Supreme Court held in 1928 that the police could use any manner of surveillance device as long as they did not breach physical barriers — for instance, by literally inserting a microphone into the walls of a home.[47]

In 1967, however, the Supreme Court reversed course, holding in *Katz v. United States* that "the Fourth Amendment protects people, not places."[48] The Court ruled in that case that even when a person uses a public phone booth to make a call, the act of closing the door to the phone booth indicates that the caller meant to keep it private and that the police must get a warrant to listen in.[49] Since *Katz*, when a defendant asserts that the government has conducted a search under the Fourth Amendment by observing or collecting information about him via some method other than a physical intrusion, the court looks to whether he had a "reasonable expectation of privacy." In other words, the court considers (1) whether the individual had an "actual (subjective) expectation of privacy" in the particular information or activity that produced it and (2) whether society is "prepared to recognize" that expectation as reasonable.[50]

In the decades after *Katz*, the Court ruled that surreptitiously gathering information about activities inside private homes violates Americans' reasonable expectations of privacy, whether by secretly sending in a tracking device like a beeper (as in *U.S. v. Karo*) or by using cutting-edge technological tools like thermal imaging (as in *Kyllo v. U.S.*).[51] On the flip side, the Court held in *U.S. v. Knotts* that a driver on a public road could not reasonably expect his movements to be private from an officer observing where he drove.[52] Even in *Knotts*, however, the justices observed that "dragnet-type law enforcement practices" could change that calculation.[53] And in recent years, the Court has begun to more fully embrace the maxim that an individual "does not leave his privacy behind when he walks out his front door."[54]

Thus, in *United States v. Jones* (2012), a majority of justices opined that using a GPS tracker to monitor a car's location on a nearly minute-by-minute basis for a month, producing over 2,000 pages of data, raised significant privacy concerns in light of the duration of the monitoring, the comparatively low cost, and the secrecy and intrusiveness of the surveillance tool.[55] (The narrowly drawn opinion concluded simply that physically attaching the GPS tracker to the car without a warrant was an unconstitutional trespass, but twin concurrences from Justices Alito and Sotomayor delved into the privacy concerns.[56]) Two years later, the Court ruled in *Riley v. California* that police need a warrant to search the cell phone of an arrestee. The opinion, which emphasized the vast storage capacity of modern-day phones, noted that historical cell phone location information — "a standard feature on many smart phones" — can "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[57]

Taken together, these cases suggest the Court is developing a more expansive vision of the Fourth Amendment in the digital age. If the Court is committed to "assuring preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted,"[58] it must "contend with the seismic shifts in digital technology that [make] possible the tracking of not only" a single individual's location but everyone's location.[59]

It is worth noting that the Supreme Court has not yet addressed cell tower dumps. Some lower courts have tackled this question, with several allowing the government to access cell tower dump data with a court order under 18 U.S.C. § 2703(d) of the Stored Communications Act.[60] Notably, these courts relied in part on the robustness of the third-party doctrine, a legal framework that has shifted substantially in the wake of *Carpenter v. United States*.[61] Other decisions have required a warrant and obligated prosecutors to purge any information not relevant to the investigation.[62] In light of *Carpenter* and the possibility that these collection methods rise to the level of the "dragnet" warned of by *Knotts*, the Supreme Court may rethink in the coming years whether a warrant is required for collection of this data.

REAL-TIME CELL PHONE TRACKING

The Supreme Court has not yet squarely addressed real-time cell phone tracking, and it declined to do so in *Carpenter v. United States*, ruling only that a warrant is required to obtain more than a week's worth of CSLI.[63] Lower courts, however, have already faced the issue, and a number of courts have held that police must get a warrant before requesting or obtaining real-time location data.[64] In 2016, for instance, a Maryland appeals court ruled that police must obtain a warrant to use a cell site simulator, observing that "people have a reasonable expectation that their cell phones will not be used as real-time tracking devices," and most other courts to have considered the issue have followed in its footsteps — though often relying on statutory grounds and avoiding delving into the constitutional question.[65] The Florida Supreme Court reached a similar decision in 2014, recognizing that people have a reasonable expectation of privacy in the location information transmitted by their cell phones.[66] The court held that the police must get a warrant in order to compel a cell phone service provider to provide real-time updates on a user's location.

Unlike with historical data, courts ruling on real-time tracking largely have not distinguished between tracking for a short versus a long period of time — perhaps because tracking someone in real time is invasive regardless of how long it lasts.[67] However, several cases on real-time tracking are pending before state supreme courts,[68] and at least one appeals court has held that real-time tracking for a brief period does not raise constitutional problems.[69] The issue may therefore come before the Supreme Court sooner rather than later. In the meantime, many states are taking matters into their own hands: As of this writing, nine states require a warrant for all location information; four states have legislation prohibiting real-time tracking without a warrant, while another two state supreme courts have held that a warrant is required for real-time tracking; two states require a warrant for a cell site simulator; three states require a court order to use a cell site simulator; and five states require court orders to obtain location information.[70]

In addition, the Departments of Justice and Homeland Security adopted policies in 2015 requiring their components to obtain a warrant in order to use a cell site simulator, with some limited exceptions.[71] But no federal law codifies this requirement, there is no penalty for noncompliance, and the Justice Department policy does not bind state or local law enforcement agencies that acquire their own cell site simulators instead of borrowing them from federal agencies.[72] A handful of individual states have legislatively restricted law enforcement's use of cell site simulators, suggesting a path forward for lawmakers.[73]

