WHO’S PINGING YOUR PHONE? EXPLORING THE FOURTH AMENDMENT RAMIFICATIONS OF STINGRAY DEVICES


KAREN VAYSMAN*

INTRODUCTION

In 2001, the Supreme Court in Kyllo v. United States profoundly declared that “[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”¹ No less true is this statement today than when it was made, sixteen years ago, at a time when smartphones of the kind that exist today were unheard of to the Court. The modern smartphone device possesses unprecedented capabilities. With its massive storage capacity and ability to collect, all in one place distinct types of information, the phone can reconstruct an individual’s private life, all in the palm of a hand.²

Technological progress has a dual capability to decrease privacy, yet simultaneously augment the expectation of privacy. As cellphones become more sophisticated, so too does police surveillance. With


Stingrays and cell-site simulator devices, long gone are the days when law enforcement needed to heavily rely on a phone carrier company’s assistance for surveillance. Stingrays enable law enforcement to obtain directly, in real time (indeed, automatically), unique device identifiers and detailed location information of cellphones—data that it could not otherwise obtain without the assistance of phone companies. These devices can uncover more than just a phone’s location: they can eavesdrop on calls, block cell service, and intercept data transmitted and received by the phone, including, emails, text messages and web pages visited. This is just the tip of the iceberg.

While law enforcement may only seek to identify, or locate the target’s mobile device, “a Stingray will also, as a matter of course, collect data from many other mobile devices in the surrounding area.”

3 “Stingray” is the trade name for a cell-site simulator device manufactured by the Harris Corporation. A cell-site simulator goes by many different names, including, “Stingray,” “Triggerfish” and “Kingfish.” Cell-site simulators are also called International Mobile Subscriber Identity (“IMSI”) catchers, referring to the unique identifier or international subscriber identity of the wireless devices that they track. Howard W. Cox, Stingray Technology and Reasonable Expectations of Privacy in the Internet of Everything, 17 FEDERALIST SOC’Y REV. 29, 29 n.3 (2016); Ryan Gallagher, Meet the Machines That Steal Your Phone Data, ARS TECHNICA (Sept. 23, 2013, 12:00 PM), https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/. This Note uses the term “Stingray” to refer generally to cell-site simulator devices.

4 Once the cell phones in the area send their signals to the cell-site simulator, the device captures a vast array of information, including, but not limited to, the cell phones’ IMSI or electronic serial number (“ESN”). In re Application of the United States of America for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, 2015 WL 6871289, at *2 (N.D. Ill. Nov. 9, 2015); 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, 142–43 (2014).

5 Pell & Soghoian, supra note 4, at 142–43.

6 Harris offers an optional “GSM Intercept Software package” for the Stingray. See id. at 146 n.36 (citing HARRIS GCSD PRICE LIST, HARRIS CORP. WIRELESS PRODS. GRP. 4 (2008), https://info.publicintelligence.net/Harris-SurveillancePriceList.pdf).

7 Pell & Soghoian, supra note 4, at 134, 145–48.
Regardless of whether law enforcement install the device in a vehicle, mount it on a drone, or carry it by hand on the street, the search is the same: it casts a wide net, receiving information from *all cellphones* within its range until the target phone is located. 8 These cellphones belong to people not suspected of any wrongdoing, wholly unconnected and unrelated to a search. Unfortunately, the high-volume collection of their information becomes collateral damage.

*United States v. Patrick*9 is the first time that constitutional questions posed by Stingrays reached a court of appeals, and the Seventh Circuit got the first word. In *Patrick*, police used a Stingray that pinpointed the defendant’s location for his arrest, and factual deficiencies in the record raised serious questions of whether their location tracking warrant authorized them to do so.10 The defendant then challenged the validity of his arrest and seizure of the gun that police found in his possession during his arrest based on the warrantless Stingray search.11 A divided panel found that the police’s use of the Stingray did not warrant application of the exclusionary rule.12 Judge Easterbrook, writing for the majority, explained the Stingray issues diverted from the meat and potatoes: police arrested the defendant on a public street, with probable cause to arrest and pursuant to an outstanding arrest warrant; this rendered the arrest and seizure of the gun incident to the arrest lawful.13 Chief Judge Wood disagreed, focusing her dissent not on *where* police found him, but

---


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

10 *Id.* at 541–43.

11 *Id.* at 541.

12 *Id.* Judge Easterbrook, joined by Judge Kanne, affirmed the district court’s denial of the defendant’s motion to suppress and affirmed the defendant’s conviction. *Id.* at 540–45 (majority opinion). Chief Judge Wood dissented. *Id.* at 545–52 (Wood, C.J., dissenting).

13 *Id.* at 540–45 (majority opinion).
She argued the many factual holes regarding the Stingray and its use in the case precluded a meaningful resolution of whether the police violated the defendant’s Fourth Amendment rights. In light of 

Patrick and the inevitable rapid advancements in technology, this Note tackles the inexhaustible question: to what extent will courts allow technology to limit the realm of guaranteed privacy? This Note unfolds in five parts. Part I explains how Stingrays operate. Part II focuses on the Fourth Amendment jurisprudence and discusses the Supreme Court’s instructive cases governing what constitutes a “search or seizure,” that is “unreasonable,” the warrants requirements, and the exclusionary rule. Part III then examines the Court’s precedential Fourth Amendment case law pertaining to electronic surveillance and its recent decision on the exclusionary rule in Utah v. Strieff, all of which that the court in Patrick heavily relied upon. Part IV then turns to Patrick and reviews the factual background and main points raised by the majority and dissent. Part V argues three ways in which the Seventh Circuit’s decision chipped away at the realm of guaranteed privacy. Given the high stakes of Stingray searches, and in particular, the implications on third parties, this Note concludes with a discussion on the need for greater judicial oversight to strike an effective balance between the objectives of law enforcement and Fourth Amendment privacy rights.

I. What Are Stingray Devices?

Stingray technology, in some form or another, is more than 20 years old. Cell-site stimulators were initially developed and used by military and intelligence agencies, and they have since made their way

14 Id. at 552 (Wood, C.J., dissenting).
15 Id.
to state and local law enforcement agencies. The American Civil Liberties Union ("ACLU") reports that state and local police began to purchase these devices as early as 2002. The ACLU estimates that 72 agencies in 24 states and the District of Columbia own a Stingray-type device.

While a comprehensive analysis of Stingray technology lies beyond the scope of this Note, this Part briefly discusses the basics of Stingray devices and surveillance technology to illustrate the magnitude of the Stingray’s departure from traditional surveillance. Cellphones contain radio signal transmitters and receivers that connect to cellphone towers or “cell sites.” These cell sites are your typical raised structures with antennae that facilitate the transmission and receipt of electronic communication. Cellphones and cell sites communicate with one another by sending each other signals, and this back-and-forth communication enables the phone carrier to route calls, text messages and Internet data to and from a cellphone on networks like Sprint, Verizon, AT&T, etc. Cellphones also have unique digital identifiers, assigned by the device’s manufacturer or cellular network provider, which blast out to cell sites and allow networks to identify a

---

18 Id.
21 For example, a cellphone displays “bars,” which represent the measurement of signal strength. Shane Dingman, Tracking our Phones: How Stingray devices are being used by police, THE GLOBE AND MAIL (Mar. 21, 2016, 10:37 PM), http://www.theglobeandmail.com/technology/tracking-our-phones-how-stingray-devices-are-being-used-by-police/article29322747/.
22 See e.g., Dingman, supra note 21; Brinson, supra note 17.
23 See e.g., Brinson, supra note 17.
cellphone user and their device.\textsuperscript{24} This process automatically generates identifying information, including location data of varying degrees of precision.\textsuperscript{25}

As a general matter, with a valid order, government agencies can compel a provider to disclose location data, whether that data was generated by the wireless carrier in the normal course of business or specifically created in response to a surveillance request to “ping” a phone.\textsuperscript{26} Pinging is the process that allows service providers to generate location data at any time with a signal that directs the built-in satellite receiver in the particular cellphone to calculate its location and transmit that data back to the service provider.\textsuperscript{27} The cellphone needs only to be turned on; no calls need to be made, received, or completed for the service provider to ping a cellphone and determine its location.\textsuperscript{28} And unlike Global Positioning System (“GPS”) technology,\textsuperscript{29} a user cannot disable cell site location information technology and it does not require any specific device capability.\textsuperscript{30}

\begin{itemize}
  \item \textsuperscript{24} Id.
  \item \textsuperscript{25} Id.
  \item \textsuperscript{26} Pell & Soghoian \textit{supra} note 4, at 145 & n.29.
  \item \textsuperscript{27} \textit{In re Application of the U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone}, 849 F. Supp. 2d 526, 534 (D. Md. 2011).
  \item \textsuperscript{28} People v. Moorer, 959 N.Y.S.2d 868, 875 (Monroe Cnty. Ct. 2013); \textit{In re Application of the U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone}, 849 F. Supp. 2d at 533.
  \item \textsuperscript{29} GPS is a satellite based navigation system. It consists of satellites that orbit the Earth and transmit signals that give the current GPS satellite position and time. Once the GPS receiver in a cellphone captures signals from multiple satellites, it uses the transmitted data to calculate, based upon the relative strengths of signals from these multiple satellites and the time it took to receive a transmitted signal, a user’s location. \textit{The Global Positioning System}, GPS.GOV (last updated Sept. 26, 2016), http://www.gps.gov/systems/gps.
  \item \textsuperscript{30} GPS technology can typically calculate high quality accuracy location within ten meters. But limitations expose its fallible nature. A cellphone user can deactivate the GPS function (i.e.—turning off “location services” on an iPhone), and thus disable the ability to locate them. Also, if a GPS receiver’s view of the satellites is obstructed, it can comprise the reliability of GPS data. \textit{In re Application of U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless

370
Stingrays operate in both similar and very different manners. They operate by mimicking cell towers, sending a mimicked “ping” signal. Nearby cellular devices then “identify the simulator as the most attractive cell tower in the area and transmit signals to the simulator that identify the device in the same way that they would with a networked tower.” Stingrays achieve greater precision; while a carrier’s cell-site location data can identify the location of a suspect’s complex, a Stingray can zero in on a phone’s location, down to a specific apartment.

