NOTE

Stingray Confidential

*Spencer McCandless**

ABSTRACT

For nearly three decades, American law enforcement has conducted a coordinated campaign across all levels of government to hide its use of a powerful surveillance technology called cell site simulation. Commonly referred to as "stingrays," the devices allow police to covertly monitor cellular communications and track individuals in real-time with remarkable precision. Despite the tenuous legal ground on which the warrantless use of the devices rests, federal law enforcement has contractually forbidden their state and local counterparts from revealing to courts when they employ stingrays in an investigation. Records indicate authorities have facilitated this secrecy by attributing information gained from the devices to a "confidential source" when presenting it in court.

This Note examines law enforcement's concealment of stingrays within the broader context of "the informant's privilege," the legal doctrine that allows the government to shield the identity of confidential sources in criminal cases. It argues that neither the legal requirements of the privilege nor its underlying policy rationales support extending protections to inanimate surveillance technologies and the state actors who employ them. Further, this Note

* J.D., 2017, The George Washington University Law School; B.A., Political Science, 2013, University of New Orleans. I thank *The George Washington Law Review* staff and Brian Smith for their invaluable contributions throughout the publication process, as well as Professors Orin Kerr and Alan Morrison for their feedback and other assistance. Any remaining errors or oversights are my own.

contends that doing so undermines the rights of defendants and impinges on the core prerogatives of legislatures and the judiciary.

To rectify the hole in current law that permitted the secrecy surrounding stingrays to long go unchecked, this Note proposes a pre-trial disclosure requirement for the investigative utilization of technology not in general public use. The elements of such a requirement are well established in case law, and the simple rule would strike the proper balance between security, defendants' rights, and the integrity of the legal system.

Table of Contents

INTRODUCTION

Tadrae McKenzie was offered "the deal of the century."[1] Authorities had charged the then-teenager with robbery with a deadly weapon after the high school senior and two friends met up with a small-time drug dealer outside a Tallahassee Taco Bell and used BB guns to rob him of $130 worth of marijuana.[2] Florida law classifies the crime as a violent felony, carrying a minimum sentence of four years imprisonment.[3] Prior to trial, however, McKenzie's public defender stumbled upon a hole in law enforcement's account of their investigation: McKenzie did not closely match the victim's imprecise descriptions of the men who had robbed him, and the police never explained in any of their official statements and court filings how they had identified and located McKenzie to arrest him.[4]

When McKenzie's defender questioned the detectives in court, they initially made vague statements regarding phone records before finally conceding that they had employed a mysterious technology called a cell site simulator.[5] More commonly known as a "stingray" after the trade name of a popular model, the device imitates a cell tower in order to trick nearby phones into connecting to it.[6] Using a phone number provided by the robbery victim, the police intercepted the signal from McKenzie's prepaid disposable phone and followed it directly to his home.[7]

When McKenzie's public defender attempted to subpoena the stingray, however, the detectives insisted that a nondisclosure agreement with the FBI prevented them from showing or even discussing the device any further.[8] The secrecy was necessary, they contended, to avoid inhibiting law enforcement's ability to catch criminals.[9]

---

1 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.

2 *Id.*

3 *Id.*; *see* FLA. STAT. § 812.13(1)–(2)(b) (2016).

4 *See* Nakashima, *supra* note 1.

5 *Id.*

6 *Id.*; *see also* Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013, 1:00 PM), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/ (listing the specifications of various models of cell site simulators, including the StingRay). This note adopts the term "stingray" to generally refer to cell site simulators for the sake of simplicity and consistency.

7 Nakashima, *supra* note 1.

8 *Id.*

9 *Id.*

The Florida judge was not convinced: "Inhibiting law enforcement's rights are second to protecting mine!" he exclaimed before signing an order compelling the department to display the device in court.[10] Two days prior to the scheduled disclosure, McKenzie's public defender received notice that the prosecution was offering the most favorable plea bargain she had ever seen in an apparent effort to avoid revealing the technology.[11] McKenzie pleaded guilty to a second-degree misdemeanor and was sentenced to six months' probation.[12]

McKenzie was extremely lucky. Public records indicate that the Tallahassee Police Department alone deployed stingrays over thirty-five times per year on average between 2007 and 2014 in a city of only 186,000 people.[13] Similar figures have been reported by local law enforcement agencies across the country in response to public record disclosure suits.[14] Yet courts have remained unaware of the devices' existence in the vast majority of cases, and very few defense teams have connected the dots as McKenzie's counsel did.[15]

One reason for the paucity of legal conflict over the devices was revealed in a series of emails obtained by the ACLU through a public

---

10 *Id.*

11 *See id.*

12 *Id.*

13 *See* Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, ACLU (Feb. 22, 2015, 5:30 PM), https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida.

14 *See generally Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Mar. 21, 2017).

15 *See* Justin Fenton, *Former High Court Judge: Stingray Secrecy 'Wrong,'* BALT. SUN (Apr. 16, 2015, 7:14 PM), http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-stingray-murphy-react-20150415-story.html ("The extent of the Baltimore Police Department's use of the stingray device was largely secret until last week, when a detective testified in court that the agency has used it 4,300 times since 2007 . . . ."); Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 24, 2015, 7:51 AM), http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/ ("Defense attorneys assigned to many of those cases said they did not know a stingray had been used until USA TODAY contacted them, even though state law requires that they be told about electronic surveillance."); Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker,* NEWS TRIB. (Nov. 15, 2014, 12:00 AM), http://www.thenewstribune.com/news/local/crime/article25894096.html ("From 2009 to [early 2014], the county's Superior Court judges unwittingly signed more than 170 orders that . . . authorized [police] to use a device . . . to track a suspect's cellphone . . . ."); Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, WASH. POST (Mar. 7, 2013), https://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html (quoting Southern District of Texas Magistrate Judge Brian L. Owsley: "[T]here are magistrate judges around the country that are getting these requests and not realizing what these requests are.").

records request[16]: some prosecutors and law enforcement agencies refer to information obtained with stingrays as originating from a "confidential source" when using it in court.[17] Under a legal doctrine known as the informant's privilege, the government may often withhold the identity of an anonymous source, making further inquiry into the origin of the information a rare occurrence.[18] When courts believe law enforcement utilized a human informant rather than electronic surveillance, the fact of the surveillance goes unchallenged.[19]

This Note argues that neither the legal requirements of the informant's privilege nor the policy considerations underlying its existence support extending the doctrine to cover inanimate technology like the stingray or the state actors who employ it.[20] Further, this Note demonstrates that permitting law enforcement to withhold this information both violates the rights of individual defendants and frustrates traditional separation of powers principles by impinging on the core prerogatives of the legislature and the judiciary.[21] To prevent this and

16 *See* Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, ACLU (June 19, 2014, 9:01 PM), http://www.aclu.org/blog/internal-police-emails-show-efforts-hide-use-cell-phone-tracking.

17 *See, e.g.*, Email from Kenneth Castro, Sergeant, N. Port Police Dep't, to Terry Lewis, Chief, N. Port Police Dep't (April 15, 2009 11:25 AM), https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf. News outlets and civil rights groups have reported that federal law enforcement requested that state and local authorities use this terminology. *See, e.g.*, LINDA LYE, AM. CIV. LIBERTIES UNION OF N. CAL., STINGRAYS: THE MOST COMMON SURVEILLANCE TOOL THE GOVERNMENT WON'T TELL YOU ABOUT 35 n.63 (2014), https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won%27t_Tell_You_About_0.pdf; Kim Zetter, *Emails Show Feds Asking Florida Cops to Deceive Judges*, WIRED (June 19, 2014, 9:04 PM), https://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray/.

18 *See infra* Section II.C.

19 *See infra* Section II.C.

20 Existing scholarship primarily analyzes stingrays within the larger framework of the Fourth Amendment. *See, e.g.*, Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 186–87 (2014); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 150–52 (2013); Brittany Hampton, Note, *From Smartphones to Stingrays: Can the Fourth Amendment Keep Up With the Twenty-First Century?*, 51 U. LOUISVILLE L. REV. 159, 160 (2012); Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 492 (2012). The effort to shield the technology from public disclosure and judicial review, however, has thus far garnered little academic attention, and the confidential source rationale asserted to justify the secrecy has received even less.

21 The many legal ramifications of stingrays and the ways they have been used is too broad a topic to be covered with one stroke. This Note does not analyze, for example, the FBI's nondisclosure agreements within the field of contract law or the administrative law implications of the Federal Communication Commission's involvement. Similarly, it considers only those aspects of

similar information imbalances as surveillance technologies continue to develop, this Note proposes a solution under which the investigatory use of stingrays and other technologies not readily available to the public must be disclosed to a defendant in the same manner as exculpatory evidence under present law.

Part I provides background on stingrays, including the known history of the technology and its basic mechanics. It also details the coordinated efforts by law enforcement to keep the devices secret for nearly three decades and provides criticism of the campaign's methods and rationale. Part II presents a survey of the relevant legal framework involved in law enforcement's use of stingrays, as well as their subsequent withholding of information about the devices pursuant to the informant's privilege. Part III examines the manner in which courts have addressed similar disclosure failures in the past, as well as the legal significance they have attached to law enforcement's use of other obscure surveillance technology. It then utilizes these precedents to formulate a disclosure rule that will ensure the appropriate parties within the government evaluate the legal implications of new technologies, thus aiding the law in keeping pace with our rapidly evolving society.

I. Background on Stingrays

Many specific details about stingrays and their use are shrouded in secrecy. Investigative news reports and public record lawsuits have revealed key facts, however, from which a general picture may be pieced together.[22] This Part summarizes what is publicly known of the devices, including their origins and mechanics, as well as the efforts of law enforcement to keep them secret from courts and the general population.

A. Origins

As with many surveillance techniques employed by the military and intelligence communities, little is publicly known about the origins of stingrays.[23] Some news outlets report that the technology was developed for use by defense and spy agencies, while others claim the

---

Fourth Amendment and separation of powers analysis that bear on the topic at hand. These other areas form fertile ground for further scholarship.

22 *See generally Stingray Tracking Devices: Who's Got Them?*, *supra* note 14.

23 Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J.L. & Tech. 1, 13–14, 13 n.58 (2014).

devices were originally diagnostic equipment, utilized by technicians working on early cellular networks.[24] Even leading academics studying the legal significance of stingrays ultimately concede that "it is impossible to tell a totally accurate history of the development of wireless telephone interception technology."[25]

Regardless of its original purpose, the technology was well enough established as a surveillance tool by 1991 that stingrays were marketed to the general law enforcement community at the National Technical Investigators' Association's annual conference in Washington, D.C.[26] Scattered court filings, government documents, and news accounts suggest that the devices have been in use since then.[27]

Today, law enforcement's use of stingrays has become ubiquitous. An ACLU study compiled news reports and public records to identify over seventy law enforcement agencies in twenty-four states and the District of Columbia that employ these devices.[28] The organization states that this number "dramatically underrepresents the actual use of stingrays by law enforcement agencies nationwide" because many departments continue to withhold information about their purchase and use of the technology.[29]

B. A Summary of Stingray Mechanics

The equipment that makes up a stingray is relatively small, ranging from about the size of a bulky handset to that of a briefcase.[30] The devices exploit the architecture of cellular networks by imitating net-

---

24 *Compare, e.g.*, John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 8, 2013), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ ("Initially developed for military and spy agencies, the Stingrays remain a guarded secret by law enforcement . . . ."), *with* Tsutomu Shimomura, *Catching Kevin*, WIRED (Feb. 1, 1996, 12:00 PM), https://www.wired.com/1996/02/catching/ ("The simulator was a technician's device normally used for testing cell phones . . . .").

25 Pell & Soghoian, *supra* note 23, at 13 n.58.

26 *NATIA Conference*, FULL DISCLOSURE, 1991, at 7, 8. The National Technical Investigators' Association (NATIA) is a trade organization for individuals who "provide the technical operations, surveillance activities, and scientific support for hundreds of federal, state, and local agencies across the United States, Canada and the United Kingdom." *About Us*, NAT'L TECH. INVESTIGATORS' ASSOC., https://www.natia.org/about_us.php [https://perma.cc/UWA7-2NEQ] (last visited Mar. 24, 2017).

27 *See, e.g.*, *In re* Application of the United States for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 198–99 (C.D. Cal. 1995) [hereinafter *1995 Digital Analyzer Order*]; *The Office of Enforcement Operations—Its Role in the Area of Electronic Surveillance*, USABULLETIN, Sept. 1997, at 8, 13–14, https://www.justice.gov/sites/default/files/usao/legacy/2007/01/11/usab4505.pdf; Shimomura, *supra* note 24.

28 *Stingray Tracking Devices: Who's Got Them?*, *supra* note 14.