THIRD-PARTY DOCTRINE

Until recently, arguments that CSLI should be protected by the Fourth Amendment because the data reveals individuals' private information ran into another roadblock: the third-party doctrine. This rule, which arose out of cases dating back to the late 1970s, decrees that there is no expectation of privacy when information is voluntarily shared with a third party, be it a bank, a bookstore, or an auto shop. In other words, the doctrine frees police to collect the data from a third party without having to serve a warrant or involve the individual with the greatest interest in keeping the information secret.[74]

In *Carpenter*, however, the Supreme Court held that the third-party doctrine is no longer a bright-line rule when it comes to CSLI. The Court reasoned that cell site location information is sensitive enough that people retain a reasonable expectation of privacy in it.[75] The Court also observed that having a cell phone is a near-requirement in the 21st century and that transmission of information from a cell phone to a tower is a necessary function of cellular technology. As a result, sharing this information is not truly "voluntary."[76] Thus, except in cases of emergency, police must now obtain a warrant to acquire seven days' or more worth of CSLI from a cell phone provider.[77]

DATA RETENTION AND DISCLOSURE

Questions persist regarding how long police or prosecutors retain cell phone location data — particularly of individuals who are not the intended targets of the collection — as well as whether defendants in criminal cases are notified of its existence. When it comes to tower dumps, some agencies appear to retain non-germane information for long periods of time.[78] As for cell site simulators, the DOJ policy requiring warrants mandates relatively swift deletion of any irrelevant data. And in California, anyone whose digital information is targeted may petition for the destruction of any data obtained in violation of federal or state law.[79] California state

law also requires law enforcement agencies to have a publicly available privacy and use policy. However, no other state appears to have a similar mandate.[80]

Without proper regulation, these troves of location information could be used to identify and track individuals' past, present, and future activities. This is particularly concerning in the context of protests or other political gatherings, or other expressions of First Amendment-protected activity. The retention of such information could chill individuals' First Amendment rights, especially where it is used by law enforcement to identify, target, and prosecute political dissidents and their allies.[81]

Finally, secrecy around data acquisition and retention deprives defendants of their right to due process. Under *Brady v. Maryland*, prosecutors must disclose evidence that is favorable to the defendant or otherwise material to his or her defense.[82] Failure to disclose all relevant evidence deprives defendants of the opportunity to challenge the quality and veracity of the government's investigation and prevents them from building their strongest case.

Recommendations

1. Surveillance transparency: Jurisdictions considering the procurement and use of cell site simulators and other cell phone monitoring or tracking devices should require law enforcement to disclose the nature, scope, and privacy impact of the surveillance technologies. This should include information about any disparate impact of the technology's use on protected classes of individuals such as communities of color or other marginalized communities prior to disbursing funds for the technology's acquisition. Model legislation can be found in the cities of Oakland and Berkeley, California, where recently approved ordinances have implemented robust disclosure, accountability, and approval mechanisms.[83] Legislation has also been introduced in New York City that would require the New York Police Department to disclose information about its use of surveillance technologies.[84]

2. Require community feedback before, during, and after procurement: When law enforcement seeks to acquire and use surveillance technologies such as cell site simulators, the communities affected should be afforded the opportunity to review and respond to the stated law enforcement objective and to comment on the necessity for the acquisition of such tools. There should be opportunities for such input prior to the technologies' procurement, during the selection process if approved for acquisition, and after implementation to hold law enforcement accountable.

3. Expand warrant requirements: Federal and state legislation should require a probable cause warrant for the use of cell site simulators and for access to real-time cell site information (with appropriate exceptions for emergencies). In 2015, California passed a robust state privacy law, CalECPA, that could be a model for such efforts. CalECPA provides for, among other things, the suppression of any information obtained in violation of the Fourth Amendment.[85] A number of other states have passed legislation requiring a warrant for phone tracking; the included chart provides more details.

4. Disclose all information in criminal cases: Location data collected by cell site simulators should be disclosed to defendants and to the court. The federal government should cease the use of nondisclosure agreements and instead facilitate "clarity and candor to the court."[86]

5. Limit Data Retention: Extraneous cell site location information not pertaining to the particular phone and user targeted should be promptly segregated and destroyed. If an investigation requires retention of additional information for a legitimate law enforcement purpose, the period should be as brief as possible. These limits could be imposed not only by departmental policy but also by state and federal law, with penalties for failure to comply including the exclusion of data that is improperly retained.[87]

6. Content collection: Cell site simulators and similar devices should not be used to intercept content of phone calls without a wiretapping warrant issued under Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[88] This so-called "superwarrant" requires, among other things, that the agent requesting it certify that all other investigative techniques have been exhausted (or that it is overly dangerous to do so). This ensures an added level of protection against government surveillance of the content of private conversations.[89]

HOW CAN THE GOVERNMENT FIND OR TRACK PEOPLE THROUGH THEIR PHONES?