There is one alarming difference: the signal a Stingray sends out compels all cellphones within range to transmit their unique identification information and location data to the Stingray, thereby scooping up data from every cellphone within reach, not just the target. Unlike the target specific search a phone carrier executes when asked to reveal data of the “sought after person,” no such boundary exists with Stingrays. One can dress up a Stingray with the purchase of an “Intercept Software Package,” which allows the user

---


33 See generally Pell & Soghoian, supra note 4.

34 United States v. Patrick, 842 F.3d 540, 543 (7th Cir. 2016) (“[a] cell-site simulator collects the relative location of everyone whose phone is induced to connect to the simulator . . . .”); Jonathan Bard, Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment, 57 B.C. L. REV. 731, 748 (2016).

35 Patrick, 842 F.3d at 542–44.

36 HARRIS GCSD PRICE LIST, supra note 6, 8.
of a Stingray to intercept calls, text messages, e-mail, and other data as well as block service to all or some devices in the area.\textsuperscript{37}

The severity of a Stingray’s implications vis-à-vis third parties not subjects of an investigation becomes evident when considered in our era of cellphone primacy. Although initially cellphones were primarily used to make calls, modern advancements have transformed the device into a multi-functional tool “more accurately labeled a pocket super-computer.”\textsuperscript{38} The Pew Research Center reports that as of January 2017, 95 percent of all Americans own a cellphone of some kind.\textsuperscript{39} And of that share, 77 percent own smartphones.\textsuperscript{40} Smartphones have internet access and the ability to download a bountiful number of applications.\textsuperscript{41} Those that provide directions and social networking platforms barely scratch the surface.\textsuperscript{42} And because many third-party applications automatically send and receive data through the cellphone subscriber’s network, it makes this information vulnerable to a Stingray search too.\textsuperscript{43} As smartphones evolve, their storage capacities become the fulcrum; these devices can store for long periods of time

\textsuperscript{37} The Department of Justice concedes that Stingrays possess such abilities and relies on law enforcement to configure the device to disable these functions. DOJ Policy Guidance, supra note 31, at 2; Pell & Soghoian, supra note 4, at 11–12.

\textsuperscript{38} The “basic” cellphone model today far exceeds simple call-making capabilities: “Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.” Riley v. California, 134 S. Ct. 2473, 2489 (2014). See also Steven I. Friedland, Riley v. California and the Stickiness Principle, 14 DUKE L. & TECH. REV. 121, 125–27. (2016).

\textsuperscript{39} Mobile Fact Sheet, PEP RESEARCH CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/.

\textsuperscript{40} This is a significant increase from the 35 percent that the Pew Research Center reported in 2011 in a survey of smartphone ownership. Id.

\textsuperscript{41} Friedland, supra note 38, at 126.

\textsuperscript{42} Riley, 134 S. Ct. at 2490 (“There are over a million apps available in each of the two major app stores; the phrase “there's an app for that” is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user’s life.”)

\textsuperscript{43} United States v. Patrick, 842 F.3d 540, 547 (7th Cir. 2016) (Wood, C.J., dissenting) (citing Pell & Soghoian, supra note 4, at 11–12).
and disseminate, huge amounts of data, photos, financial and medical records, emails, and messages. Viewed in the aggregate, the data represents “a picture of a person’s private world.” All of this begs the question, how would 95 percent of the population at large react if they knew that police can access the privacies of their world with a simple add-on like the “Intercept Software Package”?

II. FOURTH AMENDMENT JURISPRUDENCE

The Fourth Amendment to the United States Constitution states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

During the Colonial era, the crown of England frequently issued general search warrants known as “Writs of Assistance.” At their core, these instruments authorized English officials to enter places, search at their will, and seize customs-prohibited items. The officials needed no factual basis to justify the intrusion; the Writ alone gave them all the power.

---

44 Friedland, supra note 38, at 126. A prime example of advances that facilitate the interconnectedness of cellphone data is Apple’s recent release of “Continuity,” a software that enables all a user’s devices to work together. Use Continuity to connect your Mac, iPhone, iPad, iPod touch, and Apple Watch, APPLE, https://support.apple.com/en-us/HT204681 (last visited Apr. 7, 2017).
45 U.S. CONST. amend. IV.
47 Id.
48 Id.
To serve as safeguard against such abuses, the Fourth Amendment was enacted with two separate clauses that articulate two distinct requirements.\(^{49}\) The Reasonableness Clause provides a broad prohibition against all “unreasonable searches and seizures” of “persons, houses, papers, and effects.”\(^{50}\) The Warrants Clause then requires that a warrant for a search or seizure be supported by “probable cause” and “particularly describe the place to be searched, and the persons or things to be seized.”\(^{51}\) Read in tandem, the Fourth Amendment requires any search or seizure, subject to certain exceptions, be authorized by a warrant and supported by a showing of probable cause.\(^{52}\)

Section A of this Part briefly explores the Court’s Fourth Amendment jurisprudence on the Reasonableness Clause. This involves a two-part, and often blurred, analysis that asks whether a “search” or “seizure” occurred within the meaning of the Fourth Amendment. The inquiry turns on whether an individual had a “reasonable expectation of privacy” in the item seized or the place searched.\(^{53}\) Section B then addresses the warrant requirements triggered when a court finds that a “search” or “seizure” has occurred. Part II concludes with Section C, which introduces the exclusionary rule available for a court to apply to safeguard the Fourth Amendment.

### A. The Evolution of the Fourth Amendment & the Reasonableness Clause

Since the Fourth Amendment’s ratification, the Court’s interpretation of a “search” has been in flux. In 1886, the Court in *Boyd v. United States* articulated the first major interpretation of the


\(^{50}\) U.S. CONST. amend. IV

\(^{51}\) See *id*.


term within the meaning of the Fourth Amendment. In doing so, the Court explained it must interpret the Fourth Amendment broadly, given its protection of “the privacies of life.” Drawing on pre-Revolutionary events and cases, the Court analogized a forced document production to the physical invasion of one’s home and concluded that the compelled production of private papers at issue in Boyd constituted a search under the Fourth Amendment.

In 1928, however, the Court in Olmstead v. United States abandoned Boyd’s liberal interpretation. Olmstead involved a case of wiretaps attached to telephone wires on public streets. Rooting the inquiry in the concept of trespass, which requires a physical intrusion, the Court reasoned that because the wiretapping involved neither a physical entry into the defendant’s house nor a confiscation of tangible property, no Fourth Amendment violation had occurred. Justice Brandeis wrote a noteworthy dissent, finding it “immaterial where the physical connection with the telephone wires was made.” He argued that while the private conversation transmitted by wire did not fall within the literal words of the Fourth Amendment, the way to meaningfully protect privacy rights is to deem “every unjustifiable intrusion by the government upon the privacy of the individual” as a Fourth Amendment violation.

Nearly forty years later, the Court decided Katz v. United States, proving once again that the Fourth Amendment jurisprudence did not remain static. At issue in Katz was the government’s eavesdropping

54 116 U.S 616 (1886).
55 Id. at 630; see also Jonathan Bard, Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment, 57 B.C. L. Rev. 731, 735 (2016).
56 Boyd, 116 U.S. at 633.
57 277 U.S. 438 (1928).
58 Id. at 457.
59 Id. at 466; Sklansky, supra note 52, at 152.
60 Olmstead, 277 U.S. at 479 (Brandeis, J., dissenting).
61 Id. at 478; United States v. Jones, 565 U.S. 400, 421–22 (2012).
of a public telephone booth from which the defendant placed calls.\(^{63}\) Police conducted surveillance through an electronic listening and recording device attached to the outside of the booth.\(^{64}\) This form of surveillance fell on par with the wiretapping at issue in *Olmstead*.\(^{65}\) Interestingly, under the *Olmstead* framework, no search (physical trespass) or seizure (confiscation of tangibles) occurred in *Katz*.\(^{66}\) And like the street wires in *Olmstead*, the booth in *Katz* logically did not fall within the realm of “persons, houses, papers, and effects” that the Court had understood the Fourth Amendment to protect.

Notwithstanding these parallels, Justice Stewart, writing for the majority, notoriously declared: “the Fourth Amendment protects people, not places.”\(^{67}\) The *Katz* Court ultimately held that the police’s eavesdropping on the defendant’s calls constituted a search and seizure because it “violated the privacy upon which he justifiably relied when he used the telephone,” despite the booth’s public location.\(^{68}\)

The holding in *Katz* extended the Fourth Amendment’s protections from physical intrusions onto physical and tangible property to individual’s privacy interests and intangible property.\(^{69}\) *Katz* thus marked a clear shift in the Court’s Fourth Amendment jurisprudence focused on a common-law property-based trespass approach.\(^{70}\)

*Katz* also laid the groundwork for the expanded definition of a search to where the government intrudes on an individual’s “expectation of privacy.”\(^{71}\) In order for an individual’s expectation of privacy to be afforded constitutional protection, two prongs must be

\(^{63}\) Id. at 348.

\(^{64}\) Id.

\(^{65}\) *Olmstead*, 277 U.S. at 457.

\(^{66}\) *Katz*, 389 U.S. at 351–52.

\(^{67}\) Id. at 351.

\(^{68}\) Id. at 353.

\(^{69}\) Id.; see also Sklansky, *supra* note 52, at 150–54.