29 *Id.*

30 *See* Gallagher, *supra* note 6.

work towers, tricking phones and other devices within range into connecting to the stingray instead of the carrier's legitimate infrastructure.[31] By intercepting a signal in transit before relaying it to the intended receiver, stingrays are able to extract an extensive range of data about a user's transmission, including the contents of a call, text message, or visited website.[32] All the while, the individual user remains unaware that anything out of the ordinary is taking place.[33] Further, by measuring the strength and direction from which the repetitive "ping" signal that a phone constantly transmits to nearby towers originates, stingrays are able to track an individual with remarkable precision, even pinpointing the specific room in which a person is standing.[34]

Stingrays differ from other existing surveillance techniques, such as a wiretap or pen register, in two key respects. First, the devices do not require the permission or involvement of phone companies that previous techniques necessitated.[35] This undermines accountability by eliminating the paper trail inherent in the business records that result from coordinating surveillance with a third-party carrier.[36] Additionally, phone companies have previously served as a proxy advocate for their customers' privacy by pushing back on requests that were overbroad or otherwise improper.[37] In their absence, law enforcement is able to conduct surveillance without the participation of any other actor, facilitating the continued secrecy surrounding the devices.[38] Second, stingrays intercept and capture information not only from devices belonging to the target of the surveillance, but from all devices

---

31 *See* Owsley, *supra* note 20, at 192.

32 *See* Pell & Soghoian, *supra* note 20, at 146.

33 *See id.*

34 *See, e.g.*, Cyrus Farivar, *How Florida Cops Went Door to Door with Fake Cell Device to Find One Man*, ARS TECHNICA (June 4, 2014, 12:38 PM), http://arstechnica.com/tech-policy/2014/06/how-florida-cops-went-door-to-door-with-fake-cell-device-to-find-one-man/. In a process called "registration," most phones maintain contact with nearby network infrastructure by transmitting a simple, repeating transmission, regardless of whether the phone is in use. Owsley, *supra* note 20, at 188–89.

35 *See* U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 41 (rev. 2005), www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf ("[A] pen register/trap and trace order must be obtained by the government before it can use its own device to capture the ESN or MIN of a cellular telephone, even though there will be no involvement by the service provider.").

36 *See* Pell & Soghoian, *supra* note 20, at 146–47, 164.

37 *Id.* at 147.

38 *Id.* at 146–47.

present in the area.[39] The privacy interests of uninvolved bystanders are therefore implicated in addition to that of the suspect.[40]

C. *The Campaign of Secrecy*

Given that law enforcement has employed these devices for nearly three decades, it may seem remarkable that stingrays are not better known. As revealed through a series of lawsuits and investigative reports, this obscurity comes not as a result of random circumstance, but rather through a concerted effort by federal, state, and local governments to keep their use of the technology hidden.[41]

1. *Motivations and Justifications*

In their few public statements on the matter, law enforcement officials maintain that it is necessary to minimize any disclosure of details regarding the stingray's use and mechanics in order to prevent criminals from circumventing the technology.[42] The chief of the FBI's Tracking Technology Unit recently summarized this position in a sworn statement filed with an Arizona Superior Court in response to an open records lawsuit.[43] The chief stated that even disclosure of in-

---

39 *See id.* at 148.

40 *See id.* at 148–49.

41 *See, e.g.*, Am. Civil Liberties Union of N. Cal. v. U.S. Dep't of Justice, 13-CV-03127-MEJ, 2015 WL 3793496, at *16 (N.D. Cal. June 17, 2015) (ordering Department of Justice to disclose records on stingrays); Am. Civil Liberties Union of N. Cal. v. U.S. Dep't of Justice, 70 F. Supp. 3d 1018, 1039 (N.D. Cal. 2014) (same); Elec. Privacy Info. Ctr. v. FBI, 933 F. Supp. 2d 42, 44, 50 (D.D.C. 2013) (compelling FBI to turn over records on stingrays); Cyrus Farivar, *Journalist Appeals Lawsuit to Force Cops to Give Up Info on Stingray Use*, ARS TECHNICA (June 18, 2015, 11:55 AM), http://arstechnica.com/tech-policy/2015/06/journalist-appeals-lawsuit-to-force-cops-to-give-up-info-on-stingray-use/; Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's a Secret*, N.Y. TIMES (Mar. 15, 2015), http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html; Nakashima, *supra* note 1; Nakashima, *supra* note 15.

42 *See, e.g.*, Am. Civil Liberties Union of N. Cal., 2015 WL 3793496, at *12 ("[T]he Government argues that the information it seeks to protect . . . provides 'particularized detail on what tactics and factors DOJ attorneys take into account in deciding whether, how, and when to use [stingrays]—information that could assist unlawful actors in evading detection.'"); Am. Civil Liberties Union of N. Cal., 70 F. Supp. 3d at 1036 ("If would-be wrongdoers have access to the information . . . they will also learn when and where certain investigatory techniques are not employed, and would be able to conform their activities to times, places, and situations where they know that unlawful conduct will not be detected."); Deposition of FBI Supervisory Special Agent Bradley S. Morrison, Chief, Tracking Technology Unit, Operational Technology Division in Quantico, Virginia at 2, Hodai v. City of Tucson, No. C20141225, 2014 Ariz. Super. LEXIS 2158 (Ariz. Super. Ct. Dec. 11, 2014), *rev'd in part*, 365 P.3d 959 (Ariz. Ct. App. 2016) [hereinafter Morrison Deposition]; Nakashima, *supra* note 1 ("[The prosecutor] protested that the information about the device was sensitive and that disclosure could inhibit the police's ability to catch criminals.").

43 Morrison Deposition, *supra* note 42, at 1–2.

formation that appears to be "innocuous" about stingrays would allow "adversaries" to accumulate data on the technology over time.[44] If awareness becomes more widespread, criminals will "develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of this technology."[45] He further cited the utility of the device in investigating and prosecuting serious crimes, including "terrorism, kidnappings, murder, and other conspiracies," when defending the lack of transparency.[46] Records indicate that local law enforcement obtain stingray equipment under counterterrorism grants, lending some ostensible validity to these contentions.[47]

These justifications do not completely reflect reality, however, taken in light of evidence that law enforcement employs the devices in trivial and even political contexts. Police frequently utilize stingrays in routine investigations of, for example, small time robberies, auto theft, and harassing phone calls.[48] Further, several federal agencies with primary missions far removed from national security are in possession of the devices, such as the Drug Enforcement Administration, U.S. Immigration and Customs Enforcement, and the Internal Revenue Service.[49] Some have even claimed that police officers have used stingrays to monitor activists during public demonstrations.[50]

---

44 *Id.*

45 *Id.*

46 *Id.* at 2; *see also* CJ Ciaramella, *How the Justice Department Keeps Its Cell Phone Snooping a Secret*, VICE NEWS (June 18, 2014, 8:17 AM), https://news.vice.com/article/how-the-justice-department-keeps-its-cell-phone-snooping-a-secret ("Law enforcement agencies purchase the devices through federal grants under the auspices of anti-terrorism operations. Police say the technology can also be used for search-and-rescue operations, kidnappings, and mass-casualty events.").

47 *See* Tim Cushing, *Stingray Documents Show Law Enforcement Using 'Terrorism' to Obtain Equipment to Fight Regular Crime*, TECHDIRT (June 20, 2014, 3:35 AM), https://www.techdirt.com/articles/20140619/09211027625/stingray-documents-show-law-enforcement-using-terrorism-to-obtain-equipment-to-fight-regular-crime.shtml; Jason Leopold, *Police in Washington, DC Are Using the Secretive "Stingray" Cell Phone Tracking Tool*, VICE NEWS (Oct. 17, 2014, 9:05 AM), https://news.vice.com/article/police-in-washington-dc-are-using-the-secretive-stingray-cell-phone-tracking-tool ("Back in 2003, the Metropolitan Police Department (MPD) in Washington, DC was awarded a $260,000 grant from the Department of Homeland Security (DHS) to purchase surveillance technology called Stingray . . . . The rationale behind the DHS grant to MPD and other law enforcement agencies was to help them secure new antiterrorism technology . . . .").

48 Heath, *supra* note 15; Nakashima, *supra* note 1; Wessler, *supra* note 13.

49 *Stingray Tracking Devices: Who's Got Them?*, *supra* note 14.

50 Mike Krauser, *Activists Say Chicago Police Used 'Stingray' Eavesdropping Technology During Protests*, CBS CHICAGO (Dec. 6, 2014, 11:19 AM), http://chicago.cbslocal.com/2014/12/06/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/.

The threat of scrutiny by the public, lawmakers, and the courts may form an alternate motive for the secrecy. Legislators at the state and national level have responded to recent revelations about stingrays with concern, in some cases proposing and even passing legislation to limit police use of the technology.[51] The existing legal framework governing stingray surveillance is in flux and largely unsettled,[52] and some courts have denied police permission to deploy the technology when police have applied for it forthrightly.[53] These reactions indicate that a separate incentive, independent of the possibility of criminal circumvention, exists for law enforcement to keep their use of stingrays hidden: the secrecy facilitates their ability to freely use the surveillance devices without interference from other branches of government.

2. Methods and Criticism of Information Suppression

Regardless of motivation, the techniques that law enforcement has employed to suppress information about stingray technology are comprehensive and innovative, utilizing prosecutorial discretion, regulatory oversight, traditional principles of contract law, and a pointed lack of disclosure to courts. The effort begins with federal law enforcement tightly regulating the manufacture and sale of the technology.[54] Existing federal law aids in this restriction; the Wiretap Act[55] contains provisions making it illegal to "manufacture, distribut[e], possess[ ], [or] advertis[e] . . . wire, oral, or electronic communication inter-

---

51 *See, e.g.*, H.B. 1440, 64th Leg., Reg. Sess. (Wash. 2015) (requiring a warrant for all use of stingrays, passed unanimously); H.R. 3871, 114th Cong. (2015) (proposing warrant requirement for all use of stingrays); Letter from Senator Charles E. Grassley, Chairman, Senate Comm. on the Judiciary, & Senator Patrick Leahy, Ranking Member, Senate Comm. on the Judiciary, to Jeh Johnson, Sec'y, Dep't of Homeland Sec. (Sept. 29, 2015), http://www.leahy.senate.gov/imo/media/doc/9-29-15%20CEG-PJL%20Stingray%20letter%20to%20DHS.pdf (expressing concerns about privacy implications of stingrays); Letter from Senator Patrick Leahy, Chairman, Senate Comm. on the Judiciary & Senator Charles E. Grassley, Ranking Member, Senate Comm. on the Judiciary, to Eric Holder, Attorney Gen., & Jeh Johnson, Sec'y, Dep't of Homeland Sec. (Dec. 23, 2014), http://www.grassley.senate.gov/sites/default/files/news/upload/2014-12-23%20PJL%20and%20CEG%20to%20DOJ%20and%20DHS%20%28cell-site%20simulators%29.pdf (same).

52 *See infra* Part II.

53 *See, e.g.*, *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012) [hereinafter *2012 South Texas Order*] (denying application to use cell site simulator on grounds that a warrant, not court order, is required); *see also infra* Section II.C.

54 *See* Pell & Soghoian, *supra* note 23, at 38.

55 Wiretap Act, 18 U.S.C. §§ 2510–2522 (2012).

cepting devices" unless that device is intended for use by a domestic communications provider or state actor.[56]

The FBI further limits dissemination by coordinating with the primary company responsible for the manufacture and sale of stingrays to domestic law enforcement—the Harris Corporation.[57] Redacted emails obtained from the Federal Communications Commission ("FCC") through public records requests reveal that Harris Corporation includes language at the behest of the FBI when applying for equipment authorization licenses, conditioning government approval on two specifications.[58] As all information on the arrangement is derived from these heavily edited documents, it is unclear whether this cooperation is voluntary and what tools the FBI may have to enforce the agreement.[59] The licensing agreement first requires that the Harris Corporation limit marketing and sale of the devices to only public safety and law enforcement officials.[60] Second, the agreement stipulates that that the corporation sell stingrays to only those state and local agencies that have first coordinated the purchase with the FBI.[61]

Although statements from the FCC have raised some doubt as to whether the measure is legally mandated,[62] the FBI interprets the sec-

---

56 *Id.* § 2512.

57 *See* Pell & Soghoian, *supra* note 23, at 15. Other companies have sizable market shares within the military and intelligence communities, including Boeing, CellXion, and Martone Radio Technology. *Id.* at 15 n.76.

58 Email from [redacted] to [redacted] (June 28, 2010, 10:56 AM), https://www.aclu.org/sites/default/files/field_document/fcc_foia_harris_emails.pdf. [hereinafter Redacted FCC Email] ("Harris has agreed with the Federal Bureau of Investigations ('FBI') to request that the Commission condition its equipment authorization for the StingRay® product in order to address concerns over the proliferation of surreptitious law enforcement surveillance equipment."). Other emails obtained in the same request indicate that the license may also have been conditioned on the devices only being used in emergency situations. *See* Email from Tania W. Hanna, Vice President, Legislative Affairs & Pub. Policy, Harris Corp., to Bruce Romano, Associate Chief (Legal), FCC Office of Eng'g & Tech. (June 24, 2010, 6:13 PM), https://www.aclu.org/sites/default/files/field_document/fcc_foia_harris_emails.pdf ("As you may recall, the purpose is only to provide state/local law enforcement officials with authority to utilize this equipment in emergency situations."). The administrative and legal implications of conditional licensing warrant further investigation but are beyond the scope of this Note.