Types of location data	How is it produced and stored?	How can law enforcement access this data?
Cell site location information (CSLI), stored by service providers	A phone accesses its network through signals transmitted by cell towers and continually connects to a cell tower as a user moves through the network. Upon connection to a cell tower, the phone transmits identifying information to the service provider.	Archived CSLI: ▪ **Less than seven days:** Law enforcement agents must obtain a court order under the Stored Communications Act (SCA), which requires the government to provide only "specific and articulable facts showing that there are reasonable grounds to believe … [the records] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). ▪ **Seven days or more:** In 2018, the Supreme Court ruled that police must obtain a search warrant supported by probable cause (*U.S. v. Carpenter*), a higher standard than an SCA court order. ▪ **Tower dumps** (information about all cell phones in the vicinity of an individual tower during a specified time period): Courts are split on whether a warrant is required or if a court order under the SCA is sufficient. While some courts have been satisfied with a court order because they concluded there was no reasonable expectation of privacy in voluntarily shared data, *U.S. v. Carpenter* may alter this analysis going forward. Real-time CSLI: ▪ Most courts have held that police must get a probable cause warrant to demand real-time information from a service provider, though some have permitted the police to use a court order under the SCA. In addition, four states have passed laws requiring police to get a search warrant to track a cell phone in real time, while another nine require police to get a warrant to obtain any location information.
Cell site simulator ("Stingray")	Cell site simulators trick nearby cell phones into connecting to the device rather than to functioning cell towers, gathering real-time geolocation data of all cell phones within range.	A Maryland appeals court has held that police must obtain a warrant to use a cell site simulator. The Supreme Court has not yet addressed the issue. Three states — California, Connecticut, and Washington — have passed laws requiring a court order to use a cell site simulator, and Illinois and Vermont have passed legislation requiring a warrant.

HOW CAN THE GOVERNMENT FIND OR TRACK PEOPLE THROUGH THEIR PHONES? (CONTINUED)

Types of location data	How is it produced and stored?	How can law enforcement access this data?
Smartphone location data stored on the phone itself	Wi-Fi, Bluetooth, and GPS data can establish a phone's location as well, with more precision than CSLI. Smartphones store this data until the user takes affirmative steps to clear the data.	Law enforcement officers can request this information from companies like Google and Apple through subpoenas, court orders, or search warrants.
Geolocation data produced by third-party applications, such as Facebook and Google Maps.	Third-party applications that use location data as part of their services, such as mapping applications or fitness trackers, store users' location data and transmit it back to the application's servers, where it is stored until the user takes steps to clear the data.	Law enforcement officers can request this information via court orders to the third-party application developers, such as Facebook and Google. Facebook, for instance, requires a court order under the Stored Communications Act.

Endnotes

1 CTIA, "The State of Wireless 2018," July 10, 2018, https://api.ctia.org/wp-content/uploads/2018/07/CTIA_State-of-Wireless-2018_0710.pdf.

2 *See* Riley v. California, 134 S.Ct. 2473, 2480 (2014) (defining a smartphone as "a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and internet connectivity"); *id.* at 2490 ("According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."); Chuck Jones, "What do People Use Their Cell Phones for Besides Phone Calls?" *Forbes,* November 29, 2012, https://www.forbes.com/sites/chuckjones/2012/11/29/what-do-people-use-their-cell-phones-for-beside-phone-calls/#4b7fc9b361cd.

3 *Cf. Riley*, 134 S.Ct. at 2490 ("[Cellphones] can reconstruct someone's specific movements down to the minute."); United States v. Powell, 943 F. Supp. 2d 759, 780 (E.D. Mich. 2013).

4 *See* Jemal R. Brinson, "Cell site simulators: How Law Enforcement can Track You," *Chicago Tribune*, February 18, 2016, www.chicagotribune.com/news/plus/ct-cell-phone-tracking-devices-20160129-htmlstory.html.

5 *Powell*, 943 F. Supp. 2d at 780; *see also Riley*, 134 S. Ct. at 2490.

6 *See generally* Lauren E. Babst, "No More Shortcuts: Protect Cell Site Location Data with a Warrant Requirement," *Michigan Telecommunications and Technology Law Review* 21 (Spring 2015): 363-400.

7 In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1024 (N.D. Cal. 2015).

8 *See* House Committee on Oversight and Government Reform, Staff Report, *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations*, 114th Cong., 2d sess., December 19, 2016, 9 [hereinafter Committee Staff Report], https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf; *see also* Justin Hill, "Digital Technology and Analog Law: Cellular Location Data, the Third-Party Doctrine, and the Law's Need to Evolve," *University of Richmond Law Review* 51, no. 3 (March 2017): 786 (clarifying that connectivity is maintained by transferring a phone between towers as required, based on signal strength and capacity of the individual cell site, as well as distance to the nearest tower).

9 Hill, *supra* note 8, at 786; *see also* Brinson, *supra* note 4.

10 Brinson, *supra* note 4. Carriers put stolen phones onto a "blacklist" that prevents them from being used on any network, even internationally, in order to reduce the incentive to traffic in stolen phones. *See* "What is the Cell Phone Blacklist, Anyway?" *Orchard* (blog), April 13, 2015, https://www.getorchard.com/blog/cell-phone-blacklist/.

11 *See e.g.,* Andy Greenburg, "Reminder to Congress: Cops' Cellphone Tracking Can be Even More Precise than GPS," *Forbes*, May 17, 2012, http://www.forbes.com/sites/andygreenberg/2012/05/17/reminder-to-congress-cops-cellphone-tracking-can-be-even-more-precise-than-gps/#578e3957263c.