\(^{70}\) See United States v. Jones, 565 U.S. 400, 409 (2012) (“Our later cases, of course, have deviated from [the] exclusively property-based approach.”).

\(^{71}\) *Katz*, 389 U.S. at 360 (Harlan, J., concurring).
satisfied: (1) the individual must exhibit an actual, subjective expectation of privacy; and (2) that expectation must be one that society is prepared to recognize as reasonable.\textsuperscript{72} Since \textit{Katz}, the Court has understood the Fourth Amendment to protect a person’s reasonable expectation of privacy, but has clarified that that \textit{Katz}’s “reasonable expectation of privacy” test has been “\textit{added to, not substituted for}” the “common-law trespass” test.\textsuperscript{73}

\textbf{B. The Warrants Clause}

Absent exceptional circumstances, if a court finds that a search or seizure has occurred under the Fourth Amendment, it triggers the warrants requirements.\textsuperscript{74} The Court has interpreted the Warrants Clause to consist of three requirements: (1) warrants must be issued by a neutral and detached magistrate; (2) those seeking the warrant must demonstrate to the magistrate their probable cause to believe that “the evidence sought will aid in a particular apprehension or conviction” for a particular offense; and (3) warrants must particularly describe the place to be searched and the things to be seized.\textsuperscript{75}

\textsuperscript{72} \textit{Id.} at 361. The Court in \textit{Katz}, however, did not refine the understanding of “reasonableness.”

\textsuperscript{73} \textit{Jones}, 565 U.S. at 409.

\textsuperscript{74} \textit{Katz}, 389 U.S. at 357. The Court eloquently described the purpose and meaning of the Warrants Clause in \textit{Johnson v. United States}:

\textit{[T]he point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity . . . When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.}


When the Court decided *Katz*, it typically found searches conducted without warrants to be unlawful “notwithstanding facts unquestionably showing probable cause.”

In fact, the Court in *Katz* affirmed that the prevailing understanding of an “unreasonable search” under the Fourth Amendment generally meant “without probable cause and a warrant.”

Consistent with its precedent, the *Katz* Court also reaffirmed that subject only to the specific established and well-delineated exceptions, “searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment.”

Six months after *Katz*, the Court in *Terry v. Ohio* shed light on its new view on the connection between the Warrants Clause and the unreasonableness of a search. When confronted with the legality of the widespread and controversial stop and frisk procedures that police conducted without a warrant and probable cause, the Court in *Terry* broke with traditional understanding of what constituted “unreasonable” under the Fourth Amendment. Rather than reconciling the warrantless stop and frisk procedures under the limited exceptions referred to in *Katz*, the Court instructed that the central inquiry under the Fourth Amendment is “the reasonableness in all the circumstances of the particular governmental intrusion of a citizen's personal security.”

Translated to the context of *Terry*, a stop and frisk was not unreasonable simply because it was not authorized by a warrant or because the police lacked the probable cause needed for an arrest. The reasonableness of such a search rather turned on whether an

---

76 Katz, 389 U.S. at 357 (citing Agnello v. United States, 269 U.S. 20, 33 (1925)).
77 *Id.* (citing Wong Sun v. United States, 371 U.S. 471, 481–482 (1963)). See also Sklansky, *supra* note 52, at 151–52.
78 Katz, 389 U.S. at 357.
80 *Id.* at 4; Sklansky, *supra* note 52, at 154.
81 *Terry*, 392 U.S. at 19.
82 *Id.* at 26–27; see also Sklansky, *supra* note 52, at 155.
officer had “reasonable suspicion” to first initiate the search, and whether the resulting search was reasonably related to the scope of the circumstances which justified the officer’s search in the first instance. This line of analysis thus allows courts to find that a warrantless search does not violate the Fourth Amendment if the search was “reasonable.” In this respect, Terry and Katz both clarify that while one may generalize that a warrantless search is “presumptively unreasonable,” it is not per se unreasonable.

Despite this wrinkle, the Court has repeatedly held that where law enforcement conducts a search for discovering evidence of criminal wrongdoing, reasonableness generally requires it first obtain a judicial warrant. Magistrates are vested with a vital constitutional responsibility in the issuance of search warrants. To prevent an overly intrusive search, they must determine that all aspects of the search are supported by probable cause and impose appropriate limitations and conditions on the scope by fulfilling the particularity requirements. A sufficiently particular warrant includes an authorization to search places and things in which the particular things described might be concealed. If a court finds that the “scope of the search exceeds that permitted by the terms of a validly issued warrant” then “the subsequent seizure is unconstitutional without more.”

---

83 Terry, 392 U.S. at 19–20. The framework Terry created grants police latitude to conduct a search without a warrant where “the intrusion on the citizen's privacy 'was so much less severe' than that involved in a traditional arrest that 'the opposing interests in crime prevention and detection and in the police officer’s safety could support' the seizure as reasonable.” See Bailey v. United States, 133 S. Ct. 1031, 1037 (2013).


87 Groh v. Ramirez, 540 U.S. 551, 561 (2004). A particular warrant “assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.” Id.

88 Michigan v. Summers, 452 U.S. 692, 694 (1981). See also Groh, 440 U.S. at 557 (“[A] warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional.”) (citations omitted).

Police officers must execute the warrant in a reasonable manner, and the reasonableness of execution is subject to later judicial review. The scope of the warrant does not need to specify the manner of execution because the warrant process and the particularity requirements are concerned more with what may be searched and seized rather than how. The vitality of this distinction becomes unclear in the context of electronic surveillance, because not all information gathering technology is equivalent both in function and degree of intrusiveness.

To illustrate, an officer may obtain a warrant that authorizes the disclosure of an individual’s physical location, and there are numerous ways an officer can then ascertain this information. But, a location tracking warrant that authorizes the disclosure of a phone’s location does not, without more, authorize a search of the contents of the cellphone itself. The latter requires an independent search warrant. A search that forces a cellphone to transmit location data through contents stored within the phone is thus not the same as a phone provider initiating a signal to determine that same information. The two are simply not equivalent, even if the officer’s purpose in both scenarios focuses on identifying the phone’s physical location, which the location warrant may have authorized. It is then possible that an officer’s chosen method includes a device that functions in a manner sufficiently different from the location-gathering methods specified in a warrant that its use should constitute a search outside the warrant’s scope. Part V will discuss these issues in further detail.

Ultimately, because police conduct does not always conform to the Fourth Amendment’s mandates, the Court has recognized that it,

---

91 United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999).
92 United States v. Patrick, 842 F.3d 540, 549 (7th Cir. 2016) (Wood, C.J., dissenting).
94 Patrick, 842 F.3d at 549 (Wood, C.J., dissenting).
and other courts, must exclude evidence obtained by unconstitutional police conduct.\textsuperscript{95} Part C now turns to the exclusionary rule.

\textit{C. The Exclusionary Rule}

In practice, the exclusionary rule allows a court to suppress evidence obtained in violation of the Fourth Amendment’s guarantee against unlawful searches and seizures.\textsuperscript{96} As written, the Fourth Amendment does not contain a provision that expressly precludes the use of evidence obtained through unconstitutional conduct.\textsuperscript{97} Whether the application of the exclusionary rule is appropriate in a particular case is “an issue separate from the question of whether the Fourth Amendment rights of the party seeking to invoke the rule were violated by police conduct.”\textsuperscript{98} This means a court may recognize that an individual’s Fourth Amendment rights were violated but still decide not to apply the exclusionary rule.

The exclusionary rule is neither intended nor able to “cure the invasion of the defendant’s rights which he has already suffered.”\textsuperscript{99} Rather, it operates as “a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved.”\textsuperscript{100} Because the purpose of the exclusionary rule is to deter police misconduct, a court may only apply the rule and suppress evidence if it determines that the deterrent benefits of exclusion outweigh its costs.\textsuperscript{101} So even when police obtain evidence through an

\textsuperscript{95} Utah v. Strieff, 136 S. Ct. 2056, 2059 (2016).
\textsuperscript{96} Id. at 2029.
\textsuperscript{97} United States v. Leon, 468 U.S. 897, 906 (U.S. 1984).
\textsuperscript{98} Id. (citing Illinois v. Gates, 462 U.S. 213, 223 (1983)).
\textsuperscript{99} Indeed, the Court has indicated that through its examination of the Fourth Amendment’s origin and purposes, the use of “fruits” of a past unlawful search or seizure “works no new Fourth Amendment wrong.” Id.
\textsuperscript{100} Id. (citing United States v. Calandra, 414 U.S. 338, 348 (1974) (emphasis added)).
\textsuperscript{101} Strieff, 136 S. Ct. at 2059. sBecause the Court severs the inquiry of whether a Fourth Amendment violation has occurred from the exclusionary rule’s remedy to
unconstitutional search or seizure, suppression of that evidence is not the automatic consequence.\textsuperscript{102}

Standing doctrine principles also limit a defendant’s ability to invoke the exclusionary rule.\textsuperscript{103} The Fourth Amendment right against an unreasonable search and seizure is a personal right, which “may not be vicariously asserted.”\textsuperscript{104} Thus, to have the requisite standing to bring a Fourth Amendment claim and invoke the exclusionary rule, a defendant must show that the challenged conduct invaded his own legitimate expectation of privacy rather than that of a third party.\textsuperscript{105}

Axiomatically, then, a defendant cannot succeed on a motion to suppress evidence by arguing that the challenged police conduct effectively violated others Fourth Amendment rights.\textsuperscript{106} Suppression is proper only if the defendant’s own rights have been violated.\textsuperscript{107} The Court has made clear that a court cannot suppress otherwise suppressible evidence, it can manipulate the results. For an argument on how the Supreme Court has utilized the rule’s deterrent aspect to circumvent the inadmissibility of evidence obtained in violation of the Fourth Amendment, see Gerald G. Ashdown, \textit{The Fourth Amendment and the “Legitimate Expectation of Privacy”}, 34 \textit{VAND. L. REV.} 1289, 1292–94 (1981)\textsuperscript{102} \textsuperscript{Leon}, 468 U.S. at 906.

