CLAIRE POWERS*

Surveillance Remedies: Stingrays and the Exclusionary Rule

INTRODUCTION

A crime occurs, and a cell phone is stolen. By tracking the phone, police believe they can also track the person who committed the crime. They have no suspects, no leads, and no warrants. But they do have a secret (and I do mean secret) weapon. They circle the streets—one team on foot, another in a van—and fire up a small, box-like device. As they circle, they narrow their search, slowly focusing their

* J.D. Candidate 2018, University of Oregon School of Law; B.A. Middlebury College. Thank you to Professor Carrie Leonetti for the feedback, encouragement, and expertise.

efforts on a single neighborhood, then a single block, then a single apartment complex. They enter the complex. They walk the hallways. They pause at every door and every window. Finally, finding what and whom they are looking for, they stop.

What is going on? What tool allowed them to locate this suspect? The answer, the secret weapon, is a high tech surveillance device called a "stingray." In this real Florida case, a stingray allowed the police to track down a single cell phone, and thus locate a single suspect, by gathering information from every cell phone in the area.[1] As police drove through the streets, each and every cell phone in the vicinity was forced to "register" with the stingray as it drew near.[2] In other words, each and every cell phone unknowingly and involuntarily transmitted information to the police. Thus, as the search narrowed—down to a specific apartment complex—police began "lurking outside people's windows and sending powerful electronic signals into their private homes in order to collect information from within."[3] Only by intruding on the privacy of everyone could the police determine the location of a single person.

Stingrays and other forms of high tech surveillance have been the focus of many recent articles in legal journals and newspapers. From "Angel Fire," the secret aerial surveillance system in Baltimore, to "Hemisphere," the AT&T program designed to mine call records and analyze cellular data,[4] government surveillance has fascinated the American public. With emerging evidence of widespread use, unsettled case law, and vignettes like the one above, it is no surprise that the warrantless use of stingrays by police is controversial. While many academic papers have tracked the possibility and importance of preventative measures to ensure law enforcement's compliance with the Fourth Amendment, this Article examines what comes next. What happens—or should happen—after Fourth Amendment violations have *already* occurred?

Part I of this Note discusses the technology: What are stingrays and how are they used by law enforcement. Part II discusses the current

---

[1] *See* Thomas v. Florida, 127 So. 3d 658 (Fl. Dist. Ct. App. 2013); Nathan Freed Wessler, *VICTORY: Judge Releases Information about Police Use of Stingray Cell Phone Trackers*, ACLU (June 3, 2014, 3:15 PM), https://www.aclu.org/blog/victory-judge-releases-information-about-police-use-stingray-cell-phone-trackers.

[2] Wessler, *supra* note 1.

[3] *Id.*

[4] Kenneth Lipp, *AT&T Is Spying on Americans for Profit*, THE DAILY BEAST (Oct. 25, 2016, 1:13 AM), http://www.thedailybeast.com/articles/2016/10/25/at-t-is-spying-on-americans-for-profit.html.

state of the law regulating the warrantless use of stingrays. Part III discusses current Fourth Amendment remedies for illegal acts of surveillance, specifically, the exclusionary rule for illegally obtained evidence. Finally, Part IV discusses alternative remedies that might fare better in this context.

I
INTRODUCING THE TECHNOLOGY

A. Stingrays

Cell-site simulators, known commonly by trade names such as "Stingray,"[5] and "Hailstorm," are box-like, portable surveillance devices that allow law enforcement agencies to collect information and locate cell phones using cellular networks.

Cell phone networks are relatively simple to conceptualize. Each network provides service to a discrete geographic area by dividing land into "honeycomb-shaped segments."[6] Providers, such as Sprint or Verizon, equip each geographic segment with a transceiver, or "base station." These base stations, frequently located on the top of buildings or other relative high points, receive and disseminate the radio signals that contain voice conversations and text messages within the boundaries of each segment.[7] These base stations also collect data from those cell phones that are located within the segment, including "the strength, angle, and timing of the caller's signal."[8]

As a cell phone moves through these segments, it automatically connects with the closest base station—the base station emitting the strongest signal.[9] This provides continuous service as a phone moves from place to place, passing through different geographic regions served by different base stations.[10] The phone also engages in a process called "registration." All cell phones (when powered on) send a signal to the nearest base station every seven seconds, regardless of

---

5 Although "Stingray" is the brand name of a device that is no longer widely used (largely replaced by newer models), this Article will use the term as an interchangeable, generic name for all cell-site simulators, as is common practice.

6 Brian L. Owsley, *Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 187 (2014).

7 *Id.* at 188.

8 *Id.*

9 *Id.*

10 *Id.*

whether they are "in use."[11] The base station "registers" the signal, and "[t]his registration process enables the cell phone to communicate with its network, transmitting information and data, including audio content."[12]

A cell-site simulator, used by law enforcement officers, mimics a local base station. Because the simulator emits a stronger signal than an actual base station, nearby cell phones will connect with it, mistaking it for the closest tower. Thus, a cell-site simulator "causes or forces cell phones in an area to send their signals—with all the information contained therein—to the cell-site simulator," in essence registering with the simulator as it would with a cell tower.[13] This connection allows the devices to collect a significant amount of data, including identifying information (for example, the international mobile subscriber identifier or IMSI number), metadata about calls (like dialed numbers and the length of calls), content (like text messages or voice calls), and data usage (such as visited websites).[14]

Once deployed, these devices act indiscriminately; they intercept information from any and all nearby phones, not just from a specifically targeted phone.[15] In addition, because these devices are portable and can measure signal strength, law enforcement can triangulate the geographic position of a specific phone by moving through different cells and taking various readings as they travel.[16] "The authorities can then hone in on specific phones of interest to monitor the location of the user in real time or use the spy tool to log a record of all phones in a targeted area at a particular time."[17]

B. Law Enforcement's Use of the Technology

Information about law enforcement's use of these devices has long been cloaked in secrecy. Only recently, through creative discovery

---

[11] *Id.* at 188–89.

[12] *Id.* at 192.

[13] *In re* Application of the U.S. for an Order Relating to Tels. Used by Suppressed, No. 15 M 0021, 2015 WL 6871289, at *2 (N.D. Ill. Nov. 9, 2015).

[14] *Cell-Site Simulators*, ELEC. FRONTIER FOUND., https://www.eff.org/sls/tech/cell-site-simulators (last visited Mar. 14, 2017).