12 *See* "Cellular Provider Record Retention Periods," *ProDigital*, April 5, 2017, https://prodigital4n6.com/cellular-record-retention-periods (listing data retention times for different service providers).

13 To receive the order, the government must provide "specific and articulable facts showing that there are reasonable grounds to believe … [the records] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

14 Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

15 *See* John Kelly, "Cellphone Data Spying: It's Not Just the NSA," *USA Today*, August 11, 2015, https://www.usatoday.com/story/news/nation/2013/12/08/cell-phone-data-spying-nsa-police/3902809/ ("A typical dump covers multiple towers, and wireless providers, and can net information from thousands of phones.").

16 Katie Haas, "Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions," American Civil Liberties Union, March 27, 2014, https://www.aclu.org/blog/national-security/privacy-and-surveillance/cell-tower-dumps-another-surveillance-technique.

17 "United States report," Verizon, accessed December 6, 2018, https://www.verizon.com/about/portal/transparency-report/us-report/; *see also Transparency Report,* AT&T, July 2016, http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf; Katie Bo Williams, "Verizon

reports spike in government requests for cell 'tower dumps,'" *Hill*, August 24, 2017, https://thehill.com/policy/national-security/347800-government-requests-for-cell-tower-dumps-spikes-verizon.

18 *See* "The Problem with Mobile Phones," Electronic Frontier Foundation, February 10, 2015, https://ssd.eff.org/en/module/problem-mobile-phones; Rachel Levinson-Waldman, "Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public," *Emory Law Journal* 66, no. 3 (2017): 538–39.

19 *See* Enhanced 911 Emergency Calling Systems, 61 Fed. Reg. 40,374 (Aug. 2, 1996) (codified at 47 C.F.R. § 20.18) (requiring wireless service providers to have E911 technology available in order to assist with emergency response). *See also* U.S. v. Wallace, 85 F.3d 806 (5th Cir. 2018) (discussing "Ping Order"); United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012), *cert. denied*, 570 U.S. 919 (2013) (declining to suppress three days' worth of geolocation information obtained by "pinging" phone pursuant to court order, though noting that "[t]here may be situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes"); In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 532–33 (D. Md. 2011) (describing E911 requests and noting that "[t]his process, known as 'pinging,' is undetectable to the cellular telephone user");

20 For cases imposing a warrant requirement, *see, e.g.,* United States v. Espudo, 954 F. Supp. 2d 1029, 1035 (S.D. Cal. 2013); In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 539–42 (D. Md. 2011); *In re U.S. For an Order Authorizing the Disclosure of Prospective Cell Site Info., No. 06-MISC-004, 2006 WL 2871743, at *5 (E.D. Wis. Oct. 6, 2006);* In re U.S. for an Order Authorizing Monitoring of Geolocation & Cell Site Data for a Sprint Spectrum Cell Phone No., Misc. No. 06-0186, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006); In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); Tracey v. State, 152 So. 3d 504 (Fla. 2014); State v. Earls, 214 N.J. 564 (2013). For cases requiring only a court order, see, e.g., In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448 (S.D.N.Y. 2006); In Matter of Application of U.S. For an Order, 411 F. Supp. 2d 678 (W.D. La. 2006); In re Application of U.S. for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005).

21 Adam Bates, "Stingray: A New Frontier in Police Surveillance," Cato Institute, Policy Analysis No. 809 (January 25, 2017): 4.

22 *See* Sam Biddle, "Long-Secret Stingray Manuals Detail How Police can Spy on Phones," *Intercept*, September 12, 2016, https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/.

23 George Joseph, "Cellphone Spy Tools Have Flooded Local Police Departments," *CityLab*, February 8, 2017, http://www.citylab.com/crime/2017/02/cellphone-spy-tools-have-flooded-local-police-departments/512543/; *see also* Kim Zetter, "Hacker Lexicon: Stingrays, the Spy Tool the Government Tried, and Failed, to Hide," *Wired*, May 6, 2016, https://www.wired.com/2016/05/hacker-lexicon-stingrays-spy-tool-government-tried-failed-hide/ ("[Stingrays] intercept encrypted mobile communication by forcing a phone to downgrade from a 3G or 4G network connection to a 2G network—a less secure network that doesn't authenticate cell towers to the phone and contains vulnerabilities that make it easier to decrypt secure communication."); *see also* United States v. Artis, 315 F. Supp. 3d 1142, 1144 (N.D. Cal. 2018); United States v. Lambis, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016).

24 Andrew Crocker, "New FOIA Documents Confirm FBI Used Dirtboxes on Planes Without Any Policies or Legal Guidance," Electronic Frontier Foundation, March 9, 2016, https://www.eff.org/deeplinks/2016/03/new-foia-documents-confirm-fbi-used-dirtboxes-planes-without-any-policies-or-legal.

25 *See* Jeremy Scahill & Margot Williams, "Stingrays: A Secret Catalogue of Government Gear for Spying on your Cellphone," *Intercept*, December 17, 2015, https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone (describing the capabilities of cell phone tracking technologies, noting that "[s]ome are designed to be used at static locations, while others can be discreetly carried by an individual" or attached to "vehicles, drones, and piloted aircraft" to capture information about any phone in range of the device). The range of a cell phone can vary widely, depending on signal strength and general direction, as well as the number and strength of cellular

towers in the area. *See Examining Law Enforcement Use of Cell Phone Tracking Devices: Testimony before the Subcommittee on Information Technology*, 114th Cong. (October 21, 2015) (statement of Elana Tyrangiel, Principal Deputy Assistant Attorney General), https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2016/01/28/10-21-15_pdaag_tyrangiel_testified_re_examining_law_enforcement_use_of_cell_phone_tracking_devices_web_ready.pdf.