Standing stems from the “Case-or-Controversy” requirement under the judiciary’s Art. III powers. (“The judicial power shall extend to all Cases . . . [and] Controversies.” U.S. CONST. amend. III, § 2, cl.1. It pertains to who is the proper party to litigate a matter in court\textsuperscript{104} Rakas v. Illinois, 439 U.S. 128, 133–34 (1978).\textsuperscript{105} United States v. Payner, 447 U.S. 727, 731 (1980).\textsuperscript{106} Defendants commonly bring Fourth Amendment challenges in pre-trial motions to suppress incriminating evidence. The proponent of a motion to suppress has the burden of establishing that his Fourth Amendment rights were violated by the challenged search or seizure by a preponderance of the evidence. \textit{Rakas}, 439 U.S. at 130 n.1; United States v. Johnson, 63 F.3d 242, 245 (3d Cir. 1995). Once a proponent establishes a basis for the motion (i.e.—the conduct constituted a search or that a seizure was conducted without a warrant), the burden shifts to the government to show each individual act constituting a search or seizure was reasonable. Johnson, 63 F.3d at 245.

In \textit{Patrick v. United States}, both the majority and the dissent raised this issue. 842 F.3d 540, 545–46. \textit{See also infra} pp. 55–57 (expanding upon the implications of standing and Stingray searches).
admissible evidence on the ground that it was seized unlawfully from a third party not before the court.\textsuperscript{108} “The interest in deterring illegal searches does not justify the exclusion of tainted evidence at the instance of a party who was not the victim of the challenged practices.”\textsuperscript{109}

These constrains limit the discussion of unconstitutional conduct that may affect innocent parties, particularly in the context of digital searches. Recall that during a Stingray search, police send out pings that may collateral search third parties’ phones. But, a defendant does not have an expectation of privacy in the cellphones of third parties, so he cannot attack the search as “too sweeping.”\textsuperscript{110} Sadly, this may be unconstitutional conduct as to the parties whose interests were unreasonably invaded, but “a search can be unconstitutional with respect to one person yet lawful as to another.”\textsuperscript{111}

III. Background Precedential Case Law

Although United States v. Patrick is the focus of this Note, the Seventh Circuit’s analysis heavily relied on a collection of Supreme Court case law dealing with electronic surveillance as well as the Court’s recent decision in Utah v. Strieff pertaining to the exclusionary rule. To understand the Patrick decision and why it suggests a departure from Supreme Court precedent, it is imperative to first discuss the facts and analyses of these prior cases.

A. Supreme Court Fourth Amendment Surveillance Case Law

Consistent with Katz, the Supreme Court began to explore whether the use of various novel technologies intruded upon individuals’ reasonable expectations of privacy. In 1979, the Court in Smith v. Maryland held that the installation and use of a “pen register,”

\begin{footnotes}
\item[108] Payner, 447 U.S. at 735–36.
\item[109] Id.
\item[110] See id.
\item[111] United States v. Gray, 491 F.3d 138, 144–45 (4th Cir. 2007).
\end{footnotes}
a device that attaches to a telephone line and records the phone numbers dialed did not constitute a search and thus did not require a warrant. In Smith, police requested that a telephone company install a pen register to record the numbers dialed by the defendant. The Court held that an individual does not have an expectation of privacy in information conveyed to a third party. Accordingly, the defendant did not have a reasonable expectation of privacy in the numbers he dialed, since he communicated that information to his telephone company.

Then, in United States v. Knotts, questions surfaced regarding the propriety of police monitoring using a “beeper,” a radio transmitter device. In Knotts, police, with the consent of the seller, placed a beeper in a container of chloroform that was subsequently sold to the defendant who they suspected of using the chemicals to manufacture illegal drugs. Police observed the sale and transfer of the container to a car, and they maintained contact, relying both on visual surveillance (following the car that contained the chloroform container as it traveled across the public highways and ultimately to the defendant’s cabin), and a monitor which received the beeper signals. The Court found that the beeper surveillance amounted “to the following of an automobile on public streets and highways.” The police thus obtained information that the defendant voluntarily conveyed through his movements in public, which entitled him to no expectation of privacy. The Court also noted that there was no indication that the beeper was used in any way to reveal information about the movement of the container within the cabin, or information

113 Id. at 737.
114 Id. at 742.
115 Id.
117 Id.
118 Id. at 278.
119 Id.
120 Id. at 281.
that would not have been visible to the naked eye from outside the cabin.\footnote{Id. at 281–82.} The police then did not need a warrant to use the beeper, since no “search” had occurred.\footnote{Id. at 279–80.}

One year later, on nearly identical facts, the Court in \textit{United States v. Karo} revisited law enforcement’s warrantless use of a beeper.\footnote{468 U.S. 705 (1984).} Like \textit{Knotts}, the container in \textit{Karo} contained a beeper device previously attached with the consent of the original owner.\footnote{Id. at 707. Consistently, the Court held the mere transfer of the container to the defendant was not a search nor seizure because it did not convey any information that the defendant wished to keep private and did not reveal information that could not have been obtained through visual surveillance. \textit{Id. at 712}.} But, in \textit{Karo}, the defendant brought the container into various private residences, and the beeper signal identified the homes that the container had visited.\footnote{Id. at 714.} It was this information that police then used to obtain a warrant, which ultimately led to a search of the homes that revealed illegal drug operations.\footnote{Id. at 719.} Recall that in \textit{Knotts}, the record indicated the police limited the use of the beeper to only when they followed the defendant along public streets and not when the container arrived in its final location and transferred to the cabin.\footnote{Knotts, 460 U.S. at 281–82.} In \textit{Karo}, the police established the location of the beeper inside private residences, information gained from inside the home, and thus information that police would normally need a warrant to obtain.\footnote{Karo, 468 U.S. at 715.} Logically, since entering a private residence is a search, so too was the use of the tracking device inside the residence.\footnote{Id. at 715–16.}

\textit{Kyllo v. United States} presented the Court with the use of a then-novel thermal imagining device.\footnote{533 U.S. 27 (2001).} In \textit{Kyllo}, police suspected that the defendant was growing marijuana plants inside his home, which
normally requires a high-intensity heat lamp. Law enforcement, positioned on a public street nearby, used an advanced thermal imaging device that gathered information about the temperature inside the defendant’s home. This device allowed police to assess whether the amount of heat that flowed from the home was consistent with the use of marijuana grow lamps. The reading from the device showed high levels of heat, and police obtained a warrant to search the home based, in part, on this information. The Court held that when the government “uses a device that is not in general public use” to permeate the walls of the home and find out details it could not know without a physical intrusion, the surveillance constitutes a Fourth Amendment search and requires a warrant. The government thus may not use technology to observe the inside of the home, even if it does so from a location open to the public.

Harmonizing these three cases, a strong distinction emerged. Whether a search occurs turns on whether police could have obtained that information through ordinary visual surveillance (i.e.—monitoring movements in public areas, which does not require a warrant), or if police could not obtain such information through visual surveillance, because the monitoring occurred in a location that it could not access without a warrant (i.e.—the inside of a private residence).

The Court next turned to GPS tracking. In 2012, all nine Justices unanimously agreed in United States v. Jones that a GPS monitoring device attached to the bottom of the defendant’s car was a search, and its use without a warrant violated the Fourth Amendment. While all

131 Id. at 29.
132 Id. at 29–30.
133 Id. at 30.
134 Id.
135 Id. at 34.
136 See id. at 34–35.
139 United States v. Jones, 565 U.S. 400 (2012). In a notable moment during oral argument, arguing on behalf of the United States, the Deputy Solicitor General
nine agreed that the police’s attachment of the GPS device on the car and subsequent tracking of the car’s movements for 28 days in public constituted a search, they disagreed as to why. Five Justices deviated slightly with the Court’s almost exclusive reliance on the *Katz* framework for resolving Fourth Amendment cases and couched its holding in the government’s physical trespass on the defendant’s property consistent with the historical common-law trespass test.

The four Justices that signed on to the majority opinion explained, the government, by attaching the GPS device, “occupied private property for the purpose of obtaining information.” This narrow basis alone was sufficient to decide the case, because such “a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.” Four Justices concurred in judgment, but disagreed with the majority’s reliance on the trespass theory. Justice Alito wrote on behalf of the four concurring Justices, arguing the Court should have applied *Katz* and held more broadly that, “reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle

indicated that his theory, which permits attachment of devices to monitor a car’s movement on public roadways, applies equally to the Justices. Oral Argument at 7:02–7:50, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259), https://www.oyez.org/cases/2011/10-1259. Chief Justice Roberts, taken aback, inquired “so you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?” Id. The Deputy Solicitor General responded in the affirmative, an unpopular concession. *Id.* The *Jones* colloquies demonstrate that arguments personal for the Justices when they imagine themselves in the shoes of the target. It may be wise for advocates to keep this consideration in mind, as questions regarding the constitutionality of Stingray devices will undoubtedly reach the Supreme Court in due time.