59 *See* Redacted FCC Email, *supra* note 58.

60 *See* Letter from Tania W. Hanna, Vice President, Legislative Affairs & Pub. Policy, Harris Corp., & Evan S. Morris, Counsel, Gov't Relations, Harris Corp., to Marlene H. Dortch, Sec'y, FCC 2 (Apr. 28, 2011), http://files.cloudprivacy.net/Harris-FCC-confidential-request-1.pdf [hereinafter Harris Corp. Letter 1]; Letter from Tania W. Hanna, Vice President, Legislative Affairs & Pub. Policy, Harris Corp., & Evan S. Morris, Counsel, Gov't Relations, Harris Corp., to Marlene H. Dortch, Sec'y, FCC 2 (Mar. 21, 2011), http://files.cloudprivacy.net/Harris-FCC-confidential-request-2.pdf [hereinafter Harris Corp. Letter 2].

61 *See* Harris Corp. Letter 1, *supra* note 60, at 2; Harris Corp. Letter 2, *supra* note 60, at 2.

62 *See* Letter from Julius P. Knapp, Chief, Office of Eng'g & Tech., FCC, to Phil Mocek

ond condition of Harris Corporation's FCC licenses to require that state and local law enforcement sign a contractual nondisclosure agreement with the agency prior to acquiring stingray equipment.[63] The boiler-plate nondisclosure agreement forbids the signing agencies from disclosing information on stingrays "to the public in any manner, including by [sic] not limited to: in press releases, in court documents, during judicial hearings, or during other public forums or proceedings."[64] The agreement goes on to require the signing agency to notify the FBI of any pending court order to release information related to the devices, and specifies that an agency will, "at the request of the FBI, seek dismissal of the case in lieu of using or providing . . . any information concerning the Harris Corporation wireless collection equipment/technology."[65] These terms make clear that the decision to withhold information on stingrays from courts, legislatures, and the public is not the result of individual agencies exercising discretion in isolation, but rather of a systemic policy orchestrated and enforced at the federal level. The agreement contractually prohibits state and local law enforcement from discussing stingrays in public in any capacity.[66] Moreover, it expressly contemplates withholding information about devices from courts, requiring that the signatory agencies omit any mention of the devices in all filings and other judicial proceedings.[67]

This contractual obligation to refrain from revealing information on the stingrays to courts stands at odds with the prosecution's duty of candor. Although the duty is codified in the ABA's Model Rules of

---

(Oct. 2, 2014), http://muckrock.s3.amazonaws.com/foia_files/FOIA_2014-671_Phil_Mocek.pdf (denying that the agency requires law enforcement to sign nondisclosure agreements). Though this discrepancy is ripe for further investigation, it lies beyond the scope of this Note.

63 *See* Letter from Ernest Reith, Acting Assistant Dir., Operational Tech. Div., FBI to Frederick H. Bealefeld, III, Police Comm'r, Balt. Police Dep't, & Gregg L. Bernstein, State's Attorney (July 13, 2011), http://s3.documentcloud.org/documents/1808819/baltimore-police-stingray-non-disclosure-agreement.pdf ("Consistent with the conditions on the equipment authorization granted to Harris by the Federal Communications Commission (FCC), state and local law enforcement agencies must coordinate with the Federal Bureau of Investigation (FBI) to complete this non-disclosure agreement prior to the acquisition and use of the equipment/technology authorized by the FCC authorization.").

64 *Id.* at 1–2 (containing copy of the agreement).

65 Letter from Christopher M. Piehota, Special Agent in Charge, Buffalo Div., FBI, to Scott R. Patronik, Chief, Erie Cty. Sherriff's Office (June 29, 2012), https://www.cehrp.org/text-of-fbi-non-disclosure-agreement-for-harris-corporation-stingray/ (detailing requirements and containing a copy of FCC's non-disclosure agreement).

66 *See id.* at 2.

67 *See id.* at 2–3.

Professional Conduct,[68] a general duty of candor does not arise from any statute or regulation, but instead is "attendant to the attorney's role as an officer of the court."[69] The Supreme Court has interpreted the responsibility to impose "a continuing duty" on all attorneys "to inform the Court of any development which may conceivably affect the outcome" of a proceeding[70] and to prohibit an attorney from "deliberately mislead[ing] the court with respect to either the facts or the law."[71] Because stingray surveillance does not fit neatly within current legal frameworks, the use of the technology can and has affected the outcome of judicial proceedings.[72] Prosecutors are therefore obligated by the duty of candor to disclose to courts when stingrays are used, and the contractual bar to disclosing this information conflicts with this responsibility. The infraction is more egregious when a prosecutor avoids the disclosure of stingray surveillance by asserting the informant's privilege, for this amounts to deliberately misleading the court to believe that the information gained from the surveillance originated from a human source who was not a state actor.

The requirement that prosecutors seek a dismissal in lieu of revealing information on stingray technology in court is likewise problematic. Under a theory of prosecutorial discretion, executive agencies normally have the unreviewable authority to determine whether and how to prosecute criminal offenses, including by the termination of cases through dismissals and plea bargains.[73] Underlying this doctrine are concerns for the separation of powers and the assumption that the executive is best positioned to determine the manner in which limited resources should be allotted in the pursuit of justice.[74] There are limits

---

68 *See* MODEL RULES OF PROF'L CONDUCT r. 3.3 (AM. BAR ASS'N 2016).

69 United States v. Shaffer Equip. Co., 11 F.3d 450, 457 (4th Cir. 1993).

70 Bd. of License Comm'rs of Tiverton v. Pastore, 469 U.S. 238, 240 (1985) (per curiam) (quoting Fusari v. Steinberg, 419 U.S. 379, 391 (1975) (Burger, C.J., concurring)).

71 McCoy v. Court of Appeals of Wis., 486 U.S. 429, 436 (1988).

72 *See, e.g.*, United States v. Espudo, 954 F. Supp. 2d 1029, 1043 (S.D. Cal. 2013) (holding that a warrant was required to use a stingray for real-time tracking of defendant); *2012 South Texas Order*, *supra* note 53, at 750–52 (denying application for pen register order and holding warrant was required to use stingray technology to obtain information on narcotics trafficker's phone); *see also infra* Section II.B.

73 U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL, § 9-27.110(B) (2017), https://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/27mcrm.htm#9-27.110.

74 *Id.*; *see* Rebecca Krauss, *The Theory of Prosecutorial Discretion in Federal Law: Origins and Developments*, 6 SETON HALL CIR. REV. 1, 10 (2009) (summarizing case law that holds the prosecutorial discretion lies solely with the prosecutor); *see also* McCleskey v. Kemp, 481 U.S. 279, 363 (1987) (Blackmun, J., dissenting) ("Prosecutors undoubtedly need adequate discretion to allocate the resources of their offices and to fulfill their responsibilities to the public in deciding how best to enforce the law . . . .").

to this power, however.[75] Executive actors have "basic responsibilities," including "making certain that the general purposes of the criminal law . . . are adequately met, while making certain also that the rights of individuals are scrupulously protected."[76]

Here, the dismissal of suits to avoid disclosure of stingray technology does not concern the allocation of limited resources by the officials best situated to determine their effective use. The nondisclosure agreements originate with federal entities far removed from the details of particular prosecutions, and they impose a blanket policy without regard to the circumstances of individual cases. The dismissals further subvert the rights of individuals by terminating proceedings before precedent may be established through court rulings, precluding courts from evaluating whether civil liberties were violated and imposing protections to prevent similar violations in the future. They are thus contrary to the underlying purposes, if not the legal requirements, of prosecutorial discretion.

The secrecy also raises questions of federalism, in some instances placing federal law enforcement in tension with state disclosure laws. When the ACLU submitted a state law-based public records request for information related to stingrays to the Sarasota Police Department, for example, the police initially scheduled a meeting for the organization to inspect a range of responsive files.[77] The police cancelled only hours before the appointment, however, claiming that the U.S. Marshals Service had deputized the local police officer responsible for maintaining the files and claimed federal ownership of the records.[78] Despite the ACLU's request that the disputed records be preserved in accordance with state law for review by a court, the Marshals Service removed the physical files to an undisclosed location.[79] The ACLU sought an injunction, and following the removal, a federal district court denied the organization's request for discovery regarding whether the officer actually maintained the records in the capacity of

---

75 Nader v. Saxbe, 497 F.2d 676, 679–80 n.19 (D.C. Cir. 1974) ("It would seem to follow that the exercise of prosecutorial discretion, like the exercise of Executive discretion generally, is subject to statutory and constitutional limits . . . .").

76 U.S. DEP'T OF JUSTICE, *supra* note 73, § 9-27.110(B).

77 Nathan Freed Wessler, *U.S. Marshals Seize Local Cops' Cell Phone Tracking Files in Extraordinary Attempt to Keep Information from Public*, ACLU: FREE FUTURE (June 3, 2014, 12:15 PM), https://www.aclu.org/blog/us-marshals-seize-local-cops-cell-phone-tracking-files-extraordinary-attempt-keep-information.

78 *Id.*

79 *Id.*; *see also* FLA. STAT. § 119.07(1)(h)–(i) (2016) (requiring preservation of disputed records for thirty days upon request by party seeking disclosure).

a federal official.[80] It then denied the ACLU's motion to remand the case to state court and dismissed the case.[81] The ACLU appealed, and the Eleventh Circuit heard oral arguments on May 11, 2017.[82]

II. Cellular Surveillance and Confidential Sources—The Legal Framework

Law enforcement efforts to conceal stingray technology from courts, legislatures, and the public threatens the integrity of the legal system because much of the law governing their use is largely unsettled. Many controlling legal doctrines and privacy statutes pre-date the modern digital age, and courts and lawmakers are now struggling to apply these legal frameworks to contemporary technologies.[83] This Part provides an overview of existing surveillance law and its general application to stingrays. It then examines the history of the informant's privilege and the legal implications of law enforcement's reliance on the doctrine to withhold information on stingray surveillance from courts and criminal defendants.

A. Electronic Surveillance Generally

Stingrays are difficult to place within the larger framework of constitutional and statutory law because of their diverse set of capabilities.[84] Courts apply differing legal standards to law enforcement's interception of the content of communications, interception of metadata,[85] and tracking of an individual's location.[86] Stingrays pos-

---

80 Initial Brief for Petitioner at 15–16, Am. Civil Liberties Union of Fla. v. City of Sarasota, No. 16-15848 (11th Cir. Oct. 28, 2016).

81 *Id.*; Am. Civil Liberties Union of Fla. v. City of Sarasota, 8:14-cv-1606-T-23TGW, 2015 WL 82250, at *3 (M.D. Fla. Jan. 6, 2015).

82 Am. Civil Liberties Union of Fla., 2015 WL 82250, *appeal docketed*, No. 16-15848 (11th Cir. Sept. 6, 2016).

83 *See generally* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 Ohio St. L.J. 1071, 1072–73 (2013).

84 *See supra* Section I.B (explaining the mechanics and capabilities of stingrays).

85 Metadata is loosely defined as "data about data." *Metadata*, Privacy Int'l, https://www.privacyinternational.org/node/53 [https://perma.cc/7JTK-MCFC] (last visited Mar. 26, 2017). It includes a range of information about a communication, such as the phone numbers and other identifiers of the sender and recipient, the time the communication was transmitted, and the length or size of the communication. *Id.*; *see also* 18 U.S.C. § 3127 (2012) (referencing "dialing, routing, addressing, or signaling information").

86 *See, e.g.*, Wiretap Act, 18 U.S.C. §§ 2510–2522 (2012) (governing content surveillance); Pen Register Statute, 18 U.S.C. §§ 3121–3127 (2012) (governing metadata); Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (declining to extend to constitutional protection to information shared with third party); Katz v. United States, 389 U.S. 347, 357 (1967) (establishing constitu-

sess all three capabilities, however, triggering legal analysis on a case-by-case basis.[87] The following discussion outlines the constitutional and statutory provisions that govern the various forms of stingray surveillance and highlight areas of uncertainty where the devices do not fit well within existing frameworks.

1. Stingrays and the Constitution

The Fourth Amendment prohibits law enforcement from engaging in unreasonable searches and seizures.[88] Once an action is held to be a search under the Fourth Amendment, it is "per se unreasonable" if it is not supported by a warrant or an established exception to the warrant requirement.[89] The modern standard for identifying a search was established by Justice Harlan's concurrence in *Katz v. United States*,[90] in which FBI agents attached an electronic listening device to a public telephone booth in order to eavesdrop on the defendant's conversation.[91] Justice Harlan wrote that a search under the Fourth Amendment occurs when the government violates an individual's "reasonable expectation of privacy," as determined by both actual subjective expectation and an objective measure of society's standards.[92]

The baseline inquiry in analyzing the legal implications of stingrays is, therefore, whether an individual has a reasonable expectation of privacy in the information sought by law enforcement, making the use of the device a search under the Fourth Amendment. The interception of the content of communications with a stingray is readily classified as a search in light of *Katz*, in which the Court held that electronically intercepting even one side of a private conversation violated the speaker's reasonable expectation of privacy.[93] The real-time tracking of an individual's phone signal and the interception of metadata, however, are less easily categorized.