[15] Cyrus Farivar, *County Sheriff Has Used Stingray over 300 Times with No Warrant*, ARS TECHNICA (May 24, 2015, 10:00 AM), http://arstechnica.com/tech-policy/2015/05/county-sheriff-has-used-Stingray-over-300-times-with-no-warrant/.

[16] Owsley, *supra* note 6, at 193.

[17] Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013, 10:00 AM), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

requests from criminal defendants and exhaustive public information requests from civil rights and media organizations, has information about the expansive use of these devices started to emerge.[18] For example, though details about these devices began appearing in court documents in 2012,[19] certain federal authorities have been using stingray technology since the mid-1990s.[20]

The systemic implementation of this secrecy is becoming more clear. The government, to protect the technology, has insisted on an extensive structure of nondisclosure agreements between manufacturers and law enforcement agencies.[21] Specifically, the Federal Bureau of Investigation (FBI) signed a nondisclosure agreement with the Harris Corporation, the private company that produces and distributes the Stingray, Triggerfish, and other similar technology.[22] Local authorities wishing to purchase the devices have in turn been required to sign nondisclosure agreements with the FBI.[23] Even individual employees have been required to sign.[24]

Since 2004, federal agencies "have spent more than $30 million on Stingrays and related equipment and training."[25] These agencies include the FBI, Drug Enforcement Agency (DEA), United States Secret Service, Bureau of Immigration and Customs Enforcement,

---

[18] For example, the Electronic Privacy Information Center (EPIC), a civil liberties organization, has obtained documents relating to the FBI's use of stingray technology through ongoing Freedom of Information Act litigation. EPIC has requested approximately 25,000 pages of documents, 6000 of which are classified. In response, the FBI has released a few documents each month and a number of interesting details have emerged. For instance, the FBI has a manual called "cell tracking for dummies." Certain details in this manual suggest that the FBI is aware that its warrantless use of stingrays is legally questionable. Ryan Gallagher, *FBI Accused of Dragging Feet on Release of Info About "Stingray" Surveillance Technology*, SLATE (Oct. 9, 2012, 4:00 PM), http://www.slate.com/blogs/future_tense/2012/10/19/stingray_imsi_fbi_accused_by_epic_of_dragging_feet_on_releasing_documents.html.

[19] *See* LINDA LYE, ACLU, STINGRAYS: THE MOST COMMON SURVEILLANCE TOOL THE GOVERNMENT WON'T TELL YOU ABOUT 7–8 (2014), https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won%27t_Tell_You_About_0.pdf.

[20] Gallagher, *supra* note 17.

[21] *See* Mike Katz-Lacabe, *Non-Disclosure Agreements Between FBI and Local Law Enforcement for StingRay*, THE CENTER FOR HUMAN RIGHTS AND PRIVACY, https://www.cehrp.org/tags/nda/ (last visited Mar. 15, 2017).

[22] Mike Katz-Lacabe, *FBI Won't Say If it Has Agreement with Harris (But it Does)*, THE CENTER FOR HUMAN RIGHTS AND PRIVACY, https://www.cehrp.org/fbi-wont-say-if-it-has-agreement-with-harris-but-it-does/ (last visited Mar. 15, 2017).

[23] *See* Mike Katz-Lacabe, *supra* note 21.

[24] Owsley, *supra* note 6, at 200.

[25] Gallagher, *supra* note 17.

Internal Revenue Service, United States Army, and United States Navy.[26] Yet this device is hardly limited to federal use—state and local authorities in California, Texas, Wisconsin, New York, Florida, Illinois, Michigan, Maryland, Alaska, Washington, Oklahoma, Louisiana, and North Carolina also have confirmed access to cell-site simulators.[27]

Law enforcement uses these devices for a variety of purposes. These include locating missing persons, kidnap victims, fugitives, and those who may have simply failed to appear for court.[28] Stingrays can also be used to gather evidence for an ongoing investigation. In one New Jersey case, law enforcement used the device to build a case against a suspected drug dealer.[29] In Miami, procurement records show that police officers obtained a stingray to monitor cell phones at a free trade conference in 2003.[30] In San Bernardino, police admitted to using a stingray device more than 300 times.[31] The Baltimore public defender's office began to reexamine more than 2000 cases in which police secretly used stingrays after a 2015 newspaper investigation revealed a nondisclosure agreement between local police, prosecutors, and the FBI.[32]

---

[26] *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Mar. 13, 2017).

[27] *Id.*

[28] Cyrus Farivar, *Powerful "Stingrays" Used to Go After 911 Hangup, ATM Burglary*, ARS TECHNICA (Feb. 25, 2015, 4:45 AM), https://arstechnica.com/tech-policy/2015/02/powerful-stingrays-used-to-go-after-911-hangup-atm-burglary/; TALLAHASSEE POLICE DEP'T (2014), https://www.documentcloud.org/documents/1674421-03-27-2014-master-ce-log.html (last visited Sept. 30, 2017).

[29] United States v. Tutis, 216 F. Supp. 3d 467, 475–76 (D.N.J. 2016).

> By gathering identifying signals from many cell phones in proximity, and then gathering new samples from other locations where the suspect is present at other times, a law enforcement officer can narrow the list of identified cell phones to those that watch the suspect's locations and eliminate the many that do not appear to follow the suspect from one place to another. By such process of elimination, the officer can deduce the phone numbers which may belong to the suspect, and then match those few numbers to numbers known to be involved in the illegal transactions. Thus, from an array of cell phone identification data at various locations where the suspect is known to be when the CSS is used, the officer can by process of elimination and deduction narrow the field to the data associated with the suspect's cell phone or phones.

Id.

[30] Gallagher, *supra* note 17.

[31] Farivar, *supra* note 15.

[32] Nicky Woolf, *2,000 Cases May be Overturned Because Police Used Secret Stingray Surveillance*, THE GUARDIAN (Sept. 4, 2015, 2:09 PM), https://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance.