140 *Jones*, 565 U.S. at 404.
141 *Id.* at 404–05 (majority opinion). Justice Sotomayor provided the fifth vote.
142 *Id.* at 415 (Sotomayor, J., concurring).
143 *Id.*
144 *Id.* at 419 (Alito, J., joined by Ginsburg, Breyer, Kagan, JJ., concurring in judgment).
[the defendant] drove."\textsuperscript{145} Justice Sotomayor joined the majority’s trespass holding, but she also agreed with the four concurring Justices, that the long-term surveillance violated the defendant’s reasonable expectation of privacy.\textsuperscript{146} Significantly, then, all five concurring Justices emphasized the heavy weight the expectation of privacy analysis should carry in an era where physical intrusion is no longer necessary to many forms of modern government surveillance.\textsuperscript{147}

Nonetheless, the Jones Court reaffirmed that the trespass test is not the exclusive test.\textsuperscript{148} “Situations involving merely the transmission of electronic signals without trespass,” it stated, “would remain subject to Katz analysis.”\textsuperscript{149} Under the Katz framework, a court can thus find a Fourth Amendment violation has occurred when police track movements through electronic signals if the individual has a reasonable expectation of privacy in the thing or place searched.\textsuperscript{150}

Most recently, in Riley v. California, the Court broke with its long-standing categorical rule, that under the search-incident-to-arrest exception to the warrant requirement, police need not obtain a warrant to search “personal property immediately associated with the person of the arrestee.”\textsuperscript{151} The Riley Court unanimously held that police must

\textsuperscript{145} Id. at 419.
\textsuperscript{146} Id. at 415 (Sotomayor, J., concurring) ("I agree . . . that, at the very least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.’").
\textsuperscript{147} The concurring Justices rightfully warned that “the Court’s reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact . . . .” Id. at 426 (Alito, J., dissenting); id. at 415–418 (Sotomayor, J., concurring). The majority in Jones responded to these concerns, acknowledging, “[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.” Id. at 412 (majority opinion).
\textsuperscript{148} Id. at 411.
\textsuperscript{149} Id. (alternation in the original) (emphasis omitted).
\textsuperscript{150} See id.
\textsuperscript{151} 134 S. Ct. 2473, 2490 (2014).
obtain a warrant to search the contents of an arrestee’s cellphone seized incident to arrest.152

Tugging at the seams of Riley are countless references to “the pervasive nature of smartphone technology, its “immense storage capacity,” and the bountiful applications that manage “detailed information about all aspects of a person's life.”153 Unsurprisingly, the Court rejected California’s proposed test, which would allow officers to search, incident to an arrest, cellphone data if they could have obtained the same type of information from a pre-digital counterpart.154 Given the sophisticated functionality of most modern cellphones, the Court indicated that the pre-digital analogue test would lead to a “significant diminution in privacy rights” because it lacked meaningful limits.155 The test would permit police to search not only a vast quantity of information but also an unwarranted array of information. Just because a pre-digital era search could have turned up a couple of photographs in an arrestee’s wallet or a bank statement tucked away in a pocket, it did not justify “a search of thousands of photos in a digital gallery” nor “a search of every bank statement from the last five years.”156 The test would also allow police to search a range of items contained on a phone, even though an individual is unlikely to carry that information in physical form.157 It is highly suspect that individuals would walk around with physical copies of photos and financial records, all jammed in their pockets. Yet because each of these has a pre-digital analogue, they would be fair game.158 The Court stated that determining whether a pre-digital counterpart existed would “launch courts on a difficult line-drawing expedition to

152 Id. at 2490.
153 Id. at 2484–95.
154 Id. at 2493.
155 Id.
156 Id.
157 Id.
158 Id.
determine which digital files are comparable to physical records” and “keep defendants and judges guessing for years to come.”

At the heart of Riley is the Court’s realization that the rules from the pre-digital era are not so readily transferable to cellphones. Particularly, the possible intrusion on privacy with cellphones is not constrained by physical limitations:

A cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

Undeniably, Jones and Riley both illustrate the Court’s genuine and growing concern with privacy rights under the Fourth Amendment considering sophisticated capabilities of surveillance technology continue to evolve with breakneck speed.

Before turning to United States v. Patrick, this Part concludes with a discussion on Utah v. Strieff. Though not an electronic surveillance case, the Court shed light on the contours of the exclusionary rule in Strieff, a decision that the Seventh Circuit extended in Patrick.

B. Utah v. Strieff

Though the Court has generally held that officers must articulate proper justification for stops aimed at gathering evidence, it has also recognized exceptions. One exception, the “attenuation doctrine,”

---

159 Id. The Court illustrated the unworkable nature of the test when it questioned, “Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip?” Id. The test also lacked any meaningful predictability, because “[i]t is not clear how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule after the fact.” Id.

160 Id. at 2491.

permits the use of evidence against individuals even when discovered through misconduct if the connection between the misconduct and discovery of evidence is sufficiently weak.\textsuperscript{162} Consistent with the exclusionary rule’s deterrence objectives,\textsuperscript{163} the attenuation doctrine “mark[s] the point at which the discovery of evidence becomes so attenuated from the police misconduct that the deterrent benefit of exclusion drops below its cost.”\textsuperscript{164}

In Strieff, a police officer stopped the defendant after he observed him leave a home that he suspected might contain drug activity.\textsuperscript{165} During the stop, the officer asked the defendant for identification and to explain what he was doing inside that home.\textsuperscript{166} The officer relayed the defendant’s identification information to a police dispatcher, who informed him that the defendant had an outstanding arrest warrant for a traffic violation.\textsuperscript{167} The officer then arrested the defendant pursuant to that warrant.\textsuperscript{168} He also performed a search incident to the arrest and found methamphetamine in the defendant’s pockets.\textsuperscript{169}

The State of Utah conceded that the initial stop was illegal because the officer lacked the requisite suspicion for the stop, but that the subsequent arrest was lawful because it was performed after he discovered the defendant’s outstanding arrest warrant.\textsuperscript{170} It thus argued that the officer’s discovery of the defendant’s valid arrest warrant attenuated the connection between the unconstitutional investigatory stop and the illegal drugs found in the defendant’s possession during the lawful arrest.\textsuperscript{171} The defendant argued that if the attenuation doctrine applied, it would “create a powerful incentive for police

\textsuperscript{162} Id.
\textsuperscript{163} Id. at 2063.
\textsuperscript{164} Id. at 2071 (Kagan, J., dissenting).
\textsuperscript{165} Id. at 2059–60 (majority opinion).
\textsuperscript{166} Id. at 2060.
\textsuperscript{167} Id.
\textsuperscript{168} Id.
\textsuperscript{169} Id.
\textsuperscript{170} Id.
\textsuperscript{171} Id.
officers to walk up to people on the street and simply stop them.”172 He maintained that the exclusionary rule should apply to exclude the drug evidence discovered as a result of the illegal stop.173

After analyzing the “temporal proximity” and “the presence of intervening circumstances” factors, the Court in Strieff moved to discuss the final factor of the attenuation doctrine test, “the purpose and flagrancy of the official misconduct.”174 The purpose and flagrancy factor reflects the deterrence rationale of the exclusionary rule by “favoring exclusion only when the police misconduct is most in need of deterrence—that is, when it is purposeful or flagrant.”175 When police exhibit deliberate, reckless, or a grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion becomes strong enough to outweigh the resulting costs.176

Looking to the facts, the Court found that the officer made “good faith” mistakes, and was “at most negligent” in his decision to initiate the unlawful stop of the defendant.177 The facts did not rise to the level of flagrant misconduct the Court found in Kaupp v. Texas, where police carried out a warrantless search “some of whom, at least, were conscious that they lacked probable cause.”178 And while the purpose and flagrancy factor considers whether the misconduct was “calculated” to procure the evidence,179 the Court found that the officer in Strieff did not seek to initiate a fishing expedition when he stopped the defendant.180 Notably, the Court added “there [was] no

173 Strieff, 136 S. Ct. at 2064.
174 Id. at 2061.
175 Id. at 2063.
177 Strieff, 136 S. Ct. at 2063.
179 Strieff, 136 S. Ct. at 2066 (Sotomayor, J., dissenting) (citing Brown v. Illinois, 422 U.S. 590, 603–04 (1975)).
180 Id. at 2064 (majority opinion).
indication that this unlawful stop was part of any systemic or recurrent police misconduct.”

Though it recognized a prevalence of outstanding warrants in various jurisdictions, it was unpersuaded that the mere suspicion of an outstanding warrant would lead police to conduct dragnet searches without cause. The Court ultimately held that the officer’s discovery of the valid outstanding warrant attenuated the connection between the unconstitutional stop and the evidence found during the later lawful arrest.

Undeniably, the majority opinion diluted the deterrent effect of exclusionary rule. Pre-Strieff, an officer that wanted to stop an individual without any reasonable suspicion may have hesitated to consider the effect of the unlawful investigatory stop on the admissibility of any evidence discovered. But, Strieff tells an officer he need not think twice. Post-Strieff, an officer is more likely to make a stop even if he or she lacks reasonable suspicion because the stop “may well yield admissible evidence.”

Both the majority and dissent in Strieff agreed that the role of deterrence is the gravamen of the exclusionary rule; they simply parted on whether the circumstances in Strieff called for its application. The majority believed that the fear of being held civilly liable should serve as an effective deterrent against the temptation of dragnet searches. Evidence of such conduct, however, is not always readily available, and Strieff opened the door for courts to chisel away at the remedy that the exclusionary was designed to afford.

181 Id.
182 Id.
183 Id.
184 Id.
185 Id. at 2064 (majority opinion).
IV. UNITED STATES V. PATRICK

A. Background Facts

On October 28, 2013, Milwaukee Police Department (“MPD”) officers arrested Damian Patrick while he was in his car on a public street. During the arrest, police found a gun in Patrick’s possession. Patrick was subsequently federally prosecuted as a felon in possession of a firearm under 18 U.S.C. § 922(g)(1).

During the time of his arrest, Patrick had two outstanding warrants. He was on parole, and a warrant was issued for his arrest because he failed to comply with the terms of his probation. To find Patrick, the MPD obtained a location tracking warrant, which authorized them to locate Patrick using cellphone data. But, the MPD did not locate Patrick by receiving coordinates from Patrick’s cellphone provider as the warrant authorized. After Patrick filed his opening brief in his appeal, amicus raised the question of whether the government used a Stingray to locate him. Only then—a year and a half after Patrick’s arrest—did the government admit that the MPD used a Stingray to gather data to pin down his location for the arrest.