26 *See, e.g.*, State v. Sylvestre, 254 So. 3d 986 (Fla. Dist. Ct. App. 2018).

27 Ibid. at *5.

28 *See* Joseph, *supra* note 23 (discussing the use of cell site simulators to target protest groups); Levinson-Waldman, *supra* note 18, at 553; Brad Heath, "Police Secretly Track Cellphones to Solve Routine Crimes," *USA Today*, August 24, 2015, http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

29 Committee Staff Report, *supra* note 8, at 10.

30 *See* "Stingray Tracking Devices: Who's Got Them?," American Civil Liberties Union, March 2018 (updated November 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them?redirect=map/stingray-tracking-devices-whos-got-them; *see also* Kelly, *supra* note 15.

31 *See* "The Problem with Mobile Phones," *supra* note 18; Stephanie Lockwood, Note, "Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phone as Personal Locators," *Harvard Journal of Law & Technology* 18, no. 1 (Fall 2004): 308; Ed Hewitt, "No Signal? 5 Ways to Use Your Phone GPS Without Data," SmarterTravel.com, October 24, 2017, https://www.smartertravel.com/use-phone-gps-without-data/.

32 Emily Dreyfuss, "Google Tracks You Even If Location History's Off. Here's How To Stop It," *Wired*, August 13, 2018, https://www.wired.com/story/google-location-tracking-turn-off/; Jake Peterson, "How to View, Delete & Disable Location History Data That's Been Collected on You," *Gadget Hacks*, May 3, 2018, https://smartphones.gadgethacks.com/how-to/facebook-101-view-delete-disable-location-history-data-thats-been-collected-you-0184527/.

33 *See, e.g.*, Jennifer Valentino DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

34 *See, e.g.,* "Manage or Delete your Location History," *Google*, https://support.google.com/accounts/answer/3118687?hl=en; *cf.* Russell Brandom, "Police are Filing Warrants for Android's Vast Store of Location Data," *Verge*, June 1, 2016, http://www.theverge.com/2016/6/1/11824118/google-android-location-data-police-warrants; *see also In re Application for Tel. Info. Needed for a Criminal Investigation,* 119 F. Supp. 3d at 1014 ("Additionally, most modern smartphones have applications that continually run in the background, sending and receiving data without a user having to interact with the cell phone.").

35 18 U.S.C.A. § 2705.

36 *See, e.g.,* David Yanofsky, "Google Can Still Use Bluetooth To Track Your Android Phone When Bluetooth Is Turned Off," *Quartz*, January 24, 2018, https://qz.com/1169760/phone-data/; Ryan Nakashima, "AP Exclusive: Google Tracks Your Movements, Like It or Not," *AP News*, August 13, 2018, https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not.

37 Dell Cameron, "How to Track a Cellphone Without GPS—or Consent," *Gizmodo*, December 8, 2017, https://gizmodo.com/how-to-track-a-cellphone-without-gps-or-consent-1821125371.

38 *Cf.* Hill, *supra* note 8, at 787 (estimating that CSLI accuracy may be accurate to within a few meters).

39 U.S. v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, 564 U.S. 1036 (2011).

40 *See* Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."); Kyllo v. United States, 533 U.S. 27 (2001).

41 *See* Agreement between FBI and Scott R. Patronik, Chief of Erie County Sheriff's Office, June 29, 2012,

https://www.nyclu.org/sites/default/files/releases/Non-Disclosure-Agreement.pdf ("Disclosing the existence of and the capabilities provided by such equipment/technology to the public would… adversely impact criminal and national security investigations."); Committee Staff Report, *supra* note 8, at 31 (noting that State and local law enforcement agencies obtained cell site simulator technology through federal grants, subject to non-disclosure agreements that prohibit acknowledging how geolocation evidence was obtained); *id.* at 1-2 (noting that the technology was developed for military use, and its acquisition was often justified on the basis of counter-terrorism and the "war on drugs"); Bates, *supra* note 21, at 2 (describing a "slam dunk" narcotics and armed robbery case being pleaded to "probation with no jail time" because non-disclosure prevented the introduction of evidence that would have demonstrated guilt); Robert Abel, "Stingray Use Still Shrouded in Secrecy and Lack Regulation Despite Progress," *SC Magazine*, March 28, 2017, https://www.scmagazine.com/stingray-use-still-shrouded-in-secrecy-and-lack-regulation-despite-progress/article/647001/.

42 Bates, *supra* note 21, at 5.

43 *See, e.g.,* 18MillionRising.org and Center for Community Change Action et al. to Thomas Wheeler (Chairman, Federal Communications Commission) and Erica Brown Lee (Chief Privacy and Civil Liberties Officer, Department of Justice), March 16, 2016, 2, https://ecfsapi.fcc.gov/file/60001535539.pdf (citing Brad Heath, "Racial Gap in U.S. Arrest Rates: 'Staggering Disparity,'" *USA Today*, November 19, 2014, http://usat.ly/1u8ETXA).