Although, as discussed above, cell-site simulators have extensive tracking and data gathering capabilities, the FBI has stated that it does not use stingrays to "intercept the *content* of communications."[33] The devices do, however, have the technological capability to do so.[34] Additionally, procurement documents indicate that the stingray can be used with compatible software to boost its capabilities. "FishHawk" software, for example, allows authorities to eavesdrop on conversations. "Porpoise" software allows law enforcement officers to capture and surveil text messages.[35]

II
STATE OF THE LAW: LEGAL PROHIBITIONS AGAINST STINGRAY USE

Different jurisdictions have responded in different ways as information about stingrays' capabilities, and law enforcement's use thereof, has slowly emerged. Some states have created statutory restrictions, requiring law enforcement officers to obtain a warrant before using cell-site simulator technology.[36] The Department of Justice (DOJ), which houses the FBI, instituted a policy requiring federal agents to obtain a warrant and attempt a less-invasive search with a pen register (which tracks only telephone metadata) before using a stingray in criminal investigations (except in limited, exceptional, or exigent circumstances).[37] Case law on when and how cell-site simulators may be used, however, remains scarce and conflicting. Information about the general constitutional protections and remedies of the Fourth Amendment is therefore helpful background.

---

33 Gallagher, *supra* note 17 (emphasis added).

34 LYE, *supra* note 19, at 3 n.23.

35 *Id.*

36 States that require warrants for real-time tracking include California, Virginia, Washington, and Utah. *See, e.g.*, Joshua Brustein, *State Laws Start Catching Up to Police Phone Spying*, BLOOMBERG TECH. (Mar. 24, 2015, 9:43 AM), https://www.bloomberg.com/news/articles/2015-03-24/state-laws-start-catching-up-to-police-phone-spying; Cyrus Farivar, *Judge Rules in Favor of "Likely Guilty" Murder Suspect Found via Stingray*, ARS TECHNICA (Apr. 26, 2016, 10:30 AM), http://arstechnica.com/tech-policy/2016/04/citing-unconstitutional-search-via-Stingray-judge-suppresses-murder-evidence/.

37 U.S. DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3 (2015), https://www.justice.gov/opa/file/767321/download.

A. The Fourth Amendment

The Fourth Amendment provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[38] As a basic rule, this means that law enforcement must obtain a warrant before conducting a search; warrantless searches "are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[39] The first question is therefore whether a "specific action or intrusion by the government constitutes a 'search' within the meaning of the Amendment."[40] As a foundational matter, this question has given rise to a surprisingly complex and nuanced analysis.

Historically, the Supreme Court construed the protection against unreasonable searches as one rooted in property—an officer who trespassed on or into the property of another conducted a search for Fourth Amendment purposes.[41] In *Katz v. United States*, however, the paradigm shifted, with courts looking instead to an individual's reasonable expectation of privacy.[42] Any act that invades a person's "reasonable expectation of privacy" is a search pursuant to the Fourth Amendment and, thus, barring a handful of exceptions, must be judicially authorized by a search warrant. In *Katz*, when the defendant entered a public telephone booth and closed the door behind him, he manifested a reasonable belief that his conversation would be private.[43] The Supreme Court thus held that officers' use of a device that recorded his telephone conversation while in that telephone booth violated the Fourth Amendment.[44]

Since *Katz*, numerous Supreme Court cases have construed and refined the meaning of a "reasonable expectation of privacy." In *Smith v. Maryland*, for example, a defendant challenged the admissibility of data collected by a pen register that recorded the phone numbers dialed from his home.[45] The police requested the telephone company install the device without first obtaining a

---

38 U.S. CONST. amend. IV.

39 Katz v. United States, 389 U.S. 347, 357 (1967) (footnotes omitted).

40 Owsley, *supra* note 6, at 218 (quoting Timothy Casey, *Electronic Surveillance and the Right to be Secure*, 41 U.C. DAVIS L. REV. 977, 983 (2008)).

41 Olmstead v. United States, 277 U.S. 438, 464 (1928).

42 *Katz*, 389 U.S. at 347.

43 *Id.* at 352.

44 *Id.* at 359.

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

warrant.[46] The Court asked whether the defendant had "a 'justifiable,' a 'reasonable' or a 'legitimate expectation of privacy'" in the numbers he dialed and ultimately concluded that he did not.[47] In other words, because everyone knows that phone companies record dialed numbers, there is no reasonable expectation of privacy with regard to that information. Thus, no Fourth Amendment violation exists when officers access this information without a warrant.

Smith v. Maryland was followed by *United States v. Miller*, in which the Supreme Court expounded upon the idea of the "third-party doctrine."[48] Under this doctrine, a defendant who voluntarily turns over information to a third party (such as a bank, phone company, or internet service provider) loses his "reasonable expectation of privacy" in that information.[49] In *Miller*, federal officers used a grand jury subpoena to obtain a defendant's bank records directly from the bank.[50] The defendant filed a motion to suppress the resulting evidence, arguing that because officers did not obtain a warrant, by seizing his records they violated his Fourth Amendment rights.[51] The Court, however, concluded that the defendant did not have a reasonable expectation of privacy because he had voluntarily provided his information to the bank in the regular course of his various financial transactions.[52] Consequently, the Court held there was no protected Fourth Amendment interest.[53]

In cases where the government has conducted direct surveillance of a suspect, the Supreme Court has outlined a number of actions that violate the Fourth Amendment. In *Kyllo v. United States*, for example, the Court concluded that officers' use of a thermal imager to detect heat emanating from a private home was a search for Fourth Amendment purposes.[54] In *United States v. Jones*, the Court held that officers conducted an unlawful search when they trespassed, without warrant, onto the defendant's property by installing a GPS tracking device on his vehicle.[55] In *Riley v. California*, the Court unanimously

---

[46] *Id.* at 737.

[47] *Id.* at 740–42.

[48] United States v. Miller, 425 U.S. 435 (1976).

[49] *Smith*, 442 U.S. at 743–44.

[50] *Miller*, 425 U.S. at 436.

[51] *Id.*

[52] *Id.* at 442.

[53] *Id.* at 445.

[54] Kyllo v. United States, 533 U.S. 27 (2001).

[55] United States v. Jones, 565 U.S. 400, 404–05 (2012).

held that police needed a warrant to search the cell phone they seized during a search incident to arrest.[56]

These cases, taken together, set the legal framework under which law enforcement's use of stingray technology will be assessed. Without further direction from the Supreme Court, however, lower courts will likely remain split on whether the use of this technology constitutes a Fourth Amendment search and whether law enforcement must obtain a warrant. Does a cell phone user maintain a reasonable expectation of privacy in his or her phone's current location information? Stingray searches necessarily involve the direct interception of cell phone data. But do cell phone owners *voluntarily* provide their location information to cell phone companies in a way that might invoke the third-party doctrine of *Smith* and *Miller*? And does it matter whether law enforcement officers obtain real-time location information from a cellular service provider or obtain it themselves directly from a suspect's phone by using a stingray to mimic a cell tower and thus intercept phone signals?