---

186 United States v. Patrick, 842 F.3d 540, 541 (7th Cir. 2016);
187 Patrick, 842 F.3d at 541.
188 Id.
189 Id. at 542.
190 Id.
191 Id. This Note refers to the October 27, 2013 state court order, which authorized the disclosure of the location information associated with Patrick’s cellphone and the three approved surveillance methodologies to aid police in effectuating the arrest for the violation of parole warrant collectively as the “location tracking warrant.” See infra Section IV.B.
192 Id.
193 Id. at 546 (Wood, C.J., dissenting); Appellant’s Reply Brief at 11, United States v. Patrick, 2016 WL 2848759 (7th Cir. May 12, 2016) (No. 15-2443).
194 Patrick, 842 F.3d at 542; Appellant’s Reply Brief, supra note 193, at 11 (“In a letter . . . dated March 17th, 2016, the government confirmed that a Stingray was in fact used to track and locate Mr. Patrick.”).
B. The Location Tracking Warrant

So, what exactly did that second warrant authorize police to do? On October 27, 2013, based on an application submitted by the Milwaukee Assistant District Attorney and the supporting affidavit of a Milwaukee Police Officer, Milwaukee County Circuit Court Judge Stark found sufficient probable cause to issue an order that authorized the disclosure of location information for a cellphone that was known to be used by Patrick. Judge Stark’s order found sufficient probable cause to authorize the release of “cellular tower activity, cellular tower location, cellular toll information and cellular telephone global positioning system (GPS) location information, if available, that will permit identification of the physical location of the target cellular phone.” Judge Stark approved (1) the installation and use of a trap and trace device, (2) the installation and use of a pen register device, and (3) the release of cell-site location information related to the target cell phone.

The order also instructed Sprint, Patrick’s carrier, to provide the cell-site location information from July 27, 2013, to the date the order was signed and extending sixty days thereafter. As such, the order indicated the manner in which law enforcement was to collect the cell-site information. Specifically, it ordered Sprint, to provide cell-site location information, instructing “such service provider . . . shall initiate a signal to determine the location of the subject’s mobile phone.”

---

195 United States v. Patrick, No. 13-CR-234, 2015 WL 106158, at *2–*3 (E.D. Wis. Jan. 7, 2015), aff’d, 842 F.3d 540 (7th Cir. 2016) (Order Denying Motion to Suppress). In the order, the district court thoroughly described the contents of the October 27, 2013 state order, including the details of the application submitted by the Milwaukee Assistant District Attorney and the supporting affidavit of a Milwaukee Police Officer. This Note does not detail these documents or the facts each advanced to establish probable cause, as it does not bear on the Seventh Circuit’s analysis.

196 Id. at *2.

197 Id. at *3.

198 Id.

199 Patrick, 842 F.3d at 549 (Wood, C.J., dissenting).
device on the service provider’s network or with such other reference points as may be reasonably available . . .”

C. Patrick’s Motion to Suppress & Procedural Background

The facts leading to Patrick’s appeal are convoluted, largely because the government disclosed the truth of the Stingray’s use in drawn out phases. At the outset, three officers prepared reports concerning their involvement in Patrick’s arrest. In the reports, they indicated that they either: (1) “obtained information” of Patrick’s location; (2) had “prior knowledge” that Patrick was occupying the vehicle, which officers observed while on patrol; and (3) “obtained information from an unknown source” that Patrick was inside the vehicle at that location.

On January 11, 2014, Patrick filed his first motion to suppress the gun that MPD found in his possession, arguing that the MPD seized him unlawfully without reasonable suspicion. Then, during an evidentiary hearing on February 4, 2014, officers testified that they did not locate Patrick on an anonymous tip, revealing, for the first time, that they located Patrick by tracking his cellphone. Based on this new information, Patrick withdrew his initial motion and filed a new motion on August 1, 2014, arguing that the state order authorizing police to obtain the location of his cellphone did not amount to a warrant under the Fourth Amendment because the order lacked the requisite probable cause to track his phone in real time to determine his location.

---

200 Id.
201 Patrick, 2015 WL 106158, at *2
202 Id. at *2 & n.1.
203 Id. at *1.
204 Id. at *2.
205 Id. at *2; Brief for Appellant at 7, United States v. Patrick, 2016 WL 211768 (7th Cir. Jan. 15, 2016) (No. 15-2443); see also Patrick, 2015 WL 106158, at *3.
On January 7, 2015, the district court adopted the magistrate judge’s recommendation in full and denied Patrick’s motion to suppress the gun evidence. The court found that Judge Stark had a “substantial basis” for concluding that probable cause existed for the order she issued authorizing the disclosure of the location information related to Patrick’s cellphone. What to make of the fact that the order did not mention a Stingray? Not necessary, said the district court. Because the order complied with the three requirements of the warrants clause of the Fourth Amendment, it effectively served as a warrant, so “no further authorization was required for the government to track Patrick’s cellphone.”

Patrick then conditionally pled guilty to the unlawful possession of a firearm charge, but he reserved the opportunity to contest the district court’s denial of his motion to suppress. He received a 57-month sentence on June 29, 2015, and he subsequently filed a notice of appeal on July 8, 2015.

In his opening brief in his appeal to the Seventh Circuit, Patrick argued that the location tracking warrant did not contain the requisite probable cause to authorize the tracking of the cellphone, and accordingly, that the gun that police found as a result of the illegal tracking should be suppressed. Amicus then raised the possibility that the government used a Stingray to locate Patrick, and on March 17, 2016, the government confirmed that police did in fact use a Stingray to track and locate Patrick. Apparently, months before Patrick’s arrest, the MPD signed a non-disclosure agreement (“NDA”)

206 Patrick, 2015 WL 106158, at *1. At the time of the district court’s ruling on Patrick’s August 1, 2014 motion to suppress, the government readily acknowledged that law enforcement determined Patrick’s location on October 28, 2013, by tracking his cell phone. Id. at *2 & n.1.
207 Id. at *7.
208 Id. at *7
209 Id.
210 United States v. Patrick, 842 F.3d 540, 541 (7th Cir. 2016).
211 Id.; Brief for Appellant, supra note 205 at 7.
212 Patrick, 842 F.3d at 541; see also Brief for Appellant, supra note 205.
213 Appellant’s Reply Brief, supra note 193, at *11.
with the Federal Bureau of Investigations ("FBI").\textsuperscript{214} Per the agreement, the MPD must keep secret information about the Stingray in “pre-trial matters, search warrants and related affidavits, discovery, in response to court ordered disclosure and other affidavits, and on appeal.”\textsuperscript{215}

Patrick then argued in his reply brief that should the Seventh Circuit not order the evidence suppressed, based on the nature of his conditional plea, the court should remand the case to the district court to accept additional briefing on the government’s use of Stingray.\textsuperscript{216} This new information invoked the question of whether the Stingray’s use constituted a warrantless search outside the scope of the state location tracking warrant, and whether suppression of the gun was proper.

\textit{D. The Seventh Circuit’s Decision}

A divided panel of the Seventh Circuit held the fact that police used a Stingray to track and locate Patrick for the arrest did not justify application of the exclusionary rule.\textsuperscript{217} Accordingly, the court affirmed the district court’s denial.\textsuperscript{218} Judge Easterbrok, writing for the majority, concluded it need not resolve the issues posed by the police’s use of the Stingray.\textsuperscript{219} The majority saw this case plain and simple: Patrick was arrested in public, based on probable cause, and pursuant to a valid arrest warrant, all of which sufficed to render the arrest and incident search lawful.\textsuperscript{220} Because police arrested Patrick in a public place, they were entitled to arrest him based on probable cause alone; this made any deficiencies in the location tracking warrant immaterial.

\textsuperscript{214} Id. at *12
\textsuperscript{215} Id. As an employee of the MPD, the police officer who prepared the supporting affidavit for the location tracking order was bound to the agreement.
\textsuperscript{216} Id. at *11–*16.
\textsuperscript{217} Patrick, 842 F.3d at 545.
\textsuperscript{218} Id.
\textsuperscript{219} Id. at 542.
\textsuperscript{220} Id.
because under the circumstances, police were entitled to arrest Patrick without any kind of warrant.\textsuperscript{221}

The majority also held that \textit{Utah v. Strieff} independently supported its conclusion that suppression was improper.\textsuperscript{222} It interpreted \textit{Strieff} to hold that “a valid arrest warrant precludes the suppression of evidence seized in an arrest, even if the arrest was set in motion by officers who had neither probable cause nor knowledge of the warrant.”\textsuperscript{223} Patrick’s valid outstanding warrant was issued before any of the police’s efforts to learn his location, and so “their efforts could not taint the arrest ‘in the parlance of the exclusionary rule.’”\textsuperscript{224}

The majority acknowledged that no other court of appeals has yet to address questions about whether (1) the use of a cell-site simulator is a search, (2) if the use of a Stingray is a search, whether a warrant must authorize its use. While it stated it would be “best to withhold full analysis until these issues control the outcome of a concrete case,” it nonetheless proceeded to weigh in.\textsuperscript{225}

The government had conceded for purposes of the case only that the use of a Stingray was a search.\textsuperscript{226} Still, the majority recapped Supreme Court precedent and said it could go either way.\textsuperscript{227} The majority raised the possibility that the use of a cell-site simulator could fall under the \textit{Smith v. Maryland} and \textit{United States v. Knotts} framework and thus not a search.\textsuperscript{228} It also then recognized \textit{Jones} provided a contrary line of arguments that analogized cell-site