44 Ibid.

45 Al Franken et al. to Tom Wheeler, October 6, 2016, 1, https://apps.fcc.gov/edocs_public/attachmatch/DOC-342409A2.pdf (citing Complaint for Relief Against Unauthorized Radio Operation and Willful Interference with Cellular Communications, In re Baltimore City Police Dep't, Baltimore, Md (filed August 16, 2016), https://ecfsapi.fcc.gov/file/10816659216934/CS%20Simulators%20Complaint%20FINAL.pdf); Memorandum in Support of Complaint for Relief Against Unauthorized Radio Operation and Willful Interference with Cellular Communications and Petition for an Enforcement Advisory on Use of Cell site simulators by State and Local Government Agencies, In re Baltimore City Police Dep't, Baltimore, Md (filed September 1, 2016), https://www.aclu.org/sites/default/files/field_document/aclu-eff_fcc_cell_site_simulator_filing.pdf).

46 U.S. Const. amend. IV.

47 Olmstead v. United States, 277 U.S. 438, 465-466 (1928) (concluding that wiretapping does not "amount to a search or seizure within the meaning of the Fourth Amendment" because the wires in question "are not part of [the defendant's] home or office, any more than are the highways along which they are stretched"); *see also* Silverman v. United States, 365 U.S. 505, 509-510 (1961) (holding that electronic eavesdropping is a violation of the Fourth Amendment if "accomplished by means of an unauthorized physical penetration into the premises occupied").

48 Katz v. United States, 389 U.S. 347, 351 (1967).

49 Ibid. at 352.

50 Ibid. at 360-61 (Harlan, J. concurring).

51 United States v. Karo, 468 U.S. 705, 716-17 (1984); *Kyllo*, 533 U.S. at 34-35.

52 United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

53 Ibid. at 284.

54 United States v. Maynard, 615 F.3d 544, 563 (2010).

55 *Jones*, 565 U.S. at 415-16, 430 (Sotomayor, J., and Alito, J., concurring).

56 Ibid. at 404-08, 415-16, 430 (Sotomayor, J. and Alito, J. concurring).

57 *Riley*, 134 S. Ct. at 2490.

58 *Kyllo*, 533 U.S. at 34.

59 *Carpenter*, 138 S.Ct. at 2219.

60 *See* In re Cell Tower Records Under 18 U.S.C. 2703(D), 90 F. Supp. 3d 673, 675 (S.D. Tex. 2015) (holding that a court order sufficed, and stating that "cell tower logs requested here [are] categorized as ordinary business records entitled to no constitutional protection"); In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014) (finding a court order sufficient because § 2703(d) of the Stored Communications Act applied to cell tower dumps and the third

party doctrine eroded Fourth Amendment protections, but requiring "an amended application that (1) provides more specific justification for the time period for which the records will be gathered and (2) outlines a protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved"). *See also* Hewitt v. United States, 3:08-CR-167-B (2), 2018 WL 3853708, at *5 (N.D. Tex. July 25, 2018), report and recommendation adopted, 3:08-CR-167-B (2), 2018 WL 3845232 (N.D. Tex. Aug. 13, 2018) ("The Fourth Amendment does not prohibit the government from obtaining historical cell tower data for all cell phones used at the time of a crime."); United States v. Pembrook, 119 F. Supp. 3d 577, 585 (E.D. Mich. 2015) (suppression of cell tower dump data not required because the Government's lack of a warrant was not a deliberate, reckless, or grossly negligent disregard for defendant's Fourth Amendment rights); U.S. v. Scott, 2015 WL 4644963, *7 (E.D. Mich. 2015) (holding that subscriber had no reasonable expectation of privacy in records of cell phones that came within tower's range).

61 138 S. Ct. 2206 (2018).

62 *See* In re Application of U.S. for an Order Pursuant to 18 USC 2703(d), 964 F. Supp. 2d 674, 678 (S.D. Tex. 2013) (adding that the government should "have a protocol" addressing how to handle the "sensitive private information" of "innocent people who are not the target of the criminal investigation"); In re Search of Cellular Tel. Towers, 945 F. Supp. 2d 769, 770 (S.D. Tex. 2013); In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d), 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012). It is worth noting that all three cases were authored by the same magistrate judge, Magistrate Judge Brian L. Owsley. *See also* In re United States for an Order Pursuant To 18 U.S.C. §2703(d), 2:17-MC-51662, 2017 WL 6368665, at *2 (E.D. Mich. Dec. 12, 2017) ("any order for mass production of cell site data requires protections for third parties who are not subjects of the investigation").

63 Ibid. at 2206.

64 *See, e.g.,* Levinson-Waldman, *supra* note 18, at 538 n.69 (listing numerous federal district court and state court decisions ruling that real-time acquisition of geolocation data implicates the Fourth Amendment and requires a warrant).