B. Challenging Law Enforcement's Use of Stingrays

There are very few cases in which defendants have directly challenged the government's use of a stingray. This stems, in part, from the systemic secrecy surrounding the technology.[57] Some of the first cases to explicitly address the issue are *United States v. Rigmaiden*,[58] *Maryland v. Andrews*,[59] *In the Matter of the Application of the United States of America for an Order Relating to Telephones Used by Suppressed*,[60] and *United States v. Patrick*.[61] While perhaps none of these cases provide a clear answer as to whether use of the stingray technology amounts to a search under the Fourth Amendment, each makes Supreme Court review more necessary and probable.

The first case in which a defendant discovered and challenged the use of this technology came in 2012, with *United States v. Rigmaiden*.

---

56 Riley v. California, 134 S. Ct. 2473, 2495 (2014).

57 LYE, *supra* note 19, at 9.

58 United States v. Rigmaiden, No. CR 08-814, 2013 WL 1932800, at *1 (D. Ariz. May 8, 2013) (order denying defendant's motion to suppress); United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (order denying defendant's motion for discovery).

59 Maryland v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016).

60 *In re* Application of the U.S. for an Order Relating to Tels. Used by Suppressed, No. 15 M 0021, 2015 WL 6871289, at *1 (N.D. Ill. Nov. 9, 2015).

61 United States v. Patrick, 842 F.3d 540 (7th Cir. 2016).

Through creative discovery, a pro se defendant discovered that the government had used a cell-site simulator to locate his apartment.[62] Raising the issue in a motion to suppress, the defendant, with the ACLU as amicus curiae, argued that the government's search warrant was deficient because it never disclosed the government's reliance on stingray technology.[63] Instead, it referenced only a "mobile tracking device" and gave no additional information about how the device had been used.[64] The court disagreed. It concluded that law enforcement officers had no obligation to disclose their location tracking methodology and that referring to the cell-site simulator as a "mobile tracking device" described the search with sufficient particularity to render the warrant valid.[65]

In *Maryland v. Andrews*, a state appellate court reached the opposite conclusion.[66] In *Andrews*, the government requested and obtained a pen register/trap and trace order, then used a cell-site simulator to find a suspect accused of attempted murder.[67] The police located the suspect inside an apartment, along with a gun.[68] When the trial court discovered that police had secretly used a cell-site simulator, it suppressed all evidence obtained by the state as a result of the search.[69] The Maryland Court of Appeals affirmed the trial court's decision to suppress, holding that the Fourth Amendment precluded the warrantless use of cell-site simulators and that the pen register order was not sufficient to justify the use of the invasive stingray technology.[70]

---

62 LYE, *supra* note 19, at 8; Cory Doctorow, *How an Obsessive Jailhouse Lawyer Revealed the Existence of Stingray Surveillance Devices*, BOING BOING (Jan. 14, 2016, 12:35 PM), http://boingboing.net/2016/01/14/how-an-obsessive-jailhouse-law.html; Cale Guthrie Weissman, *How an Obsessive Recluse Blew the Lid Off the Secret Technology Authorities Use to Spy on People's Cellphones*, BUS. INSIDER (June 19, 2015, 5:04 PM), http://www.businessinsider.com/how-daniel-rigmaiden-discovered-stingray-spying-technology-2015-6.

63 *Rigmaiden*, 2013 WL 1932800, at *14, *16.

64 *Id.* at *16.

65 *Id.* at *17.

66 Maryland v. Andrews, 134 A.3d 324, 327–29 (Md. Ct. Spec. App. 2016).

67 *Id.* at 354.

68 *Id.* at 326.

69 *Id.*

70 *Id.* at 327, 360–61. Following this decision, at least one additional Maryland trial court has suppressed evidence obtained using a warrantless stingray. *See* Cyrus Farivar, *Judge Rules in Favor of "Likely Guilty" Murder Suspect Found Via Stingray*, ARS TECHNICA (Apr. 26, 2016, 10:30 AM), http://arstechnica.com/tech-policy/2016/04/citing-unconstitutional-search-via-Stingray-judge-suppresses-murder-evidence/; *see also* Kim Zetter, *Spy Tool Ruling Inches the Stingray Debate Closer to the Supreme Court*, WIRED

Most recently, the United States Court of Appeals for the Seventh Circuit neatly sidestepped the stingray issue. In *United States v. Patrick*, police secretly used a stingray to locate a defendant after he violated the conditions of his parole.[71] Officers obtained a search warrant to track the defendant, but, like in *Andrews*, failed to disclose that a stingray would be used.[72] After locating the defendant driving on a public road, officers discovered a gun in his car.[73] Both parties conceded, for the purpose of the litigation, that use of a stingray constituted a Fourth Amendment search.[74] While the court, in dicta, seemed to question this concession, it also noted that officers not only failed to reveal their plans to use a cell-site simulator, but also "implied that they planned to track [the defendant] down using his phone company data . . . perhaps misleading the judge by omitting a potentially material fact."[75] However, the court also offered that "[a] fugitive cannot be picky about how he is run to ground."[76] Thus, the court ultimately affirmed the district court's denial of his motion to suppress evidence "[b]ecause Patrick was visible to the general public, he did not have any privacy interest in his location at the time, his arrest was supported by both probable cause and a valid arrest warrant that had been issued before making any effort to learn his location."[77] The court concluded:

> Questions about whether use of a simulator is a search, if so whether a warrant authorizing this method is essential, and whether in a particular situation a simulator is a reasonable means of executing a warrant, have yet to be addressed by any United States court of appeals. We think it best to withhold full analysis until these issues control the outcome of a concrete case.[78]

In a forceful dissent, Chief Judge Wood commented on the government's deliberate secrecy and obstructionist behavior, noting that "[u]ntil recently, the government has gone so far as to dismiss

---

(Apr. 6, 2016, 7:00 AM), https://www.wired.com/2016/04/spy-tool-ruling-inches-Stingray-debate-closer-supreme-court/.