---

tional protections for content not shared with third party). Considerable controversy exists over which provision of law controls the real-time tracking of an individual. *See infra* Section II.A.2.

87 *See infra* Section II.B.

88 U.S. CONST. amend. IV.

89 *Katz*, 389 U.S. at 357.

90 389 U.S. 347 (1967).

91 *Id.* at 348.

92 *Id.* at 360–61 (Harlan, J., concurring).

93 *See id.* at 357 (majority opinion); *see also* Berger v. New York, 388 U.S. 41, 58–60, 64 (1967) (holding warrantless wiretap violated the Fourth Amendment). Congress has also provided additional statutory protections to the content of electronic communications. *See infra* Section II.A.2.

Under the currently accepted "third-party doctrine," no expectation of privacy exists in information that has been shared with a third party, including a telephone company.[94] The doctrine finds its roots in the 1979 case of *Smith v. Maryland*,[95] in which a phone company cooperated with police to install a pen register on the defendant's phone line that recorded the numbers dialed on his phone.[96] The defendant argued that under *Katz*, the Fourth Amendment required police to obtain a warrant prior to installing the device because he had a reasonable expectation that the numbers he dialed would remain private.[97] The Supreme Court disagreed, holding that because the defendant had voluntarily shared the dialed numbers with the phone company in order to route his call, he had forfeited his expectation of privacy in the information.[98] The interception of the information was therefore not a search under the Fourth Amendment, and no warrant was required.[99]

It is thus unlikely under current precedent that the use of a stingray to intercept information shared with a phone company would be considered a Fourth Amendment search, although Congress may have provided alternate protections by statute.[100] Recent developments, however, have cast doubt on the continued vitality of the third-party doctrine.

Several prominent court decisions have recognized a shift in societal expectations coinciding with the advent of the digital age. In *United States v. Warshack*,[101] for example, a defendant challenged his conviction for fraud after his motion to suppress evidence obtained from a warrantless search of his emails was denied prior to trial.[102] The government argued that Warshack possessed no expectation of privacy in the content of his emails because the email service provider reserved the right to access the information, and he had thus shared it

---

94 *See* Marley Degner, Riley *and the Third-Party Doctrine*, WESTLAW J. COMPUT. & INTERNET, Apr. 9, 2015, at *1–3.

95 442 U.S. 735 (1979).

96 *Id.* at 737.

97 *Id.* at 737–38.

98 *Id.* at 744.

99 *Id.* at 745–46.

100 *See infra* Section II.A.2. In addition to the metadata traditionally considered under *Smith*, some courts have held that the extrapolation of location data from cellular signals falls into this category, reasoning that a phone's signal is freely shared with the network's cell tower. *See, e.g.*, United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).

101 631 F.3d 266 (6th Cir. 2010).

102 *Id.* at 281.

with a third party.[103] A unanimous panel of the Sixth Circuit declined to apply the doctrine in this manner, holding that individuals have a reasonable expectation of privacy in their electronic messages because email service providers perform a function analogous to a post office, despite being private commercial actors.[104]

Individuals may similarly not forfeit their privacy interest in signals emanating from a cell phone under this new theory, calling into question the notion that a stingray's interception of location and other metadata is not a Fourth Amendment search. Unlike the forthright presentation of the email search in *Warshack*, however, the secrecy surrounding law enforcement's use of stingrays hampers the ability of courts to directly evaluate the technology.

Some Justices on the Supreme Court have likewise indicated that modern technologies necessitate rethinking classic Fourth Amendment principles. In *United States v. Jones*,[105] for instance, police attached a tracking device to the defendant's vehicle after the authorizing warrant had expired.[106] The Court unanimously held that the warrantless tracking was an unreasonable search under the Fourth Amendment.[107] Although Justice Scalia's majority opinion rested on the premise that the government performed a Fourth Amendment search by physically trespassing against the defendant's private property,[108] both Justice Alito's and Justice Sotomayor's concurring opinions articulated theories that assumed the defendant did not give up his expectation of privacy by driving in public and voluntarily sharing his location with any bystanders who may have seen him.[109] Justice Alito expressly contemplated the effect that cell phone tracking may have in altering societies privacy expectations: "Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users . . . . The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements."[110] Justice Sotomayor attacked the third-party doctrine even more directly, labeling it "ill suited to the digital age, in which people

103 *Id.* at 286.

104 *Id.* at 286–88.

105 132 S. Ct. 945 (2012).

106 *Id.* at 948.

107 *Id.* at 947, 949, 954.

108 *Id.* at 949.

109 *See id.* at 957 (Sotomayor, J., concurring); *id.* at 958 (Alito, J., concurring in the judgment).

110 *Id.* at 963 (Alito, J., concurring in the judgment).

reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[111]

In light of this skepticism, it is unclear whether courts will regard the use of stingrays to capture meta and location data as a search under the Fourth Amendment. However, courts are not afforded the opportunity to address the issue and further develop doctrine when police and prosecutors hide that they have utilized the devices in investigations.

2. The Statutory Overlay

Even in the absence of constitutional protections, Congress has passed an array of legislation governing electronic searches and seizures. The strongest of these protections is contained in the Wiretap Act, which establishes procedures for law enforcement's interception of the content of "wire, oral, or electronic communications."[112] In addition to requiring law enforcement to obtain authorization from particular, highly-ranked officials to seek a warrant, the law restricts the tactic to the investigation of only certain serious felonies.[113] Police must also demonstrate that the interception is reasonably necessary because other investigatory techniques would be ineffective or dangerous.[114]

Because Congress framed the law with reference to the type of data sought rather than the means of interception, stingrays are encompassed by the statute when they are used to capture the actual contents of an electronic communication.[115] The government therefore must obtain a warrant under the heightened standards of the Wiretap Act when they seek to deploy a stingray for content surveillance.[116]

The statutory standard for the interception of metadata is less well-established. The Pen Register Statute generally governs the collection of such information.[117] The law defines a pen register as "a device or process which records or decodes dialing, routing, addressing, or signaling information."[118] The corollary for incoming transmis-

---

111 *Id.* at 957 (Sotomayor, J., concurring).

112 18 U.S.C. §§ 2516–2518 (2012). *See generally* GINA STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., 98-326, PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING (2012), https://fas.org/sgp/crs/intel/98-326.pdf.

113 *Id.* § 2516(1)–(2).

114 *Id.* § 2518(3)(c).

115 *See* Hosein & Palow, *supra* note 83, at 1097.

116 *See id.*

117 Pen Register Statute, 18 U.S.C. §§ 3121–3127 (2012).

118 *Id.* § 3127(3).

sions is a "trap and trace device."[119] Authorization for the use of both technologies may be granted by a court order that does not require probable cause, but only a showing that "the information likely to be obtained is relevant to an ongoing criminal investigation."[120]

The Pen Register Statute does require, however, that the order granting the authorization include "*the number or other identifier* and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device *is to be attached or applied*."[121] When employing a stingray to intercept metadata, police do not attach or apply the device to any physical phone line or facility, as contemplated by the statute.[122] And in some instances, police have sought to use stingrays to identify the number or other identifier of a suspect's phone in the first place, making it impossible to include this information beforehand in the order authorizing the use of the device.[123] At least one court has ruled that these discrepancies are sufficient to remove stingrays from the purview of the Pen Register Statute.[124] In doing so, the judge expressed concern that the order being sought "would not insure sufficient accountability" as determined by Congress and embodied in a periodic reporting requirement contained within the Pen Register Statute.[125] It would therefore be the duty of Congress to amend the law to address this evolving technology. Federal and state legislatures cannot respond to these developments, however, when law enforcement hides the fact that the development has taken place. Indeed, Congress has amended the Pen Register Statute multiple times during the period in which law enforcement has covertly employed stingrays without clarifying these ambiguities.[126]

The statutory standard for real-time location tracking is the most controversial and unsettled of the stingray's many capabilities. There

---

119 *Id.* § 3127(4).

120 *Id.* § 3122(b)(2).

121 *Id.* § 3123(b)(1)(C) (emphasis added).

122 *See supra* Section I.B (describing stingray mechanics).

123 *See, e.g.*, *2012 South Texas Order*, *supra* note 53, at 748 (seeking to identify phone number and serial number of suspects phones); *1995 Digital Analyzer Order*, *supra* note 27, at 199 (seeking to identify phone numbers of five named suspects).

124 *See 1995 Digital Analyzer Order*, *supra* note 27, at 199–200; *infra* Section II.B.

125 *See 1995 Digital Analyzer Order*, *supra* note 27, at 201–02 (referencing 18 U.S.C. § 3126).

126 *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, § 207, 108 Stat 4279, 4292 (1994); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107–56, § 216, 115 Stat. 272, 288–90.

is no single federal statute that clearly governs the use of the devices for active, ongoing tracking.[127] Law enforcement contends that they may obtain such information under a hybrid authority that relies on the intersection of the Pen Register Statute with the Stored Communications Act.[128] They argue that cell phone tracking utilizes "signaling information" as contemplated by the Pen Register Statute.[129] The isolated use of the Pen Register Statute for this purpose is foreclosed, however, by a clarification contained elsewhere in federal law: "[W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . such call-identifying information shall not include any information that may disclose the physical location of the subscriber . . . ."[130]

To overcome this obstacle, the government relies on the word "solely" within the prohibition, which they argue permits the interception of location information when taken in conjunction with other statutory authority.[131] They find this alternate authority in the Stored Communications Act, which permits a court to order a communication provider to disclose historic, non-content "record[s] or other information pertaining to a subscriber to or customer of such service."[132] Law enforcement contends that this provision encompasses "all non-content information pertaining to a customer or subscriber," including cellular location data.[133] The two statutes in conjunction should therefore permit real time tracking, they argue.[134]

Courts have split on whether to accept this hybrid theory when law enforcement works directly with a phone company and utilizes the carrier's own cellular towers.[135] The theory becomes substantially

---

127 Timothy Stapleton, Note, *The Electronic Communications Privacy Act and Cell Location Data: Is the Whole More Than the Sum of Its Parts?*, 73 BROOK. L. REV. 383, 384 (2007).

128 Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012); *see id.* § 2703; *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 761 (S.D. Tex. 2005) [hereinafter *2005 South Texas Order*]; H. MARSHALL JARRETT ET AL., U.S. DEP'T OF JUSTICE, COMPUT. CRIME AND INTELLECTUAL PROP. SECTION, CRIMINAL DIV., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 159–61 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf; Stapleton, *supra* note 127, at 384–85.

129 *2005 South Texas Order*, *supra* note 128, at 761 (referencing 18 U.S.C. § 3127(4) (2012)).

130 47 U.S.C. § 1002(a)(2) (2012).

131 *See 2005 South Texas Order*, *supra* note 123, at 761; H. MARSHALL JARRET ET AL., *supra* note 128, at 160.

132 18 U.S.C. § 2703(c)(1); H. MARSHALL JARRET ET AL., *supra* note 128, at 160 (citing the Stored Communications Act, as codified in 2006).

133 H. MARSHALL JARRET ET AL., *supra* note 128, at 160.

134 *Id.*

135 *Id. Compare In re* Application of the United States for an Order Authorizing the Use of

more problematic, however, when applied to stingrays. In these instances, the phone company does not turn over any record or other non-content information to the police. Indeed, law enforcement can intercept the signal without the phone company's involvement, belying the application of the Stored Communication Act.[136] Courts are unable to evaluate this crucial difference, however, when law enforcement withholds all information about the devices during an application for an order and the subsequent trial.

Courts that reject hybrid theory often present an alternate argument based on statute.[137] The Electronic Communications Privacy Act ("ECPA")[138] contains a provision clarifying that warrants issued for "the installation of a mobile tracking device" may authorize monitoring across jurisdictional lines.[139] The statute defines the term as "an electronic or mechanical device which *permits* the tracking of the movement of a person or object."[140] As one magistrate judge observed, the law does not require that the device be "intended or designed to track movement; it is enough if the device merely 'permits' tracking."[141] Thus, he reasoned, a cell phone can be classified as a tracking device, and the appropriate standard for utilizing it as such is probable cause.[142]

This reading of the statute is as inexact as the government's hybrid theory. ECPA clarifies the scope of a court's authority to grant a warrant for the installation of a tracking device, but it does not expressly require one.[143] Indeed, as the magistrate judge observed,

---

Two Pen Register & Trap & Trace Devices, 632 F. Supp. 2d 202, 204–05 (E.D.N.Y. 2008) (authorizing hybrid orders for cell-site information), *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d. 448, 457, 462 (S.D.N.Y. 2006) (same), *and In re* Application of the United States Authorizing the Installation & Use of a Pen Register & Trap & Trace Device & Authorizing Release of Subscriber and Other Info., 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006) (same), *with In re* Application of the United States for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. [Sealed] & [Sealed], 416 F. Supp. 2d 390, 396–97 (D. Md. 2006) (rejecting hybrid orders), *In re* Application of the United States for an Order Authorizing the Use of a Pen Register & a Trap & Trace Device & Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294, 327 (E.D.N.Y. 2005) (same), *and 2005 South Texas Order*, *supra* note 128 at 761 (same).