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{221} \textit{Id.} at 542.
\item\textsuperscript{222} \textit{Id.} at 542 (citing \textit{Utah v. Strieff}, 136 S. Ct. 2056 (2016)).
\item\textsuperscript{223} \textit{Id.}
\item\textsuperscript{224} \textit{Id.}
\item\textsuperscript{225} \textit{Id.}
\item\textsuperscript{226} \textit{Id.}
\item\textsuperscript{227} \textit{Id.} at 544.
\item\textsuperscript{228} \textit{Id.} at 543 (majority opinion) (first citing \textit{Smith v. Maryland}, 442 U.S. 735, 1979); then citing \textit{United States v. Knotts}, 460 U.S. 276 (1983)). The majority also cited to recent decisions of the Fourth Circuit in \textit{United States v. Graham} (824 F.3d 421 (4th Cir. 2016) (en banc)) and the Sixth Circuit in \textit{United States v. Carpenter} (819 F.3d 880 (6th Cir. 2016)), which held that “tracking a person via data from phone companies is not a search within the scope of the Fourth Amendment.” \textit{Id.}
\end{itemize}
\end{footnotesize}
simulators to GPS locators.\textsuperscript{229} It acknowledged that all five concurring Justices suggested that the use of such devices may be searches when used for extended durations,\textsuperscript{230} and thus if the concurring approaches are adopted, it would be necessary to know how long the police used the Stingray to track Patrick.\textsuperscript{231} Lastly, it alluded that the Stingray’s degree of precision would bear a significance: “is it information that leaves uncertainty about where in several city blocks a suspect may be, such as the beeper in \textit{Knotts}, or is it closer to the precise location supplied by a GPS tracker [in \textit{Jones}]?”\textsuperscript{232}

With respect to the warrant, Patrick and the United States disagreed on the significance of the fact that police did not reveal to the state judge who issued the location tracking warrant that it planned to use a cell-site simulator.\textsuperscript{233} Patrick raised two challenges regarding the warrant and the government’s lack of candor.\textsuperscript{234} First, he argued that “leaving the judge in the dark (perhaps misleading the judge by omitting a potentially material fact) made the location-tracking warrant invalid.”\textsuperscript{235} Patrick’s position was that the issuing judge was entitled to know that the police intended to use a cell-site simulator and accordingly authorize that method as part of the warrant.\textsuperscript{236} This kind of restriction focuses on \textit{ex ante} limitations, which refer to attempts to regulate the search before it occurs.\textsuperscript{237} The majority

\begin{itemize}
\item \textsuperscript{229} \textit{Id.} at 544 (citing United States v. Jones, 565 U.S. 400 (2012)).
\item \textsuperscript{230} \textit{Id.} (first citing \textit{Jones}, 565 U.S. at 415 (Sotomayor, J., concurring); then citing \textit{Jones}, 565 U.S. at 425–30 (Alito, J., concurring)).
\item \textsuperscript{231} \textit{Id.}
\item \textsuperscript{232} \textit{Id.} (first citing \textit{Knotts}, 533 U.S. 27; then citing \textit{Jones}, 565 U.S. 400)).
\item \textsuperscript{233} \textit{Id.}
\item \textsuperscript{234} \textit{Id.} at 544–45.
\item \textsuperscript{235} \textit{Id.} at 544 (internal brackets omitted).
\item \textsuperscript{236} \textit{Id.}
\item \textsuperscript{237} The gist of the position on \textit{ex ante} restrictions is as follows: Perhaps you will sign the warrant only if the FBI agents agree to use a particular search protocol. Or . . . only if the government agrees to minimize the seizure of the suspect's hardware or if the government agrees to waive any rights to seize any items discovered in plain view outside the warrant. Whatever restriction you choose, the goal is to protect the Fourth
\end{itemize}
concluded that neither constitutional text nor precedent supports *ex ante* regulations; rather, it forbids such restrictions and confines the judiciary only to the *ex post*, after-the-fact, assessments of whether a search warrant was reasonable.  

Second, and closely related, Patrick argued that even if *ex ante* authorization of the method was unnecessary, the government must be candid when they mention methods of executing a search warrant. He sought to remand the case to explore these issues “after the fashion of a *Franks* hearing at which the court would decide whether the warrant still would have issued if the affidavits had been more forthcoming.” The majority rejected further exploration of these issues, because it found the answers to those questions were not dispositive to the case based on the factual circumstances. Patrick was arrested in a public place, and the arrest was supported by both probable cause and a valid arrest warrant issued before any effort to learn his location; therefore, the police’s subsequent effort to learn his location could not taint the arrest. The majority thus found it would be inappropriate to apply the exclusionary rule, “even if the police should have told the judge that they planned to use a cell-site simulator

---

Amendment *ex ante*: you can best protect the Fourth Amendment by imposing conditions when you issue the warrant on how it later will be executed.


---

238 Patrick, 842 F.3d at 544–45 (citing Kerr, *supra* note 237, at 1260–71).

239 *Id.* at 545.

240 *Id.* (citing Franks v. Delaware, 438 U.S. 154 (1978)). Under *Franks v. Delaware*, the defendant “must make a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit.” 488 U.S. at 156. See Justin Brown & Kasha M. Leese, *Stingray Devices Usher in A New Fourth Amendment Battleground*, 39 CHAMPION 12, 17 (June 2005), for a persuasive argument on how defendants can utilize *Franks* as a lifeline.

241 Patrick, 842 F.3d at 545.

242 *Id.* at 542, 545.
to execute the location warrant.”

In sum, the majority concluded that because the arrest was lawful, which rendered the gun seized admissible, it need not definitely resolve any issues Patrick raised regarding the police’s use of the Stingray.

Chief Judge Wood dissented, characterizing the case more about how police found Patrick rather than where they found him.”

Chief Justice Wood argued that the record was factually “fatally inadequate” on the use of the Stingray and the intricacies the device.

She argued this precluded a meaningful resolution of whether police violated Patrick’s Fourth Amendment rights, because questions posed by the police’s use of the Stingray affected whether Patrick’s initial arrest was valid.

If it was invalid, then the gun that the police spotted in plain view in the car should have been suppressed.

Chief Judge Wood would have thus remanded the case for further fact-finding.

IV. THE IMPLICATIONS OF THE SEVENTH CIRCUIT’S “BLISSFUL IGNORANCE” / IMPLICATIONS OF THE DECISION & STINGRAY TECHNOLOGY

The remainder of this Note focuses its analysis on three key points implicated by the Seventh Circuit’s decision in Patrick. Section A discusses the holding regarding Utah v. Strieff. Section B then examines the court’s discussion on whether the use of a Stingray devices constitutes a search under the Fourth Amendment. Section C looks to the court’s stance on whether the use of the Stingray exceeded

---

243 Id. at 545.
244 Id. at 542, 546.
245 Id. at 545 (Wood, C.J., dissenting) (“This case raises serious issues about the use of cell-site simulators to track down the location of a target person.”).
246 Id.
247 Id. at 546–47, 549, 552.
248 Id. at 546.
249 Id. at 552.
250 Chief Judge Wood also discussed Title III, though this Note does not address her argument on that issue in detail.
the scope of the location tracking warrant and whether a warrant that specifically authorizes the use a cell-site simulator is necessary to constitute a valid warrant under the Fourth Amendment.

A. The Majority’s Uncomfortable Extension of Utah v. Strieff

The majority’s interpretation expanded Strieff to hold that the mere existence of an outstanding warrant attenuates the police officer’s illegal conduct from the items subsequently seized. But, Strieff requires more than just an intervening event. As Chief Judge Wood pointed out in dissent, Strieff rests on a break in the casual chain that attenuates Fourth Amendment concerns from the officer’s initial illegal actions and the subsequent search. The Strieff Court indicated that necessary to its reasoning was not only a valid warrant that predated the officer’s investigation, but that the warrant “was entirely unconnected with the stop,” and that the officer’s decision to arrest the defendant was “a ministerial act that was independently compelled by the pre-existing warrant.” This is factually inapposite to the facts in Patrick. The Stingray was wholly connected—indeed, police intentionally used the device to effectuate Patrick’s arrest.

Subtly, the majority extrapolates from Strieff, “if the police had stopped Patrick’s car for no reason at all and learned only later that he was a wanted man, the gun would have been admissible in evidence.” This conclusion facilitates the very concerns the defendant in Strieff raised. In general, the court’s interpretation as written essentially gives law enforcement carte blanche to conduct searches, so long as they find incriminating evidence after the fact. In

251 Patrick, 842 F.3d at 542 (majority opinion).
253 Patrick, 842 F.3d at 549–50 (Wood, C.J., dissenting) (citing Strieff, 136 S. Ct. at 2060 (2016)).
254 Id. (citing Strieff, 136 S. Ct. at 2062).
255 Id. The MPD’s arrest of Patrick and the search that led to the gun was also not a ministerial act. Id.
256 Id. at 542 (majority opinion) (citing Strieff, 136 S. Ct. 2060).
the factual context of *Patrick*, it insinuates that law enforcement can utilize whatever means it deems fit to locate an individual, regardless of what a warrant authorizes, because the mere existence of the individual’s outstanding arrest warrant will attenuate the connection between illegal Fourth Amendment conduct and evidence seized.\textsuperscript{257}

The majority also ignored that the Court held in *Strieff* as it did because there was no evidence of purposeful or flagrant police misconduct; rather, the officer in *Strieff* was merely negligent when he conducted the unconstitutional investigatory stop.\textsuperscript{258} The record in *Patrick* lacked facts to conclude that the MPD’s conduct was simply mere negligence.\textsuperscript{259} The record quite oppositely indicated that “police knew what they were doing.”\textsuperscript{260} Facts of possible concealment of intent to use a cell-phone stimulator or knowledge of exceeding the scope of the warrant would rise to the level of flagrance or misconduct that *Strieff* specifically carved out.