71 United States v. Patrick, 842 F.3d 540, 545 (7th Cir. 2016); Cyrus Farivar, *Warrantless Stingray Case Finally Arrives Before Federal Appellate Judges*, ARS TECHNICA (Jan. 29, 2016, 4:00 AM), http://arstechnica.com/tech-policy/2016/01/warrantless-Stingray-case-finally-arrives-before-federal-appellate-judges/.

72 *Patrick*, 842 F.3d at 546.

73 *Id.*

74 *Id.* at 544.

75 *Id.*

76 *Id.* at 545.

77 *Id.* at 542.

78 *Id.* at 545.

cases and withdraw evidence rather than reveal that the technology was used."[79] He questioned whether the undivulged—indeed, purposefully concealed—use of a stingray exceeded the scope of the warrant and concluded that the district court should have held an evidentiary hearing to determine the full scope and capabilities of the technology.[80]

As is clear from the sparse and conflicting cases above, there is little consensus on the constitutional status of stingray tracking. And until the Supreme Court weighs in, this area will likely remain unclear.

III
REMEDIES

Assuming for the purposes of this Note that stingray tracking is a search for Fourth Amendment purposes, a key remedial question remains: What actually happens if law enforcement officers do engage in warrantless stingray tracking? In other words, what remedies do and should exist for such conduct?

A. The Exclusionary Rule

The primary remedy for a Fourth Amendment violation is the exclusionary rule.[81] In general terms, the exclusionary rule dictates that evidence gathered by police in violation of the Fourth Amendment may not be introduced against the defendant at trial.[82] For example, a court should exclude evidence that police uncover after searching a home or vehicle without first procuring a warrant or relying on an established exception to the warrant requirement.

The Supreme Court first established this rule as the remedy for Fourth Amendment violations in the 1914 case *Weeks v. United States*.[83] In doing so, the Court noted that exclusion of improperly obtained evidence "was essential to the Fourth Amendment's protection against unreasonable searches and seizures."[84] In a later case, the Court observed that without an exclusionary rule, the Fourth

---

79 *Id.* at 546 (Wood, C.J., dissenting).

80 *Id.*

81 1 JOSHUA DRESSLER, UNDERSTANDING CRIMINAL PROC. 56 (6th ed. 2013).

82 *Id.*

83 Weeks v. United States, 232 U.S. 383 (1914).

84 Eugene Milhizer, *The Exclusionary Rule Lottery Revisited*, 59 CATH. U.L. REV. 747, 749 (2010) (citing *Weeks*, 232 U.S. at 398).

Amendment would be reduced to a mere "form of words," a right without a remedy.[85] As Justice Brandeis further affirmed, "[t]o declare that in the administration of the criminal law the end justifies the means—to declare that the Government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution."[86]

When *Mapp v. Ohio* later incorporated the exclusionary rule to the states, it also reaffirmed the *Weeks* Court's justification for the rule.[87] However, in subsequent decisions, the Court shifted to its current conception of the rule—as a "judicially created remedy, rather than a personal constitutional right,"[88] with the primary purpose "to deter—to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it."[89] In other words, courts exclude evidence to send a message and deter future wrongdoing by law enforcement, not to vindicate the individual defendant whose rights were violated by an unconstitutional search.

B. The Exclusionary Rule Is an Inadequate Remedy for Stingray Violations

The exclusion of evidence is an inadequate remedy for Fourth Amendment violations in the context of cell-site simulators for two reasons. First, the government has a history of engaging in secretive tactics, using nondisclosure agreements, parallel construction, and misleading euphemisms to keep information about the technology hidden. This means that without additional safeguards, a defendant may never know whether a stingray was used to begin with. Second, because stingrays are frequently used to simply *locate* suspects (for example, missing persons and fugitives), there is often no suppressible evidence derived from their use. As a result, the exclusionary rule in this context fails in its primary purpose of deterring Fourth Amendment violations.

---

[85] *Id.* at 749–50 (citing Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920)).

[86] *Id.* at 750 (internal quotation marks omitted) (citing Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J. dissenting)).

[87] Mapp v. Ohio, 367 U.S. 643, 649 (1961).

[88] Stone v. Powell, 428 U.S. 465, 494 n.37 (1976).

[89] Elkins v. United States, 364 U.S. 206, 217 (1960).

1. Parallel Construction and Policies of Secrecy

The government's secretive polices, ostensibly in place to protect the technology and preclude suspects from deploying counter measures, take many forms. Parallel construction, nondisclosure agreements, and other tactics ensure that information about cell-site simulators rarely makes it into the courtroom. Through public-record and discovery requests, however, news companies, civil rights organizations, and defense attorneys have slowly started to piece together an understanding of the technology and its uses.

Parallel construction is a tactic used by prosecutors and police departments to obscure the official use of cell-site simulators. It means "using Stingrays in the first instance, then reverse-engineering a case which they can safely bring to trial without mentioning the surveillance equipment."[90] For example, an officer might use a stingray to locate a suspect, then work backward to construct an evidentiary case without referencing the direct fruits of the stingray tracking.

This practice has been documented in other contexts. For example, the National Security Agency (NSA) has long insulated its potentially illegal data acquisition from the domestic law enforcement agencies who use its fruits in criminal investigations:

> When the NSA finds evidence of criminal activity within FAA-acquired phone, email, and Internet records, it turns over "tips" to the [Special Operations Division (SOD) of a federal investigatory agency]. One federal agent estimated that about sixty percent of tips yield helpful information. Federal agents are trained to "sanitize" the information and cover up its origin as an FAA collection. For example, the SOD will tell a law enforcement agent "to look for a specific car at a certain place" and to "find his or her own reason to stop and search the car." Agents are instructed not to reveal the tip in police reports or affidavits or discuss it with prosecutors or judges. Former DEA agent Finn Selander compared the process to "laundering money–you work it backwards to make it clean." While the rhetoric of "sanitiz[ing]" and "laundering" information to remove tainted information may sound flagrantly illegal, these agents use such rhetoric so publicly because these practices are fairly common with other types of criminal investigations.[91]

The same process may be mirrored in the context of stingrays, or it may be even more subtle. For example, law enforcement might refer

---

[90] Woolf, *supra* note 32.