136 *See supra* Section I.B.

137 *See 2005 South Texas Order*, *supra* note 128, at 763.

138 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

139 18 U.S.C. § 3117.

140 *Id.* § 3117(b) (emphasis added).

141 *2005 South Texas Order*, *supra* note 128, at 753.

142 *See id.* at 765.

143 *See* 18 U.S.C. § 3117; United States v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000)

"ECPA was not intended to affect the legal standard for the issuance of orders authorizing these devices."[144] It is also not clear that the conversion of a cell phone into a tracking device amounts to an "installation" within the meaning of the law.[145] This uncertainty, however, underscores the importance of transparency and disclosure of stingrays with respect to courts and legislatures. Only with a forthright presentation of the issues involved will courts be able to decide among these competing legal theories, and only with access to relevant information will legislatures be capable of amending and clarifying this confusing statutory framework.

B. Stingray Court Decisions—A Mixed Bag

Law enforcement efforts to keep the existence of cell site simulation secret have included a concerted effort to shield the devices from judicial review.[146] Consequently, courts have had relatively little opportunity to evaluate the legality of the technology. Those few decisions have rendered mixed results.

The earliest known ruling on the devices occurred in the Central District of California in 1995.[147] Unable to identify the particular cell phones of five suspects in a narcotics investigation, the government applied for a court order to employ an early form of stingray, referred to in court documents as a "digital analyzer," to capture the phones' unique identifiers when surveilling officers observed the individuals making or receiving a call.[148] The government sought the order under the Pen Register Statute, but maintained that such an order was unnecessary and that they were doing so only out of "an abundance of caution."[149] The court reluctantly agreed, finding that applicable precedent did not require a warrant for information shared with a phone company and that the use of the digital analyzer did not fit the parameters of the Pen Register Statute.[150]

("[S]ection 3117 provides a basis for authorizing the use of a mobile tracking device. But by contrast to statutes governing other kinds of electronic surveillance devices, section 3117 does not prohibit the use of a tracking device in the absence of conformity with the section.").

144 *2005 South Texas Order*, *supra* note 128, at 751.

145 *See id.* at 756 ("Under the government's theory, law enforcement could simply install cell phones in place of the beepers currently underneath vehicles and inside drum barrels, and eliminate forever the need to obtain a Rule 41 search warrant for tracking surveillance.").

146 *See* Owsley, *supra* note 20, at 200; *supra* Section I.C.

147 *See 1995 Digital Analyzer Order*, *supra* note 27, at 199; *see also* Owsley, *supra* note 20, at 201–10 (detailing known court decisions concerning cell site simulators).

148 *See 1995 Digital Analyzer Order*, *supra* note 27, at 199–200.

149 *See id.* at 200.

150 *See id.*; *see also supra* Section II.A.2.

Since that initial decision, courts have failed to arrive at a single standard for the deployment of stingrays. Some courts have similarly concluded that stingrays simply do not fit neatly within the purview of the Pen Register Statute, particularly when the government does not know the phone number of the target as generally required in the application for the court order.[151] Instead, these courts have often required a warrant issued on probable cause.[152] Others have granted the pen register application, but only subject to judicially imposed restrictions. In 2012, for example, a magistrate judge in the Northern District of Texas reportedly granted the government's pen register application to deploy a stingray in a narcotics investigation with the additional requirement that the device not be used at any time that the suspect was "in a location in which he would have a reasonable expectation of privacy; including but not limited to: a private residence, a vehicle, or a private office."[153] Still other courts have readily granted the pen register requests, reasoning that individuals have no privacy expectation in information they share with their phone company, just as the California court did in 1995.[154]

Most recently, the Maryland Court of Special Appeals held that the Baltimore Police Department's use of a stingray to track an individual was a search within the Fourth Amendment.[155] Like the concurring Justices in *United States v. Jones*, the court reasoned that society's reasonable expectations of privacy have shifted in the modern age,

---

151 *See* 18 U.S.C. § 3123(b)(1)(C) (2012).

152 *See, e.g.*, United States v. Espudo, 954 F. Supp. 2d 1029, 1043 (S.D. Cal. 2013) (holding that a warrant is required to use a stingray for real-time tracking of defendant); *2012 South Texas Order*, *supra* note 53 at 751–52 (denying application for pen register order when the government intended to use stingray to gain information on narcotics trafficker's phone on the ground that a warrant was required).

153 Owsley, *supra* note 20, at 206 (quoting *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device (N.D. Tex. Apr. 5, 2012)). Other courts have employed similar approaches. *See id.* at 207–08 (asserting that in *In re* Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device for the Cellular Tel. Facility Currently Assigned Tel. No. [Redacted], Mag. No. 12-3016, at 4 (D.N.J. Feb. 21, 2012), the application was granted to use device only to identify the general area in which a cell phone was located but not to track it within a private space). Though these orders, and thus the courts' reasoning, currently remain under seal, this approach is consistent with conventional conceptions of the third-party doctrine and electronic surveillance. A suspect's activities in a private area would not be shared with the public, and thus a Fourth Amendment search would occur when police use technology to ascertain otherwise unknowable details about the space. *See supra* Section II.A.1; *infra* notes 243–57 and accompanying text.

154 *See* Owsley, *supra* note 20, at 210 (describing email from magistrate judge in Southern District of California who states that he and his colleagues "routinely grant" the requests).

155 *See* State v. Andrews, 134 A.3d 324, 327 (Md. Ct. Spec. App. 2016).

and no person reasonably expects that the signal from their phone is pubic information.[156] Because the use of the stingray violated this new expectation of privacy, the court held that it presumptively requires a warrant supported by probable cause under the *Katz* standard.[157]

Notably, the Maryland court expressed open disapproval of the nondisclosure agreement between the police department and the FBI, stating that "such an extensive prohibition on disclosure of information to the court—from special order and/or warrant application through appellate review—prevents the court from exercising its fundamental duties under the Constitution."[158] It is the constitutional duty of the courts to evaluate whether an "invasion of a citizen's personal security" is reasonable in light of all circumstances, the court stated, and this requires courts to understand why and how surveillance is conducted, including through the "analysis of the functionality of the surveillance device and the range of information potentially revealed by its use."[159] A nondisclosure agreement that prevents police departments from revealing the information necessary for this determination therefore obstructs courts from fulfilling their core constitutional prerogative.[160] Given this unequivocal condemnation, it is worth examining law enforcement's rationale for the nondisclosure agreements within the larger legal context of confidential sources.

C. The Law of Confidential Sources and Technology

The doctrine of confidential sources has its roots in the common law informant's privilege.[161] As early as 1790, an English judge held that "defendant's counsel have no right, nor shall they be permitted, to inquire the name of the person who gave the information" that led to arrests for smuggling.[162] In the United States, the privilege was similarly recognized in an early criminal prosecution for counterfeiting.[163]

---

156 *See id.* at 348–49.

157 *Id.* at 327.

158 *Id.* at 338.

159 *Id.* (quoting Terry v. Ohio, 392 U.S. 1, 19 (1968) in the first quotation).

160 *Id.* at 339.

161 *See Institutional Privileges*, 98 HARV. L. REV. 1592, 1596–97 (1985).

162 Worthington v. Scribner, 109 Mass. 487, 489 (1872) (quoting Rex v. Akers (1790) 6 Esp. 125, 170 Eng. Rep. 850 (NP)).

163 *See* United States v. Moses, 27 F. Cas. 5, 5 (C.C.E.D. Pa. 1827) ("[T]he officer who apprehended the prisoner is not bound to disclose the name of the person from whom he received the information, which led to the detection and apprehension of the prisoner."); *see also Worthington*, 109 Mass. at 490 (providing a survey of cases involving the privilege in American and English courts).

Until the mid-twentieth century, courts generally regarded the informant's privilege "as an absolute barrier against the disclosure of an informant's identity" with little regard for a defendant's constitutional rights.[164] This changed in 1957, when the Supreme Court articulated the modern standard for confidential sources in *Roviaro v. United States*,[165] providing that a defendant is entitled to the identity of an informant and the contents of his communication when it is either relevant and useful to the defense or the secrecy does not serve the underlying purpose of the privilege.[166] In *Roviaro*, the defendant was charged with selling heroin to a confidential informant referred to in case filings as John Doe.[167] When confronted with the defendant at the police station, though, John Doe denied having ever before met or seen him.[168] Prior to trial, the defendant moved to obtain John Doe's name, address, and occupation, and the government objected, claiming the informant's privilege.[169] The motion was denied.[170] The defendant's counsel then repeatedly sought to learn John Doe's identity through cross-examination of government witnesses, which the court declined to allow.[171] Roviaro was convicted, and the court of appeals affirmed.[172]

The Supreme Court reversed, and in doing so placed two key limitations on the informant's privilege. First, the Court held that "[t]he scope of the privilege is limited by its underlying purpose"—namely, "the furtherance and protection of the public interest in effective law enforcement" through the encouragement of "citizens to communicate their knowledge of the commission of crimes to law-enforcement officials."[173] "Thus, where the disclosure of the contents of a communication will not tend to reveal the identity of an informer, the contents are not privileged" and "once the identity of the informer has been disclosed . . . the privilege is no longer applicable."[174] Second, the Court held that even when the privilege would otherwise be applica-

164 *Institutional Privileges*, *supra* note 161, at 1597; *cf.* Scher v. United States, 305 U.S. 251, 254 (1938) ("[P]ublic policy forbids disclosure of an informer's identity *unless essential to the defense*, as, for example, where this turns upon an officer's good faith.") (emphasis added).

165 353 U.S. 53 (1957).

166 *Id.* at 59–60.

167 *Id.* at 55.

168 *Id.* at 58.

169 *Id.* at 55.

170 *Id.*

171 *Id.*

172 *Id.* at 55–56.

173 *Id.* at 59–60.

174 *Id.* at 60.

ble, the Due Process requirement of fundamental fairness requires that it "give way" when "the disclosure of an informer's identity, or of the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause."[175] Because John Doe was the only witness to the transaction and could have rebutted the government's claims or established entrapment, Roviaro was entitled to the individual's identity.[176]

The Court in *Roviaro* expressly declined to adopt a fixed rule for determining when the informant's privilege applies, instead calling for a case-by-case balancing test that pits "the public interest in protecting the flow of information against the individual's right to prepare his defense."[177] Subsequent lower court opinions have fleshed out the doctrine. Generally, when an informant participates in a crime or is otherwise a direct witness, a defendant is entitled to the individual's identity.[178] When the informant has no material connection to the crime, however, and simply provided a tip, the government may withhold identification.[179]

Roviaro establishes the basic legal principles under which the use of stingrays as a confidential source should be evaluated. First, the policy rationales that underlie the informant's privilege limit its scope, which indicates that the analysis turns in part on the degree to which keeping stingrays secret serves the traditional purposes of the informant's privilege.[180] Second, the privilege must give way to a defendant's right to prepare a defense, making the legal implications of the potential illegal search in each individual case relevant to the evaluation.[181]

---

175 *Id.* at 60–61.

176 *Id.* at 64–65.

177 *Id.* at 62.

178 *See, e.g.*, United States v. Silva, 580 F.2d 144, 147 (5th Cir. 1978) (requiring disclosure of identity of confidential informant where defense was mistaken identity and informant was only witness able to corroborate testimony of undercover agent who participated in the transaction); United States v. Martinez, 487 F.2d 973, 976–77 (10th Cir. 1973) (requiring disclosure of informant who was present at time of alleged drug sale); United States v. Barnett, 418 F.2d 309, 311–12 (6th Cir. 1969) (requiring disclosure of informant who was participant in crime).

179 *See, e.g.*, United States v. Halbert, 668 F.2d 489, 495–96 (10th Cir. 1982) (denying disclosure where informant relayed rumor of defendant's involvement in the crime to police); United States v. House, 604 F.2d 1135, 1140 (8th Cir. 1979) (denying disclosure where informant notified police that defendant was a drug dealer and kept drugs in his home); Bourbois v. United States, 530 F.2d 3, 3 (5th Cir. 1979) (per curiam) (denying disclosure of tipster's identity).

180 *See Roviaro*, 353 U.S. at 60.

181 *See id.* at 60–61.

1. Policy Analysis

To the first point, it is useful to identify the underlying reasons for the informant's privilege and evaluate the degree to which each is served by two possible conceptions of its application to stingrays: either the stingray itself is the informant whose identity the government seeks to shield, or the state actor who operates the device is the true confidential source.