65 State v. Andrews, 134 A.3d 324, 327 (Md. Ct. Spec. App. 2016); *see also* United States v. Lambis, 197 F. Supp. 3d 606 (S.D.N.Y. 2016), *appeal withdrawn*, 16-3149, 2017 WL 4127919 (2d Cir. Mar. 13, 2017) (holding that warrantless use of cell site simulator to locate suspect's apartment in real time was unreasonable search, and noting that "unlike pen register information or CSLI, a cell site simulator does not involve a third party"); United States v. Ellis, 270 F. Supp. 3d 1134, 1141–42 (N.D. Cal. 2017) ("Under the *Katz* test, [Defendant] has demonstrated that the use of the Stingray devices amounted to a search in violation of a reasonable expectation of privacy in the real-time location of his cell phone."); People v. Gordon, 58 Misc. 3d 544, 550, 68 N.Y.S.3d 306, 311 (N.Y. Sup. Ct. 2017) (requiring probable cause warrant for cell site simulator because "[b]y its very nature" its use "intrudes upon an individual's reasonable expectation of privacy"); State v. Sylvestre, 250 So.3d 986, 992 (Fla. Dist. Ct. App. 2018) ("If a warrant is required for the government to obtain historical cell-site information voluntarily maintained and in the possession of a third party, we can discern no reason why a warrant would not be required for the more invasive use of a cell site simulator."); *but see* United States v. Patrick, 842 F.3d 540 (7th Cir. 2016), cert. denied, 138 S. Ct. 2706 (2018) (holding that use of cell site simulator to determine defendant's location in order to arrest him did not warrant application of exclusionary rule)..

66 Tracey v. Florida, 152 So. 3d 504 (Fla. 2014).

67 *See, e.g.*, State v. Andrews, 134 A.3d 324, 348 (Md. Ct. Spec. App. 2016) (reasoning that "[t]e mere fact that police *could* have located [the defendant] within the residence by [using routine surveillance techniques] does not change the fact that the police did not know where he was, so they could not follow him" without use of real-time cell phone tracking) (emphasis original).

68 "EFF to Maine, Massachusetts, Courts: Rule Requiring Warrants to Access Cell Phone Location Data Applies to Real-Time Searches," press release, Electronic Frontier Foundation, August 30, 2018, https://www.eff.org/press/releases/eff-maine-massachusetts-courts-rule-requiring-warrants-access-cell-phone-location.

69 United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012), *cert. denied*, 570 U.S. 919 (2013) (holding that where a phone has a built-in geolocation function, there is no privacy in the location information transmitted by the device, at least for three days of tracking).

70 States requiring a warrant for all location information: Maine, Minnesota, Montana, New Hampshire, Rhode Island, Tennessee, Utah, Vermont, and Wisconsin. States requiring a warrant for real-time location infor-

mation: Illinois, Indiana, Maryland, and Virginia (with additional state supreme court decisions from Florida and New Jersey). States requiring a warrant to use a cell site simulator: Illinois and Vermont. States requiring a court order to use a cell site simulator: California, Connecticut, and Washington State. States requiring a court order for location information: California, Colorado, Connecticut, Louisiana, and Virginia.

71 Department of Justice, Office of Public Affairs, "Justice Department Announces Enhanced Policy for Use of Cell site simulators: Increased Privacy Protections and Higher Legal Standards to be Required," September 3, 2015, https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators; Alejandro N. Mayorkas, Deputy Secretary, "Department Policy Regarding the Use of Cell site simulator Technology," Policy Directive 047-02, Department of Homeland Security, October 19, 2015, https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.

72 *Id.*; *see also* Cell site simulator Act of 2015, H.R. 3871, 114th Cong. (2015) (introduced but not passed); Cell Location Privacy Act of 2017, H.R. 1061, 115th Cong. (2017) (same).

73 Committee Staff Report, *supra* note 8, at 30 (detailing state laws in California, Washington, Virginia, Utah, and Illinois); *see also* "Cell Phone Location Tracking Laws by State," American Civil Liberties Union, accessed October 11, 2018, https://www.aclu.org/map/cell-phone-location-tracking-laws-state (providing an interactive map identifying tracking laws by state); "Are there laws or policies regulating cell site simulators at the state level in the US?," Cell site simulators: Frequently Asked Questions, Electronic Frontier Foundation, accessed October 11, 2018, https://www.eff.org/node/89287#faq-Are-there-laws-or-policies-regulating-cell-site-simulators-at-the-state-level-in-the-US?-.

74 *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *see also* In re Smartphone Geolocation Data Application, 977 F.Supp.2d 129, 147 (E.D.N.Y. 2013) (holding that users are well aware of the geolocation functions of their smartphones, and thus have no reasonable expectation of privacy in that data).

75 *Carpenter*, 138 S.Ct. at 2217-2219, 2220 (2018); see also *id.* at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."); *Jones*, 565 U.S. at 417 (2012) (Sotomayor, J., concurring) (observing that the third-party doctrine is "ill suited to the digital age").

76 *Carpenter,* 138 S.Ct. at 2219-2220.

77 Ibid. at 2221.

78 Haas, *supra* note 16; Ellen Nakashima, "Agencies collected data on Americans' cellphone use in thousands of 'tower dumps'," *Washington Post,* December 9, 2013, https://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html?utm_term=.fd6dd1778bb5.

79 California Penal Code § 638.55(c).

80 "Department of Justice Policy Guidance: Use of Cell site simulator Technology," Department of Justice, accessed October 11, 2018, 6, https://www.justice.gov/opa/file/767321/download ("When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily. When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days."); *see also* Dave Maass, "Here are 79 California Surveillance Tech Policies. But Where Are the Other 90?," Electronic Frontier Foundation, April 11, 2016, https://www.eff.org/deeplinks/2016/04/here-are-79-policies-california-surveillance-tech-where-are-other-90; JPat Brown and Curtis Waltman, "Cell site simulator Census," MuckRock, accessed October 11, 2018, https://www.muckrock.com/project/cell-site-simulator-census-83/; Linda Lye, *StingRays: The Most Common Surveillance Tool the Government Won't Tell You About*, American Civil Liberties Union, 2014, 17 n. 77, https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won%27t_Tell_You_About.pdf (observing that immediate deletion raises collateral issues, including undermining possible challenges to a warrant's overbreadth).