[91] Amanda Claire Grayson, Note, *Parallel Construction: Constructing the NSA Out of Prosecutorial Records*, 9 HARV. L. & POL'Y REV. S25, S33 (2015).

to a stingray as a "confidential informant."[92] Defense attorneys have reported hearing "[t]erms like 'we located this phone using information from a confidential source,' which sounds a whole lot like they had an informant; it doesn't sound like they were using a sophisticated electronic device forcing all phones in the area to report back."[93]

Law enforcement uses other tactics to maintain the secrecy of these devices as well. These include requiring agencies to sign nondisclosure agreements, dismissing cases rather than revealing information in court, and using misleading language in police reports and even court documents. Indeed, defense attorneys and civil rights organizations have recounted the lengths that prosecutors and police will go to in order "to avoid being forced to reveal their use of these devices."[94] This might include using pen register/trap and trace orders for stingray tracking, "without much, if any, reference to the fact that the device to be used is a different type of electronic surveillance than the traditional pen register."[95] It might also include using less than candid legal authority for such requests,[96] or using "inscrutable euphemisms" to obscure sources and technology.[97] For example, while the government in *Rigmaiden* eventually admitted to using a cell-site simulator, the original warrant request made only fleeting reference to an unspecified "mobile tracking device."[98] The device was described as "mobile tracking equipment [that] ultimately generate[s] a signal that fixes the geographic position of the Target [Device]."[99] The request for a warrant gave no additional information about how the device actually functioned. Significantly, the phrase "mobile tracking device" "typically refers to GPS devices (or so-

---

92 E-mail from Kenneth Castro, Sergeant, Sarasota Police Dep't, to Terry Lewis, Chief of Police, N. Point Police Dep't (Apr. 15, 2009, 11:25 AM), https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf [hereinafter Castro E-mail].

93 Woolf, *supra* note 32. In addition, "[a]ccording to emails obtained by the ACLU of Florida through a public records request, police officers with the Sarasota Police Department in Florida '[i]n reports or depositions' 'simply refer [to information from an IMSI catcher] as '. . . information from a confidential source regarding the location of the suspect.' They have done so 'at the request of the U.S. Marshalls.'" LYE, *supra* note 19, at 10 n.63.

94 Woolf, *supra* note 32.

95 Owsley, *supra* note 6, at 200.

96 *Id.*

97 Woolf, *supra* note 32.

98 LYE, *supra* note 19, at 6–7.

99 *Id.* at 7.

called 'bumper beepers')," rather than a cell-site simulator.[100] While the *Rigmaiden* court found this description sufficient, other courts have flagged the use of such misleading language. The *Patrick* court noted that law enforcement officers clearly "implied that they planned to track [the defendant] down using his phone company's data . . . perhaps misleading the judge by omitting a potentially material fact."[101] This observation did not, however, change the court's analysis or conclusion.

Nondisclosure agreements have also greatly limited the exclusionary rule's efficacy in deterring police misconduct by mandating widespread secrecy. In Florida, for example, public-records requests revealed e-mails that discussed how police departments, at the request of federal agencies, obscure information about the devices. Specifically, when one detective was "too explicit in a probable cause affidavit (PCA), specifically detailing 'the investigative means used to locate the suspect,'" the department was asked to "seal the old affidavit and submit a new, more vague one."[102] One e-mail openly stated:

> In the past, and at the request of the U.S. Marshalls [sic], the investigative means utilized to locate the suspect have not been revealed so that we may continue to utilize this technology without the knowledge of the criminal element. In reports or depositions we simply refer to the assistance as "received information from a confidential source regarding the location of the suspect." To date this has not been challenged.[103]

These nondisclosure agreements also often include clauses requiring the prosecution to dismiss charges rather than disclose information about the use of stingray technology.[104] For example, the

---

100 *Id.* at 9.

101 United States v. Patrick, 842 F.3d 540, 544 (7th Cir. 2016).

102 Castro E-mail, *supra* note 92; Megan Geuss, *Cops Hid Use of Phone Tracking Tech in Court Documents at Feds' Request*, ARS TECHNICA (June 19, 2014, 9:01 PM), http://arstechnica.com/tech-policy/2014/06/cops-hid-use-of-phone-tracking-tech-in-court-documents-at-feds-request/.

103 Castro E-mail, *supra* note 92.

104 Farivar, *supra* note 15 ("[T]he [San Bernardino Sheriff's Department], like other departments nationwide, maintains a questionable non-disclosure agreement (NDA) with the FBI that indicates that the agency will work with local prosecuting authority to dismiss cases rather than reveal information in court about stingrays [sic]."); *see also* Castro E-mail, *supra* note 92; Memorandum from Christopher M. Piehota, Special Agent in Charge, Fed. Bureau of Investigation, to Scott R. Patronik, Chief, Erie Cty. Sheriff's Office, (June 29, 2012), https://www.documentcloud.org/documents/1727748-non-disclosure agreement.html#document/p3/a212440 [hereinafter Piehota Memorandum].

Patrick court noted that "[u]ntil recently, the government has gone so far as to dismiss cases and withdraw evidence rather than reveal that the technology was used."[105]

Other examples come directly from newly revealed nondisclosure agreements. One signed by the Erie County Sheriff's office in New York states:

> [T]he 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.[106]

Dismissals attributable to nondisclosure agreements are not unheard of. In St. Louis, prosecutors dropped charges against the alleged getaway driver in a string of robberies after the defense learned that police had used a stingray in her case.[107] In New York, the FBI "instructed the police to drop criminal charges instead of revealing 'any information concerning the cell site simulator or its use.'"[108] In Tallahassee, prosecutors offered a defendant charged with robbery with a deadly weapon the "deal of the century"—six months of probation—to avoid allowing the defense to examine the stingray used to locate him.[109]

In *Andrews*, after a suppression hearing, the court squarely addressed the State's nondisclosure agreement and its effects on the

---

105 *Patrick*, 842 F.3d at 546.

106 Piehota Memorandum, *supra* note 104, at 3.

107 Cyrus Farivar, *Robbery Suspect Pulls Guilty Plea After Stingray Disclosure, Case Dropped*, ARS TECHNICA (Apr. 29, 2015, 2:04 PM), http://arstechnica.com/tech-policy/2015/04/alleged-getaway-driver-challenges-Stingray-use-robbery-case-dropped/.

108 Jose Pagliery, *FBI Lets Suspects Go to Protect 'Stingray' Secrets*, CNNMONEY (Mar. 18, 2015 3:15 PM), http://money.cnn.com/2015/03/18/technology/security/police-Stingray-phone-tracker/.