Historically, the informant's privilege centered on the proposition that it is the duty of citizens to pass on information to law enforcement and that citizens should not be subject to physical or legal retaliation for performing that duty.[182] Inanimate objects like stingrays do not have any duties within the general understanding of the word. Their purpose is determined by designers, and the notion of rewarding or punishing such a device for carrying out that purpose borders on nonsensical. The operator of the stingray, on the other hand, may be said to have a duty arising from her public employment to investigate violations of the law and pass on material information.[183] This duty may shield her from personal liability as is embodied in the doctrine of qualified immunity.[184] There are limits to this application, however. The Supreme Court has endorsed an exclusionary remedy that makes evidence inadmissible at trial when it is obtained through law enforcement misconduct, including illegal searches and coerced confessions.[185] The existence of these remedies makes clear that duty alone cannot protect the government from all negative legal repercussions when the law is violated.

An alternate historic formulation rooted the privilege in the personal liberty of the informant, who the Supreme Court held possessed a fundamental constitutional right to pass information about criminal offenses to law enforcement.[186] As a threshold matter, modern courts have rejected this justification, holding that the privilege centers on the government's right and not that of the informant.[187] It is in any

182 *See* Vogel v. Gruaz, 110 U.S. 311, 316 (1884).

183 *See, e.g.*, Manganiello v. City of New York, 612 F.3d 149, 160 (2d Cir. 2010) (holding it unlawful for a police officer to fail to pass on material information to a prosecutor).

184 *See generally* Mark R. Brown, *The Fall and Rise of Qualified Immunity: From* Hope *to* Harris, 9 Nev. L.J. 185, 185–86 (2008) (outlining development and principles of the doctrine which protects state actors from liability for reasonable mistakes of law).

185 *See, e.g.*, Mapp v. Ohio, 367 U.S. 643, 654 (1961) (illegal searches); Rogers v. Richmond, 365 U.S. 534, 548–49 (1961) (coerced confessions).

186 *See In re* Quarles, 158 U.S. 532, 535 (1895).

187 *See* Roviaro v. United States, 353 U.S. 53, 59 (1957) ("What is usually referred to as the informer's privilege is in reality the Government's privilege . . . .").

event easily dispensed with in the context of stingrays. Just as with duties, inanimate objects cannot generally be said to have personal liberties under our legal system, and any protections they receive come by virtue of the owner's rights. A law enforcement officer, on the other hand, may have a right to pass on evidence or information relevant to an offense within the investigating agency and to the prosecution.[188] Police cannot simply claim this liberty to vindicate ill-gotten evidence, however, or the sanctions embodied in the exclusionary remedy could be avoided by simply passing the evidence from an officer who acts in bad faith to an officer uninvolved in the misconduct.

Roviaro presented a final possible justification: "The purpose of the privilege is the furtherance and protection of the public interest in effective law enforcement."[189] Underlying this logic is the assumption that an informant will be reluctant to inform on a suspect if she believes that she may be subject to reprisal.[190] This does not hold true, however, when applied to a stingray or to its operator. An inanimate device cannot be intimidated into withholding information. A police officer, on the other hand, has substantial protection against retaliation by virtue of her position, and moreover would be derelict in her duty if she allowed herself to be intimidated into not performing her assigned tasks. Furthermore, the personal identity of the specific agent operating the device is irrelevant to courts. It is the operation of the device itself that may constitute an illegal search, and this technical information would not expose the operator to any risk of retaliation.

A proponent of the continued secrecy might respond by echoing the FBI Chief's proffered justification—that disclosure of cell site simulation technology will allow criminals to circumvent it—and go on to reason that the diminishment of available information that would result makes the scenario comparable to an informant who is intimidated into silence. This connection is far more speculative and attenuated than the risks typically considered in a confidential informant analysis, however, and our legal system generally gives short shrift to "conjectural" or "hypothetical" harms that may occur at some indeterminate future time.[191] In the context of standing, for instance, the Supreme Court has consistently held that an injury must "clearly and

188 *See, e.g.*, United States v. Herberg, 15 C.M.A. 247, 251 (C.M.A. 1965) ("It is well settled that a valid arrest may be made by a police officer, for a reported crime not committed in his presence, solely on the strength of information passed on to him by other police officers . . . .").

189 *Roviaro*, 353 U.S. at 59.

190 *See id.* at 67.

191 Whitmore v. Arkansas, 495 U.S. 149, 155 (1990) (quoting Los Angeles v. Lyons, 461 U.S. 95, 101–02 (1983)).

specifically set forth facts" that establish that an injury is "actual or imminent."[192] "[U]nspecified, speculative threats of uncertain harm that might occur at some indefinite time in the future"[193] will not suffice, particularly when that harm would arise from "the independent action of some third party not before the court."[194]

The threat of violence to a specific source of identifiable information in a particular investigation is more concrete than the risk that the general criminal element may learn of an investigatory technique over time and that some criminals may take steps to counteract it in unrelated future criminal endeavors. The former threat is linked to a discrete source—a particular criminal defendant and her compatriots—and is associated with an individualized target—the confidential human informant. Neither is true of the risk that disclosure of investigative technology may someday lead to criminal circumvention. The government's interest in secrecy is thus greatly diminished when weighed against defendants' rights and the integrity of the justice system, which are directly and immediately undermined when law enforcement withholds pertinent information and misleads the court.

2. Legal Implications in Individual Cases

Because the Court in *Roviaro* held that the informant's privilege must "give way" when the identity of the informant is "relevant and helpful to the defense of an accused,"[195] it is necessary to evaluate the legal implications of a potentially illegal stingray search for the defense in individual cases. Under the framework established by lower court rulings in the wake of *Roviaro*, a defendant is entitled to the identity of an informant when the individual directly witnessed or participated in the crime, but the government is allowed to withhold such identification when an uninvolved party simply acts as a "tipster."[196] On first blush, this may seem to favor the application of the doctrine to stingrays and the agents that operate them because the actors are unlikely to be participants in a crime and the information gained may be collateral to the purpose of the investigation. However, this analysis neglects the underlying legal basis for the distinction. When an independent human informant provides details such as the suspect's location, for example, the tipster's identity is not relevant to the prep-

192 *Id.*; *accord* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

193 Gilligan v. Morgan, 413 U.S. 1, 14 (1973).

194 Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 42 (1976).

195 *Roviaro*, 353 U.S. at 60–61.

196 *See Institutional Privileges*, *supra* note 161, at 1598.

aration of a defense.[197] When the confidential source, however, is a technology-assisted state actor who may have engaged in a search that violated the Fourth Amendment, the fact and method of the search become highly relevant to the defense because it can lead to potential suppression of evidence.[198]

Case law to date overlooks this key distinction. A sharply divided Supreme Court held in *McCray v. Illinois*[199] that a defendant is not entitled to the identity of a confidential informant when attempting to suppress evidence as resulting from an illegal search.[200] In *McCray*, police arrested the defendant for selling heroin on the basis of a reliable confidential informant pointing the defendant out and informing authorities that he was a drug dealer.[201] The defendant moved to suppress the drugs found on his person, claiming that the search and subsequent arrest were unreasonable under the Fourth Amendment.[202] The majority held that *Roviaro* was distinguishable because the events in *Roviaro* took place "not at a preliminary hearing to determine probable cause for an arrest or search, but at the trial itself where the issue was the fundamental one of innocence or guilt."[203] In this context, the Court viewed the sworn testimony of the police officers as sufficient: "Nothing in the Due Process Clause of the Fourteenth Amendment requires a state court judge in every such hearing to assume the arresting officers are committing perjury."[204]

The dissenters pointed out the fatal flaw in this reasoning. Given the two limiting principles established in *Roviaro*, the informant's identity should have been disclosed.[205] It was relevant and helpful to the defense, for "[o]nly by requiring disclosure and giving the defendant an opportunity to present contrary or impeaching evidence as to the truth of the officer's testimony and the reasonableness of his reliance on the informer can the court make a fair determination of the issue."[206] Moreover, preserving the confidentiality did not advance the

197 *See, e.g.*, United States v. House, 604 F.2d 1135, 1140 (8th Cir. 1979) (holding tipster's identity not material to preparation of defense).

198 *See, e.g.*, State v. Andrews, 134 A.3d 324, 364–65 (Md. Ct. Spec. App. 2016) (suppressing evidence obtained through the warrantless use of a stingray as fruits of an illegal search).

199 386 U.S. 300 (1967).

200 *See id.* at 312–14.

201 *See id.* at 301–03.

202 *See id.* at 301.

203 *Id.* at 309.

204 *Id.* at 313.

205 *See id.* at 315–16 (Douglas, J., dissenting).

206 *Id.* at 316 (quoting Priestly v. Superior Court, 330 P.2d 39, 43 (Cal. 1958)).

purpose of the privilege, for "[s]uch a requirement does not unreasonably discourage the free flow of information to law enforcement officers or otherwise impede law enforcement."[207] In light of the campaign of secrecy surrounding law enforcement's use of stingrays, the dissenters have been proven prescient in expressing concern that the ruling entrusted the Fourth Amendment "to the tender mercies of the police."[208]

McCray garnered considerable contemporary criticism, including that it would "almost guarantee[ ] wholesale police perjury" because every illegal search thereafter could be retroactively justified by a claim that "an unnamed 'reliable informant' told [police] that the defendant was committing a crime."[209] This fear is if anything understated—when the informant's privilege is extended to an entire class of investigatory techniques, *McCray* potentially permits not only individual wrongdoing on the part of police, but systematic circumvention of the law at the institutional level.

3. The Surveillance Location Privilege

Some lower courts have applied *Roviaro* and *McCray* to specific aspects of surveillance techniques to protect the techniques' continued utility. In *United States v. Harley*,[210] for example, the D.C. Circuit held that the location from which police took surveillance video of a drug sale was privileged.[211] The defendant was convicted after he was covertly videotaped while selling drugs to an undercover agent.[212] On appeal, he argued that the court had erred in preventing him from questioning the witness about the exact location of the apartment from which the police shot the video.[213] The court held that the information was analogous to the identity of an informant under *Roviaro*.[214] The court compared the loss of the use of the surveillance location and the threat to the cooperating apartment owner to the intimidation and harm that may come to a confidential informant whose identity is revealed in court.[215] Terming this formulation "the surveillance location privilege," the court advanced a balancing test

207 *Id.* (quoting *Priestly*, 330 P.2d at 43).

208 *Id.*

209 Irving Younger, *The Perjury Routine*, NATION, 578, 597 (1967).

210 682 F.2d 1018 (D.C. Cir. 1982).

211 *Id.* at 1020.

212 *Id.* at 1019–20.

213 *Id.* at 1020.

214 *Id.* (citing United States v. Green, 670 F.2d 1148, 1155 (D.C. Cir. 1981)).

215 *Id.*

similar to *Roviaro* in which the need of the defense is measured against the rights of law enforcement.[216] Because the defendant had not attempted to demonstrate a need for the information that could not be adequately satisfied by alternate methods, the court had no trouble sustaining the privilege in *Harley*.[217]

The surveillance location privilege articulated in *Harley* is readily distinguishable from law enforcement's assertion of the informant's privilege to withhold their use of stingrays in an investigation. In *Harley*, the government sought to withhold specific, collateral information about the manner in which they employed surveillance.[218] It was forthcoming about the fact that the surveillance itself took place,[219] which cannot be said of police that attempt to disguise their use of stingrays by attributing it to a confidential source. Further, the legality of the surveillance technique as a whole was not in question as it is with the use of stingrays.[220]

Relying on *Harley*, the Eleventh Circuit extended the surveillance location privilege to the type and placement of a microphone in *United States v. Van Horn*.[221] Police used a hidden microphone placed in one of the defendant's offices pursuant to a warrant obtained under the Wiretap Act.[222] At trial, the defense attempted to learn the location and the type of microphone used in order to impeach the fidelity of the recording, arguing that the placement may have resulted in distortion.[223] The government objected, leading the district court to conduct an in camera review of the government's claim of privilege.[224] The privilege was ultimately sustained, and the defendants were convicted.[225] The Eleventh Circuit affirmed, holding that the *Harley* balancing test weighed in favor of keeping the information secret.[226]

Van Horn also does not support the extension of the informant's privilege to stingrays and their operators. Like in *Harley*, the government in *Van Horn* sought only to withhold collateral details about its use of surveillance and not the fact of the surveillance itself.[227] Indeed,

---

216 *Id.* (citing *Green*, 670 F.2d at 1155–56).

217 *See id.*

218 *Id.* at 1020–21.

219 *See id.* at 1021.

220 *See supra* Sections II.A–B.

221 789 F.2d 1492, 1508 (11th Cir. 1986).

222 *Id.* at 1496.

223 *Id.* at 1507–08.

224 *Id.* at 1508.

225 *Id.*

226 *Id.* at 1508, 1511.