81 The investigation and prosecution of individuals who took part in protests against President Trump's inauguration in 2016, for instance, has involved cracking locked cellphones and obtaining a warrant for a wealth of online information. Kelly Weill, "Feds Crack Trump

Protestors' Phones to Charge Them With Felony Rioting," *Daily Beast,* July 26, 2017, https://www.thedailybeast.com/feds-crack-trump-protesters-phones-to-charge-them-with-felony-rioting; Mark Rumold, "In J20 Investigation, DOJ Overreaches Again. And Gets Taken to Court Again," Electronic Frontier Foundation, August 14, 2017, https://www.eff.org/deeplinks/2017/08/j20-investigation-doj-overreaches-again-and-gets-taken-court-again.

82 Brady v. Maryland, 373 U.S. 83, 87 (1963) (requiring prosecutors to disclose to criminal defendants evidence that is "material either to guilt or to punishment").

83 Sidney Fussell, "Oakland Passes Nation's Strongest Surveillance Technology Ordinance Yet," *Gizmodo,* May 2, 2018, https://gizmodo.com/oakland-passes-nations-strongest-surveillance-technolog-1825725697; "PAC Surveillance Technology Ordinance Approved by City Council," City of Oakland, accessed October 10, 2018, https://www.oaklandca.gov/resources/pac-surveillance-technoloy-ordinance-approved-by-city-council; Michael Maharrey, "City of Berkeley Passes Ordinance Taking on Surveillance State," OffNow, April 18, 2018, https://offnow.org/city-of-berkeley-passes-ordinance-taking-on-surveillance-state/; see also "Community Control over Police Surveillance: #TakeCTRL," American Civil Liberties Union, accessed October 9, 2018, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance (ACLU CCOPS)..

84 See "The Public Oversight of Surveillance Technology (POST) Act: A Resource Page," Brennan Center for Justice, last updated October 24, 2017, https://www.brennancenter.org/analysis/public-oversight-police-technology-post-act-resource-page (detailing the proposed Public Oversight over Surveillance Technologies bill in New York City).

85 Kim Zetter, "California Now Has the Nation's Best Digital Privacy Law," *Wired,* October 8, 2015, https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/; R. Taj Moore, "So What's In the California Electronic Communications Privacy Act?", *Lawfare,* October 22, 2015, https://www.lawfareblog.com/so-whats-california-electronic-communications-privacy-act.

86 Committee Staff Report, *supra* note 8, at 31.

87 *Cf.* Bates, *supra* note 21, at 11 (deriding the limited protection offered by agencies' "self-policing" their use of Stingray technology).

88 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197 (1968).

89 18 U.S.C. § 2511; 18 U.S.C. § 2518(1)(c).

About the Brennan Center for Justice

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin American ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from ending mass incarceration to preserving Constitutional protection in the fight against terrorism. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, the courts, and in the court of public opinion.

About the Brennan Center's Liberty and National Security Program

The Brennan Center's Liberty and National Security Program works to advance effective national security policies that respect constitutional values and the rule of law, using innovative policy recommendations, litigation, and public advocacy. The program focuses on reining in excessive government secrecy, ensuring that counterterrorism authorities are narrowly targeted to the terrorist threat, and securing adequate oversight and accountability mechanisms.

About the Authors

Rachel Levinson-Waldman is Senior Counsel in the Brennan Center's Liberty and National Security Program, where she works on issues related to policing and technology, including law enforcement access to social media, predictive policing, body cameras, license plate readers, and cellular surveillance, as well as the federal government's use of surveillance technologies. Previously, she was senior counsel to the American Association of University Professors, and a Trial Attorney in the Civil Rights Division of the U.S. Department of Justice. She holds a J.D. from the University of Chicago Law School and a B.A. from Williams College.

Acknowledgments

The Brennan Center gratefully acknowledges The Bauman Foundation, Democracy Alliance Partners, Ford Foundation, Media Democracy Fund, and Open Society Foundations for their generous support of this work.

The author is grateful to current and former colleagues in the Liberty and National Security Program for their guidance and input on this paper, including Liza Goitein, Faiza Patel, and Michael Price. She received invaluable research and technical assistance from Research and Program Associates Raya Koreh and Erica Posey, and interns Stefan Ducich, Angie Liao, Jun Lei Lee, Alexia Ramirez, Raven Wells-Scott, and Wouter Zwart. She also benefited greatly from expertise offered by Stephanie Lacambra and Nathan Freed Wessler. Finally, she is grateful for the support offered by the Brennan Center's communications department, including Alden Wallace and Jennifer Woodhouse.

© 2018. This paper is covered by the Creative Commons Attribution-NonCommercial-NoDerivs license. It may be reproduced in its entirety as long as the Brennan Center for Justice at NYU School of Law is credited, a link to the Center's web pages is provided, and no charge is imposed. The paper may not be reproduced in part or in altered form, or if a fee is charged, without the Center's permission. Please let the Center know if you reprint.