109 Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH. POST (Feb. 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; Pagliery, *supra* note 108.

court. There, the nondisclosure agreement required "the Office of the State's Attorney for Baltimore [to], at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to provide, any information concerning the Harris Corporation wireless collection equipment/technology[.]"[110] The court indicated that the agreement and the State's resulting actions were problematic. By attempting to protect the technology and adhere to the nondisclosure agreement, the State "prevent[ed] the court from exercising its fundamental duties under the Constitution."[111] Specifically, without the necessary information, the court could not determine whether the search was reasonable under the Fourth Amendment and concluded that the State's actions were "inimical to the constitutional principles we revere."[112]

Such secretive tactics might help explain why so few judicial decisions address the use of these electronic surveillance devices. Defense attorneys do not know what red flags to look for, what to ask for, or when to ask for it. Policies of secrecy inhibit the development of regulating case law. Even if defendants discover stingray use in their case and attempt to challenge such use in court, restrictive nondisclosure agreements often mandate that police and prosecutors withdraw or even drop the case rather than risk revealing stingray use.[113] If the information does not emerge to begin with, the exclusionary rule cannot come into play. Thus, the exclusionary rule is again ineffective to deter police misconduct in this context.

2. Additional Complications Based on "Whom" Law Enforcement Targets

The exclusionary rule in the context of stingrays is particularly problematic for another reason: Stingrays are not only used to build cases against suspects; they are often used to recover fugitives, FTAs, and missing persons. If no additional information is found in the course of location and arrest, there might be no derivative evidence to suppress. For example, if police are required to obtain a warrant before using a stingray, but instead use the device, without a warrant, to locate someone who violates parole, what then? Assuming police find no additional evidence of a crime on his person, what can be

---

110 Maryland v. Andrews, 134 A.3d 324, 338 (Md. Ct. Spec. App. 2016) (alteration in original).

111 *Id.*

112 *Id.* at 339.

113 Woolf, *supra* note 32.

suppressed using the exclusionary rule? The arrest itself may be allowed in, but what about the location?

In *Patrick*, the Seventh Circuit wrote:

> A person wanted on probable cause (and an arrest warrant) who is taken into custody in a public place, where he had no legitimate expectation of privacy, cannot complain about how the police learned his location. Recall that the cell-site simulator (unlike the GPS device in *Jones*) was not used to generate the probable cause for arrest; probable cause to arrest Patrick predated the effort to locate him. From his perspective, it is all the same whether a paid informant, a jilted lover, police with binoculars, a bartender, a member of a rival gang, a spy trailing his car after it left his driveway, the phone company's cell towers, or a device pretending to be a cell tower, provided location information. A fugitive cannot be picky about how he is run to ground. So it would be inappropriate to use the exclusionary rule, even if the police should have told the judge that they planned to use a cell-site simulator to execute the location warrant.[114]

In *Patrick*, of course, the police found evidence of an additional crime during the course of Patrick's arrest.[115] As the court seems to recognize, however, the exclusionary rule cannot apply to a defendant's location alone: "fugitive[s] cannot be picky about how [they are] run to ground."[116] Thus, even when the police obtained a warrant through deceptive and misleading wording, the court still concluded that locating the defendant with a cell-site simulator did not warrant the suppression of evidence. It follows then, that where *no* additional evidence is found, the result would be just as clear—there would be nothing to which to apply the exclusionary rule.

More broadly, while suppression may be sufficient in a case like *Andrews*, where police found incriminating evidence upon locating the defendant, the same is not true in the case where no incriminating evidence is discovered.[117] For certain cases—where someone is missing, failed to appear for court, violated parole, or is on the run—officers' primary concern may not be looking for evidence at all. Instead, police may be interested in location alone. In such cases, once the person is located, if there is no other incriminating evidence to suppress, there is no further debate on Fourth Amendment remedies. Unlike evidentiary suppression, outright dismissal is not a

---

114 United States v. Patrick, 842 F.3d 540, 545 (7th Cir. 2016).

115 *Id.* at 542.

116 *Id.* at 545.

117 *See* Nakashima, *supra* note 109.

Fourth Amendment remedy. In these cases, though the device itself has been used no differently, with no evidence to introduce there is no evidence to suppress, and, thus, the exclusionary rule loses its deterrence value.

Furthermore, from a law enforcement perspective, the potential gain (finding a fugitive) may outweigh any potential loss (suppressed evidence in a new prosecution). Moreover, because the device is frequently used to locate suspects, not just to build a case against one, in the situation described above, there may be no downside to the violation at all. Law enforcement may very well locate a suspect without finding additional evidence to suppress in the first place. Thus, the incentive to violate the Fourth Amendment may be even higher here than elsewhere. This is directly at odds with the primary purpose of the exclusionary rule—to deter Fourth Amendment violations in the first instance. If the benefit of violating the Fourth Amendment clearly outweighs any possible harm from such a violation, then the rule as a remedy is ineffective.

C. So What?

While this calculus may not be unique to the stingray context, there is something distinct here: When used, stingrays collect data on *everyone*. Stingrays do not narrowly target a single, suspicious cell phone. Instead, they gather information from *all* phones in the area—innocent and guilty phones alike. Unlike a situation where police might, for example, conduct a search of an individual without probable cause or warrant, when a stingray is used, it interferes with and gathers data on every single phone in the vicinity.

Moreover, when engaged, stingrays do not stop the process of forced registration at the threshold of the home or other private areas. Instead, they continue to gather information from the phone wherever it may be located. And we take our phones everywhere—to work, to school, even to bed. This means that a stingray will continue to extract information even from locations where there is a well-established reasonable expectation of privacy.

Stingrays cast a wide, indiscriminate net of surveillance, and the sheer number of potentially affected people is significant. Ninety-five percent of Americans own cell phones.[118] Seventy-seven percent of

---

[118] *Mobile Fact Sheet*, PEW RESEARCH CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.

Americans own smart phones.[119] As the technological capabilities of phones grow—allowing us to send e-mail, search the web, pay our bills—so too does the amount of information that can be uncovered through stingray-type technology. Real-time location tracking has the potential to reveal our work schedules, our religions, our medical issues, our family structures, our hobbies, our community ties, and beyond.