227 *See Van Horn*, 789 F.2d at 1508; *Harley*, 682 F.2d at 1020–21.

the fact of the surveillance was not only disclosed, but actually preapproved by the neutral magistrate who issued the warrant under the heightened standards of the Wiretap Act.[228] And, in making the determination as to the validity of the privilege, the court conducted an in camera review, ensuring that the surveillance was not conducted improperly.[229] Neither of these neutral evaluations are present when police claim that information generated from the use of a stingray originates from a confidential tipster, leaving the ultimate judgement that the surveillance is lawful to the unfettered discretion of police.

An Arizona district court had occasion to examine stingrays within the context of the surveillance location privilege in *United States v. Rigmaiden*.[230] In *Rigmaiden*, police tracked an "aircard" in the defendant's laptop that allowed him to access the Internet using a cellphone network.[231] Potentially in anticipation of a legal battle, the government first obtained a tracking warrant authorizing the use of the stingray to locate the fraud suspect.[232] Prior to trial, the defendant requested discovery of the identity of the agents operating the stingray and detailed information about the device, arguing that it was relevant to establishing whether the agents violated his Fourth Amendment rights.[233] For purposes of the suppression hearing, the government conceded that the tracking was a Fourth Amendment search and that the warrant was the sole authority justifying the search.[234] The court also held an ex parte hearing in which the agent "explained how the equipment used in locating the aircard operates, how it was used in this particular case, and why disclosure of information regarding the equipment and techniques used to locate the aircard would hamper future law enforcement efforts."[235] Finding that the defendant's justifications of need were rendered moot by the government's concessions regarding the search and warrant, the court sustained the government's claim of privilege.[236]

Notwithstanding the court's extension of the surveillance location privilege to a stingray in the particular instance, *Rigmaiden* should not be read to justify the blanket withholding of information on the de-

228 *Van Horn*, 789 F.2d at 1496.

229 *Id.* at 1508.

230 844 F. Supp. 2d 982, 987 (D. Ariz. 2012).

231 *Id.*

232 *See id.* at 996.

233 *Id.* at 987.

234 *Id.* at 995–96.

235 *Id.* at 994.

236 *Id.* at 997–98, 1000–02.

vices as relating to confidential sources. As in *Van Horn*, the government obtained a warrant for the use of the stingray prior to its use, ensuring that a neutral magistrate was able to evaluate its legality under the appropriate legal standard.[237] And far from hiding the device from the court, the government disclosed detailed information about the device and its use in the investigation to the court in an ex parte hearing.[238] As in *Harley* and *Van Horn*, the factors present in *Rigmaiden* ensured neutral judicial review of the surveillance, which is not possible when the government does not disclose that the device was used in an investigation.

III. Compelling Disclosure of Obscure Technologies—A Proposed Solution

Having examined the ways in which the secrecy surrounding stingrays undermines the integrity of the American legal system and concluded that the confidentiality is not justified by the informant's privilege, we now turn to closing the gap in current law that allowed stingrays to remain hidden for nearly three decades. Even were courts to hold that prosecutorial withholding of information about the devices in criminal cases is unlawful, existing legal tools offer no easy solution for halting the practice and preventing similar infractions in the future.[239] It is therefore necessary to draw on past precedent to formulate a constitutionally-based prophylactic rule that ensures courts and legislatures can evaluate stingrays and other novel technologies as they emerge. Courts should mandate that prosecutors disclose to criminal defendants when technology that is not available to the general public is used in the course of an investigation. This basic requirement would strike the proper balance between national security, the needs of the justice system, and the rights of defendants. Further, the elements of the rule's construction are well established in current case law.

A. Kyllo *and* Brady*—The Building Blocks of an Answer*

The Supreme Court has already given legal significance to law enforcement's use of technology not commonly utilized by the general public,[240] and the Court has likewise imposed prosecutorial disclosure

237 *Id.* at 996; *see also* United States v. Van Horn, 789 F.2d 1492, 1496 (11th Cir. 1986).

238 *Rigmaiden*, 844 F. Supp. 2d at 994.

239 *But see infra* Section III.B.2.

240 *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

requirements in the interest of protecting constitutional rights.[241] By combining these two precedents, courts may fashion a rule that prevents law enforcement from shielding stingrays and other new investigative technologies from judicial and legislative review.

The Maryland Court of Special Appeals explicitly cited the first element of this solution in its recent opinion holding that the use of a stingray to track an individual constitutes a search under the Fourth Amendment.[242] The court looked to the manner in which the Supreme Court had previously addressed obscure technologies for guidance on evaluating stingrays, focusing particular attention on *Kyllo v. United States*.[243] In *Kyllo*, a federal agent employed a thermal imaging device to scan the outside of the home of a man suspected of growing marijuana.[244] The agent observed that several walls were emitting more heat than expected and reasoned that the heat was likely a result of the high intensity lamps typically used to grow marijuana indoors.[245] The agent used the heat signatures, along with the suspect's utility bills and tips from informants, to obtain a warrant authorizing the search of the house.[246] Upon raiding the home, law enforcement discovered an indoor grow operation with over 100 marijuana plants.[247] At trial, the defendant entered a conditional guilty plea after he unsuccessfully moved to suppress the evidence, arguing that the warrantless use of the thermal imaging device was an unconstitutional search under the Fourth Amendment.[248]

The government argued on appeal that the use of the device was not a search because, much like the signal emanating from a cell phone, the heat that emanated from the external surfaces of the house was broadcast into public where anyone with the right equipment could readily perceive it.[249] The Supreme Court rejected this contention, finding that it was a mechanical application of precedent that did not consider the reality of society's privacy expectations.[250] The Court expressed concern that the government's interpretation would allow law enforcement to employ a wide range of intrusive surveillance

241 *See* Brady v. Maryland, 373 U.S. 83, 86 (1963).

242 State v. Andrews, 134 A.3d 324, 344 (Md. Ct. Spec. App. 2016).

243 533 U.S. 27 (2001); *see Andrews*, 134 A.3d at 344.

244 *Kyllo*, 533 U.S. at 29–30.

245 *Id.* at 30.

246 *Id.*

247 *Id.*

248 *See id.*

249 *See id.* at 35.

250 *Id.*

techniques without a warrant, including powerful directional microphones that intercept sound "emanating" from a house or satellite imagery that detects visible light similarly "emanating" from a home.[251] Instead, the Court adopted a rule that took "account of more sophisticated [surveillance] systems that are already in use or in development."[252] It accordingly held that "[w]here . . . the Government uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[253]

As the Maryland court acknowledged, the *Kyllo* opinion rested in part on "the Fourth Amendment sanctity of the home"[254] and left open the question of whether similar surveillance outside the home would constitute a Fourth Amendment search.[255] The *Kyllo* Court recognized, however, that they were more generally addressing the "power of technology to shrink the realm of guaranteed privacy."[256] The Court was troubled by the implications of new technologies, and thus formulated a rule that acknowledged the significance of law enforcement's unique access to these state of the art devices.[257] Had the agent in *Kyllo* hidden his use of the thermal imaging device in the manner that law enforcement now hides the use of stingrays, however, the defendant would have never known to challenge it, and the Supreme Court would not have been presented with the opportunity to review the agent's actions.

A disclosure requirement is thus necessary to grant courts the opportunity to review these new technological developments. The case that established the modern informant's privilege provides guidance on where such a requirement may be derived. In reaching its holding in *Roviaro* that the defendant was entitled to the identity of the confidential informant, the Court relied on notions of fundamental fairness embodied by the Due Process Clause of the Constitution.[258] The

---

251 *Id.*

252 *Id.* at 36.

253 *Id.* at 40.

254 *Id.* at 37.

255 State v. Andrews, 134 A.3d 324, 344 (Md. Ct. Spec. App. 2016). The distinction may be unworkable in practice, however. A state actor may not know whether the target of surveillance is located within a private residence at the time the surveillance is employed. *See id.* at 331 (detailing detective's acknowledgement that the stingray allowed law enforcement to "peer[ ] over the wall of the home" after they had tracked the cell phone to the suspect's house).

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

257 *See id.* at 34, 40.

258 Roviaro v. United States, 353 U.S. 53, 60–61 (1957). Although the Court in *Roviaro* did

Court reasoned that the government deprives the accused of a fair trial when it refuses to disclose the identity of an informant that is relevant and helpful to the preparation of a defense.[259] Although the implications of the secrecy surrounding stingrays' reach beyond fairness in individual cases, the admission of evidence obtained from an illegal search nonetheless undermines a suspect's ability to mount a defense. Accordingly, it is useful to examine how the Supreme Court has addressed similar disclosure failures that prejudice a defendant at trial.

The seminal case on such omissions is *Brady v. Maryland*,[260] in which the Supreme Court addressed the failure of prosecutors to disclose evidence favorable to the accused.[261] In *Brady*, the defendant confessed that he had participated in a robbery during which a death had occurred, but he contended that his accomplice, a man named Boblit, was the actual killer.[262] Under Maryland law, Brady's admitted involvement was sufficient to establish first degree murder—a crime punishable by life imprisonment or death, depending on the presence of mitigating factors.[263] Brady thus accepted the charge against him and argued only for a verdict "without capital punishment."[264] To this end, Brady's lawyer requested that he be allowed to view records of the statements Boblit made to the police, and the prosecution supplied several such statements.[265] After Brady was convicted, sentenced to death, and had exhausted his appeals, however, he discovered that the prosecution had withheld a confession in which Boblit admitted to committing the murder.[266] Brady moved for a new trial, and on review the Maryland Court of Appeals held that the prosecution's suppression of the confession had violated Brady's due process rights.[267]

The Supreme Court agreed, holding that defendants have a fundamental due process right to see favorable evidence upon request

---

not reference the clause by name, subsequent lower court opinions have clarified that the requirement of fundamental fairness cited in *Roviaro* springs from the right to due process. *See, e.g.*, Gaines v. Hess, 662 F.2d 1364, 1367–68 (10th Cir. 1981); McLawhorn v. North Carolina, 484 F.2d 1, 2–4 (4th Cir. 1973).

259 *Roviaro*, 353 U.S. at 60–61.

260 373 U.S. 83 (1963).

261 *See id.* at 87.

262 *Id.* at 84.

263 *See id.* at 85.

264 *Id.* at 84.

265 *Id.*

266 *Id.*

267 *Id.* at 84–85.

when it is material to their guilt or punishment.[268] Just as in *Roviaro*, the Court reasoned that the withholding of such evidence deprives the accused of a fair trial by prejudicing the suspect's ability to prepare a defense.[269] The Court went on to implicitly acknowledge that the ruling could allow some guilty parties to escape punishment, much as the FBI contends would result from the disclosure of stingrays: "[The rule] is not punishment of society for misdeeds of a prosecutor but avoidance of an unfair trial to the accused. Society wins not only when the guilty are convicted but when criminal trials are fair; our system of the administration of justice suffers when any accused is treated unfairly."[270] So, too, does society win when courts and legislatures are permitted to fulfill their constitutionally-prescribed roles, and so, too, does our system of the administration of justice suffer when law enforcement deprives those branches of their mandated functions by systematically shielding controversial investigatory techniques from review.

B. The Obscure Technology Disclosure Rule

By combining *Brady*'s disclosure framework with *Kyllo*'s test for reasonable expectations of privacy within the home, courts may fashion an Obscure Technology Disclosure Rule requiring law enforcement to reveal the use of investigative technology that is not in wide public use to defendants prior to trial. This proposed rule, which closely tracks the functioning of *Brady* disclosures, would ameliorate many of the identified problems arising from law enforcement's practice of hiding stingray use from courts, legislatures, and the public.

1. The Parameters and Effects of the Rule

Although procedures for handling exculpatory evidence under *Brady* vary between jurisdictions within the United States,[271] the operation of the Obscure Technology Disclosure Rule would mirror those currently prescribed by the ABA's Standards for Criminal Justice Discovery and Trial by Jury.[272]

---

268 *Id.* at 87.

269 *See id.* at 87–88.

270 *Id.* at 87.

271 *See generally* LAURAL L. HOOPER, JENNIFER E. MARSH & BRIAN YEH, FED. JUD. CTR., TREATMENT OF *BRADY V. MARYLAND* MATERIAL IN UNITED STATES DISTRICT AND STATE COURTS' RULES, ORDERS, AND POLICIES 4–5 (2004), http://www.uscourts.gov/file/document/treatment-brady-v-maryland-material-united-states-district-and-state-courts-rules.

272 *See* AM. BAR ASS'N, ABA STANDARDS FOR CRIMINAL JUSTICE DISCOVERY AND TRIAL BY JURY 32–33, 35 (3d ed. 1996).

These guidelines clarify *Brady*'s requirements in two key respects. First, although the Supreme Court did not specify the time at which *Brady* disclosures must be made, the ABA's standards make clear that the information should be given to defendants during the course of pretrial discovery.[273] This timing is similarly suitable for the disclosure of obscure investigative technology. The mechanisms for the exchange of information during this period are already well established and understood, minimizing the disruption of integrating the new rule into current practices.[274] Moreover, a defendant who wishes to suppress evidence that the government gained through the improper use of surveillance technology must raise the issue through a pretrial suppression motion.[275] This is not possible if the defendant does not first know that the disputed technology was used, and a later disclosure time could lead to this opportunity being forfeited.