IV
ALTERNATIVES

While the exclusionary rule is the primary remedy for Fourth Amendment violations, other alternatives do exist. In this context, for example, the judiciary or legislature could shift its focus to the individual officers who engage in unconstitutional searches and seizures or the prosecutors who obscure this information in later cases. This might mean implementing police review boards with the authority to discipline or fire officers for constitutional wrongdoing. It might mean increasing criminal penalties for illegal surveillance generally, or increasing penalties for officers who use their official role to engage in illegal surveillance. It might include appointing special prosecutors, insulated from the constraints of the "team" mentality that develops between prosecutors and law enforcement agents who work together on a daily basis. Such prosecutors might be more willing to crack down on law enforcement agents who violate existing laws, like invasion of privacy or trespass. Alternatively, states or the federal government could authorize civil suits against individual officers and the agencies for which they work. These civil suits might result in compensatory and punitive damages, or even injunctive relief. With such stakes, both individual officers and their government agencies would have a significant incentive to comply, and ensure compliance, with the rules.

Though perhaps unlikely in today's political climate, top-down policies might also have a role here. While the DOJ has had, at least in the past, a policy that required law enforcement to obtain a warrant before using a stingray, these policies could go further. The FBI could refuse to sign nondisclosure agreements with the private companies that sell these devices. In criminal cases, prosecutors could be required by their offices to disclose all stingray use upfront. With information more readily available to all parties, the courts could

---

[119] *Id.*

begin overseeing and instituting appropriate safeguards that adequately uphold constitutional rights.

Each of these options has obvious drawbacks. Policies are unstable and subject to change with each administration. Pushback from law enforcement is likely. In fact, police unions and employment protections gained through collective bargaining might preclude citizen review boards from disciplining or firing police officers. While civil suits against officers for their constitutional violations are already authorized under 42 U.S.C. § 1983 and *Bivens*,[120] plaintiffs frequently run up against immunity doctrines. These doctrines, in essence, insulate officers from suit in all situations where a right is not clearly established at the time of the violation. This is especially problematic in cases of stingray surveillance, where the legal issues remain decidedly unsettled.

While these alternatives may not be perfect, they do move us one step closer to a viable remedy. Perhaps the most effective solution would be to combine these reactionary remedies with additional front-end deterrence mechanisms. This might mean advocating for statutory or judicial warrant requirements. Statutory warrant requirements could mimic, for example, the Federal Wiretap Act, which "provides a comprehensive scheme that strictly limits law enforcement's use of electronic surveillance and provides several mechanisms to ensure that surveillance stays within legal bounds."[121]

Developing case law could provide another important limit. For example, one Illinois district court devised three requirements for law enforcement to follow when using a cell-site simulator by balancing the competing interests of effective law enforcement with those privacy interests protected by the Fourth Amendment.[122] First, the court determined that "law enforcement officers must make reasonable efforts to minimize the capture of signals emitted from cell phones used by people other than the target of the investigation." This includes such reasonable measures as not using the "cell-site simulator when, because of the location and time, an inordinate number of innocent third parties' information will be collected." Second, the court required law enforcement to "destroy all data other than the data identifying the cell phone used by the target" within

---

120 Bivens v. Six Unknown Named Agents, 403 U.S. 388 (1971).

121 Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 13 (2004).

122 *In re* Application of the U.S. for an Order Relating to Tels. Used by Suppressed, No. 15 M 0021, 2015 WL 6871289, at *3–4 (N.D. Ill. Nov. 9, 2015).

forty-eight hours.[123] Finally, the court prohibited law enforcement from using any of the acquired data "beyond that necessary to determine the cell phone information of the target."[124] Encouraging the development of such concrete requirements and limits could help protect both defendants and the public at large.

Thus, perhaps the most effective solution would be to combine front-end warrant requirements—laid out by either statute or case law—with additional remedies as laid out above.

CONCLUSION

Should public safety concerns override the privacy intrusions that result from stingray surveillance? Even if law enforcement were to limit its use of the device—only tracking fleeing felons or kidnap victims and otherwise purging all data gathered from "innocent" phones—do the ends justify the means?

This Note posits that the answer is no. Stingrays are not technologically limited to tracking escaped felons and kidnap victims. Rather, they allow law enforcement to engage in real-time tracking, of anyone, without limit. They can capture identifying information, data usage, and content from every phone in a geographic area.[125] Without oversight from the courts, there is no guarantee of targeted use, probable cause, or the protection of any individual's reasonable expectation of privacy.

Law enforcement agencies have proven, in this context, that they are unwilling to be open about their use of these devices. Emerging case law, applications for public records, and discovery requests have demonstrated how nondisclosure agreements and other tactics are used to ensure widespread secrecy. While law enforcement agencies have stated that, despite the stingray's impressive capabilities, they use these devices only to locate individual suspects and otherwise ignore or delete any extraneous information they gather, secretive practices should make us cautious about accepting such statements at face value.

What is clear is that our current remedies are insufficient. Self-imposed limitations, like institutional policies, do not adequately protect constitutional rights. Case law is just beginning to develop on

---

123 *Id.* at *4.

124 *Id.*

125 *Cell-Site Simulators*, ELEC. FRONTIER FOUND., https://www.eff.org/sls/tech/cell-site-simulators (last visited Mar. 14, 2017).

the topic, and there is no guarantee that courts or legislatures will require law enforcement to obtain warrants before using stingrays. Indeed, to date, only one court—a state appellate court in Maryland—has definitively concluded that, under the Fourth Amendment, police must obtain a warrant before using a stingray. Only a few states have instituted statutory warrant requirements directed specifically at stingrays.[126]

While there may be value in this technology, there are also undeniable pitfalls. As Justice Brandeis wrote in *Olmstead v. United States*,

> [i]f the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means-to declare that the government may commit crimes in order to secure the conviction of a private criminal-would bring terrible retribution.[127]

The ends cannot justify the means, and a system dominated by secrecy—with scarce remedies for constitutional violations—is an alarming system indeed.

---

[126] Washington, California, and Vermont are among those states that have implemented statutory warrant requirements. *See, e.g.*, Cyrus Farivar, *California Cops, Want to Use a Stingray? Get a Warrant, Governor Says*, ARS TECHNICA (Oct. 8, 2015, 4:32 PM), https://arstechnica.com/tech-policy/2015/10/california-governor-signs-new-law-mandating-warrant-for-stingray-use/; *Washington State Limits Stingray Surveillance in Unanimously Approved 'Pro-Privacy' Law*, RT.COM, (May 12, 2015, 7:53 PM), https://www.rt.com/usa/257865-washington-state-stingray-signed/.

[127] Olmstead v. United States, 277 U.S. 438, 485 (1928).