Second, the ABA standards clarify the prosecution's affirmative obligations with respect to *Brady* information.[276] The court in *Brady* addressed only the specific scenario in which a defendant *requests* exculpatory evidence.[277] Subsequent cases have made clear that due process requires prosecutors to turn over exculpatory evidence without a request only when it is "obviously of such substantial value to the defense that elementary fairness requires it."[278] The ABA guidelines, however, recommend that *all* favorable evidence be unilaterally disclosed, referring to the request requirement as "a trap for unknowledgeable defense counsel," that would encourage "game-playing."[279] This affirmative requirement better serves the purposes of the Obscure Technology Disclosure Rule. As amply evidenced by the number of cases in which courts have remained unaware that law enforcement employed a stingray in an investigation,[280] a defendant is unlikely to know that police employed an obscure surveillance technology if the information is not offered. Further, the interest of courts—and by extension, legislatures—in evaluating emerging technology is not coextensive with the needs of a defendant in an individ-

273 *Id.* at 32.

274 *See, e.g.*, FED. R. CRIM. P. 16(a) (outlining prosecutors' pretrial disclosure obligations in federal courts).

275 *See* FED. R. CRIM. P. 12(b)(3)(C).

276 AM. BAR ASS'N, *supra* note 272, at 32–33.

277 *See* Brady v. Maryland, 373 U.S. 83, 87 (1963).

278 United States v. Agurs, 427 U.S. 97, 110 (1976).

279 AM. BAR ASS'N, *supra* note 272, at 33.

280 *See supra* note 15.

ual case, and their ability to do so should not be contingent on defendants' ability to guess correctly.

A rule requiring the affirmative disclosure of information regarding the use of obscure investigative technologies during pretrial discovery is therefore best suited to prevent law enforcement from hiding its use of stingrays and other obscure surveillance devices in the future. Such a requirement would allow emerging technologies to be tested through the crucible of adversarial litigation because accused defendants carry a vested interest in challenging the legality of new techniques and are well situated to do so.[281] And by bringing these technologies into the light and exploring their legal implications, courts would generate the information legislatures need in order to make informed decisions about how existing law should be altered to address new developments.[282]

2. Objections, Counterarguments, and Alternate Proposals

The proposal is undoubtedly controversial, and many criticisms will likely be rooted in in personal judgements about the appropriate balance of security and civil liberties. These base value determinations about how society should be structured are not always amenable to logical resolution. Nonetheless, this Note attempts to address several of the more obvious contentions.

An initial objection may simply be one of necessity. One might argue that prosecutors are already bound by the duty of candor to courts,[283] and this obligation should be sufficient to require the disclosure of the use of stingrays in criminal investigations. This claim proves problematic for several reasons. Foremost among these is the clear evidence that the duty of candor has not prevented law enforcement from hiding the use of stingrays for three decades.[284] This may be due in part to the government's contention that the use of stingrays for tracking and metadata interception does not constitute a search

---

281 *See* Sec'y of State of Md. v. Joseph H. Munson Co., 467 U.S. 947, 956 (1984) (noting that only a litigant with a stake in the proceeding "can reasonably be expected properly to frame the issues and present them with the necessary adversarial zeal").

282 *See, e.g.*, Cyrus Farivar, *Cops Must Now Get a Warrant to Use Stingrays in Washington State*, ARS TECHNICA (May 12, 2015, 9:49 AM), http://arstechnica.com/tech-policy/2015/05/cops-must-now-get-a-warrant-to-use-stingrays-in-washington-state/ (detailing Washington state's passage of bill requiring warrant for stingrays along with detailed explanation to judges as to the technology's workings during application process, after courts discovered police had hidden their use).

283 *See supra* notes 68–76 and accompanying text.

284 *See supra* Part I.

under the Fourth Amendment because the information is shared with cellphone carriers for call routing purposes.[285] If this proposition is accepted as true, there is a colorable argument to be made that the warrantless use of a stingray does not affect the outcome of court proceedings and prosecutors are thus not compelled by the duty of candor to disclose the information.[286] This analysis is flawed, however, because the Supreme Court has interpreted the duty to require disclosure to courts of any development that could *conceivably* affect the outcome of a proceeding.[287] The possibility that the use of a stingray may so influence a court is well demonstrated by the growing number of cases in which courts have considered and rejected the government's claim that a warrant is not required.[288] Significant obstacles nonetheless exist to challenging the candor argument under current legal frameworks. A prosecutor's decision to seek dismissal in a criminal case in which a court discovers that law enforcement has surreptitiously employed a stingray is presumptively unreviewable because it is an exercise of prosecutorial discretion.[289] A civil case challenging the use of the device would face similar procedural difficulties because the Supreme Court has interpreted the Constitution to require that a plaintiff demonstrate "'injury in fact' that is concrete and particularized" in order to have the standing necessary to seek relief against government action.[290] This requisite baseline will limit the parties capable of challenging the withholding of information on stingrays to those that can demonstrate the policy harmed them directly. The secrecy surrounding the devices complicates this task because potential litigants are unlikely to have access to the information necessary to show that police employed a stingray in that instance and caused them the required harm. And, even should these hurdles be overcome,

---

285 *See, e.g.*, Kim Zetter, *Cops Need a Warrant to Grab Your Cell Tower Data, Florida Court Rules*, WIRED (Oct. 17, 2014, 3:31 PM), http://www.wired.com/2014/10/florida-court-requires-warrant-cell-tower-data/ ("The Justice Department has long asserted that law enforcement agencies don't need a probable-cause warrant to use stingrays because they don't collect the content of phone calls and text messages.").

286 *See* Bd. of License Comm'rs of Tiverton v. Pastore, 469 U.S. 238, 240 (1985) (per curiam) ("It is appropriate to remind counsel that they have a 'continuing duty to inform the Court of any development which may conceivably affect the outcome' of the litigation." (quoting Fusari v. Steinberg, 419 U.S. 379, 391 (1975) (Burger, C.J., concurring)).

287 *Id.*

288 *See, e.g.*, State v. Andrews, 134 A.3d 324, 327 (Md. Ct. Spec. App. 2016); United States v. Espudo, 954 F. Supp. 2d 1029, 1032 (S.D. Cal. 2013).

289 *See* U.S. DEP'T OF JUSTICE, *supra* note 73, § 9-27.110(B).

290 Summers v. Earth Island Inst., 555 U.S. 488, 493 (2009) (quoting Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000)).

there is nothing to stop law enforcement from employing a similar tactic with future technological developments.

A skeptic might also question the responsiveness of the suggested framework to the present topic of stingrays. Stingrays have been in use for nearly thirty years, and technological advancements and reductions in cost have placed the technology in reach of nongovernment actors.[291] At the 2010 DEFCON hacking convention, for example, a presenter infamously demonstrated that hobbyists can construct similar devices around $1,500 by activating a homemade unit on stage and intercepting the cell phone signals of people in the audience.[292] Indeed, the technology currently appears to be in wide use; a security firm claiming to have developed a device capable of detecting stingrays reported uncovering as many as eighteen different units in operation when they spent less than two days driving around Washington, D.C.[293]

The regulatory framework of the United States, however, ensures that stingrays are not easily available to the general public. As previously stated, provisions within the ECPA forbid the manufacture, advertisement, distribution, and possession of devices intended to intercept wire, oral, or electronic communications.[294] Further, the FCC and National Telecommunications and Information Administration tightly control access to the electromagnetic spectrum, a key feature of cell site simulators.[295] Indeed, the DEFCON presenter reportedly received warnings from the FCC that she may have been acting in violation of federal law prior to her demonstration.[296] Together, these and other provisions serve to restrict public use of stingrays to a degree that individuals reasonably expect the signal from their phone to be kept private, and the devices would thus qualify for disclosure under the proposed framework.

---

291 *See* Pell & Soghoian, *supra* note 23, at 9.

292 Sean Hollister, *Hacker Intercepts Phone Calls with Homebuilt $1,500 IMSI Catcher, Claims GSM Is Beyond Repair*, ENGADGET (July 31, 2010), https://www.engadget.com/2010/07/31/hacker-intercepts-phone-calls-with-homebuilt-1-500-imsi-catcher/.

293 Ashkan Soltani & Craig Timberg, *Tech Firm Tries to Pull Back Curtain on Surveillance Efforts in Washington*, WASH. POST (Sept. 17, 2014), https://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html.

294 *See* 18 U.S.C. § 2512 (2012).

295 *See Radio Spectrum Allocation*, FCC, https://www.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation (last visited Mar. 29, 2017).

296 *See 2010 DEF CON-18 Hacking Conference Held*, W5YI GRP. (Aug. 1, 2010), http://www.w5yi.org/ama_news_article.php?id=487.

Another potential objection to a disclosure rule for new technology is identical to the FBI's and other law enforcement's proffered justification for the secrecy surrounding stingrays: disclosure of investigative technologies will allow criminals to circumvent them and render them ineffective.[297] Setting aside the substantial conjecture required to reach this conclusion, it nonetheless fails to persuade. Nearly all restrictions placed on criminal investigations involve tradeoffs in which effectiveness is sacrificed in the name of personal liberty and governmental integrity. It is likely that more criminals would be arrested, for instance, if police were free to install cameras in every home. Nonetheless, the Constitution places limits on these activities in favor of other countervailing interests. So too here, where maintaining the balance between the branches of government, including the oversight roles of the legislative and judicial branches, outweighs any incremental decrease in executive effectiveness.

Further, the proposed rule applies strictly to criminal investigations and does not concern the activities of the military and intelligence communities, including counter-terrorism operations. The Supreme Court has long held that the Fourth Amendment imposes different requirements when the government's primary purpose for a search is something other than gathering information for a criminal prosecution of a person with ties to the United States.[298] This includes when the search is aimed at preventing a terrorist attack or gathering military and foreign intelligence.[299] And the Fourth Amendment does not apply at all when the government surveils non–United States persons located abroad.[300] Government actors who fear the consequences of foreign targets learning of an emerging technology would therefore retain the option of simply not utilizing it in domestic criminal investigations. Disclosure would only be required when the techniques are utilized in an investigation governed by conventional formulations of constitutional liberties.

Lastly, privacy advocates may object that the proposed disclosure rule does not go far enough and argue that the government should be

---

297 *See* Morrison Deposition, *supra* note 42, at 2.

298 *See* 3A CHARLES ALAN WRIGHT & SARAH N. WELLING, FEDERAL PRACTICE AND PROCEDURE § 681 (4th ed. 2010) (listing administrative and special needs exceptions to the Fourth Amendment warrant requirement).

299 *See* United States v. U.S. Dist. Court for the E. Dist. of Mich., 407 U.S. 297, 321–33, 322 n.20 (1972) (holding conventional warrant requirements not to apply to domestic security surveillance and "express[ing] no opinion" as to whether similar considerations apply "with respect to activities of foreign powers or their agents").

300 United States v. Verdugo-Urquidez, 494 U.S. 259, 267 (1990).

precluded from applying the informant's privilege to any state actor. This blanket prohibition is over inclusive. Embedded undercover agents, for instance, may provide valuable information in a criminal investigation without ever employing means that implicate the Fourth Amendment or other statutory or constitutional guarantees.[301] Similarly, an argument might be advanced that all use of technology that is not in general public use should be considered an invasion of reasonable expectations of privacy, and thus a search presumptively requiring a warrant under the Fourth Amendment. Again, this proposal proves over inclusive. People reasonably expect law enforcement to use some technologies that are not prevalent in the public sphere, such as a radar gun to monitor speeding cars. Few would argue that drivers have a reasonable privacy interest in how fast they go, and it would not be practicable for police to obtain a probable cause warrant every time they use these routine technologies. While courts may be able to tailor exceptions to such general prohibitions, crafting a rule that accommodates these actors while still encompassing the problematic usage of technology detailed here, raises serious questions of administrability and lacks the simplicity of a bright line disclosure rule.

Conclusion

As the world moves further into the digital age and criminals continue to develop new tools and methods to further their enterprises, it is important that law enforcement likewise utilize innovative techniques to combat these endeavors. Such efforts, however, should not undermine the integrity of the justice system. It is the purview of the courts to ensure compliance with the law, and that of legislatures to alter the law when necessary. These parties cannot perform their function when executive law enforcement withholds information and misleads them as to their activities. The fact that a controversial investigatory technique can be surreptitiously employed for nearly thirty years without being subjected to meaningful judicial review is clear evidence that significant reform is needed. By utilizing the proposed disclosure rule, courts may take steps to close this hole in existing law and ensure that similar interbranch conflict does not occur in the future.

---

301 *See* Hoffa v. United States, 385 U.S. 293, 301–04 (1966) (holding warrantless use of undercover agents was constitutional under the Fourth and Fifth Amendments).