As *Strieff* demonstrated, the exclusionary rule rests primarily—if not solely—on the role of deterrence, a consideration wholly absent in the Seventh Circuit’s analysis. The majority tossed aside any meaningful culpability on MPD’s part, rationalizing that although the MPD purposefully concealed their intent to use a cell-site simulator, and misrepresented to the state judge that they would use phone company data to locate Patrick, “[a] fugitive cannot be picky about how he is run to ground.”\textsuperscript{261} Even if one agrees with the majority, that the circumstances of Patrick’s arrest (in public, with probable cause and pursuant to an arrest warrant) did not justify the exclusionary rule, the majority remains at fault for its failure to offer discussion on the role of deterrence as to the MPD’s misleading conduct.\textsuperscript{262}

\textsuperscript{257} *Id.* at 545.
\textsuperscript{258} *Strieff*, 136 S. Ct. at 2064.
\textsuperscript{259} *Id.*
\textsuperscript{260} *Patrick*, 842 F.3d at 550 (Wood, C.J., dissenting).
\textsuperscript{261} *Id.* at 545.
\textsuperscript{262} Admittedly, the NDA signed by the MPD affected its candor, but this Note offers no opinion on how this should impact the purpose and flagrancy factor analysis. This Note rather argues the majority should have acknowledged that *Strieff* tolerates negligence, while the MPD remained conscious of their deception. The
B. Is the Use of a Stingray Device a “Search” Under the Fourth Amendment?

Although the United States conceded that the use of a Stingray constituted a search in Patrick, the Seventh Circuit discussed, but did not definitively resolve, whether the use of a cell-site simulator constitutes a search under the Fourth Amendment. 263 To be fair, the Seventh Circuit did not need to resolve the issue. But, the court also lacked the requisite facts to offer a fair assessment both generally and in Patrick’s case. Still, it weighed in, and in doing so, made unwarranted factual assumptions.

The majority cited to a Department of Justice Policy Guideline on the use of cell-simulator technology (”DOJ Policy Guidance”), which states the Department must configure a cell-site simulator as a pen register. 264 The majority said a Stingray would then resemble the kind of pen register used in Smith, because it would not reveal communicative content, 265 and also the beeper in Knotts, because it would obtain only location information and nothing else. 266 First, the DOJ Policy Guidance is not binding on local law enforcement agencies like the MPD. 267 MPD used the Stingray, not the Department, so that renders any guarantees made in the DOJ Policy Guidance immaterial. Second, the DOJ Policy Guidance did not provide any detail on the Stingray or its capabilities, just that one must configure it as a pen register as to not catch “emails, texts, contact lists, images or

majority should have seen “purposeful evasion of judicial oversight of potentially illegal searches as exactly the kind of police misconduct most in need of deterrence.” 263 Id. at 550 (Wood, C.J., dissenting) (quoting Strieff, 136 S. Ct. at 2063).

264 Id. at 544 (majority opinion)
265 Id. at 542–53 (citing DOJ Policy Guidance, supra note 30, at 2).
266 Id. at 543 (citing Smith v. Maryland, 442 U.S. 735 (1979)).
267 DOJ Policy Guidance, supra note 30, at 2 n.2 (“This policy guidance is intended only to improve the internal management of the Department of Justice. It is not intended to and does not create any right, benefit, trust, or responsibility . . . .”).
any other data from the phone.” Chief Judge Wood pointed out, Stingrays include exactly these capabilities, so it oversimplifies the inquiry to analogize it to a “high-tech pen register.” Depending on the features of the particular Stingray and the way it is configured, a Stingray can intercept communications as well as location data. The court in Patrick knew nothing concrete about the general extent of its surveillance capabilities or the specific way the MPD configured the Stingray in Patrick’s case. Yet, to make the analogy, the majority suggested an uninformed assumption that the location information was all that was collected because that was all that police revealed.

Regarding the beeper, the majority’s analysis only got it half right. In discussing Knotts, the majority zeroed in on the fact that a beeper does not give precise location data and rather indicates a general block where a suspect may be located. But, this was not the only reason why the Court held in Knotts that the use of a beeper was not a search. Properly read, Knotts held that no Fourth Amendment violation occurred when police used a beeper to track the movements of the container, because it revealed only location information that police also obtained simultaneously through visual surveillance. Specifically, by following the car that held the container. Crucially different is that the police in Patrick obtained the warrant to find Patrick. Police did not know where he was, so fundamentally, they could not follow him.

To the majority’s credit, it did recognize that another line of case law offers support for finding that the use of a Stingray constitutes a search. It acknowledged that one could analogize a cell-site simulator

---

268 Id. at 2.
269 Patrick, 842 F.3d at 547 (Wood, C.J., dissenting).
270 Id.
271 See id. 542–43 (majority opinion).
272 Id. at 543.
274 Id. at 281.
275 See Patrick, 842 F.3d at 542.
device to a GPS locator, which the *Jones* Court treated as a search. And per the concurring justices, the length of time police used the device and the precision of the location data collected remained relevant. It also noted technology that intrudes into the home where there is a heightened privacy interest is a search under *Kyllo*. This was the extent of the court’s analysis, however.

Though the Seventh Circuit is the first court of appeals to discuss whether the use of a Stingray device is a search, other courts have had the occasion to weigh in. As a general matter, this Note takes the position that the use of a Stingray device constitutes a search within the meaning of the Fourth Amendment. And, virtually all case law agrees. Based on Supreme Court precedent, ultimately critical to any challenge of a search utilizing stingray technology will be the nature of the Stingray technology as it implicates the manner of a search in a constitutionally protected place under *Kyllo*, the location of the target phone as *Karo* and *Kyllo* both highlighted, the length of the tracking the Court in *Jones* emphasized, and whether the Stingray searched the contents of the phone, the kind of search the *Riley* Court held required a warrant.

To begin, Stingray devices fall right on par with the thermal imaging device at issue in *Kyllo*. One cannot plausibly characterize a

---

276 *Id.* at 544 (citing United States v. Jones, 565 U.S. 400 (2012))
277 *Id.* (citing *Jones*, 565 U.S. at 954–65) (concurring opinions of Sotomayor and Alito, JJ.)
278 *Id.* (citing *Kyllo* v. United States, 533 U.S. 27 (2001)).
279 State v. Andrews, 134 A.3d 324, 350 (Md. Ct. Spec. App. 2016) (holding that the use of a cell site simulator to obtain location information directly from an individual’s cell phone is a search under the Fourth Amendment and requires a search warrant; United States v. Lambis, 197 F. Supp. 3d 606, 610 (S.D.N.Y. 2016) (holding the government use of a cell-site simulator constituted a search under the Fourth Amendment that required a warrant); States v. Tutis, No. CR 14-699 (JBS), 2016 WL 6136577, at *5 (D.N.J. Oct. 20, 2016) (same). See also *Patrick*, 842 F.3d at 543 (government conceded the use of a Stingray is a search); United States v. Rigmaiden, 844 F. Supp. 2d 982, 997 (D. Ariz. 2012) (the government conceded that the search for the aircard constituted a Fourth Amendment search).
Stingray as “in general public use.” 280 These devices are not within the general public’s reach because federal law enforcement agencies and police departments receive offers for the devices exclusively through directly mailed vendor letters. 281 And parallel to Kyllo’s thermal imagining technology, a Stingray sends electronic signals that penetrate the walls of a home, allowing police to explore the details of a home and obtain information that they could not obtain otherwise without physically intruding into the home. 282 Under this rationale, two courts have ruled that law enforcement’s use of the cell-site simulator to locate the defendant’s apartment was an unreasonable search, given the “pings” from the defendant’s cell phone to the nearest cell site were not readily available “to anyone who wanted to look” without the use of a cell-site simulator. 283

The Court has repeatedly demonstrated impatience with searches conducted in private residences that failed to comport with the Fourth Amendment. Discussing Karo and Kyllo in tandem, two scholars understand the Court’s position as follows: the “Fourth Amendment draws a line at the entrance of the house, and the line “must be not only firm but also bright which requires clear specification of those methods of surveillance that require a warrant.” 284

Though the case law weighs against finding a Fourth Amendment search when police utilize a Stingray to monitor phones in public areas, it is not so simple. A Stingray is blind to any distinction of public versus private; when utilized, it recognizes all cell phones

280 Lambis, 197 F. Supp. 3d at 610. The most basic model also costs approximately $75,000, well beyond the affordability of the public to purchase. See Andrew Hemmer, Duty of Candor in the Digital Age: The Need for Heightened Judicial Supervision of Stingray Searches, 91 CHI.-KENT L. REV. 295, 308 (2016).
281 Hemmer, supra note 280, at 308.
282 Lambis, 197 F. Supp. 3d at 610 (citing Kyllo v. United States, 533 U.S. 27, 40 (2001)).
283 Id. at 610–11 (“The use of a cell-site simulator constitutes a Fourth Amendment search within the contemplation of Kyllo.”); Andrews, 134 A.3d at 324.

408
within an area of several kilometers.285 And a reasonable assumption that follows is that at least some affected cellphones will be inside private homes. If the searches in Karo and Kyllo were Fourth Amendment violations, so too is the use of a cell-site simulator to determine a suspect’s location inside a private home, even if the Stingray limits its signals to that target.286 A court should likewise find a Fourth Amendment violation in a Stingray search that collaterally searches cellphones inside third parties’ homes as a mechanism to ascertain the target cellphone’s location.287 We must take caution to remember we are in an era where 95 percent of individuals own a cellphone.288 It is precisely such sensitivity that led the one court to conclude that “[b]ecause the vast majority of the population uses cell phones lawfully on a daily basis, one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful.”289 Compared with a canine sniff of luggage at the airport, which does not intrude upon any legitimate privacy interest since the sniff reveals nothing about non-contraband items,290 a Stingray device is a completely different animal.

The scant case law does not discuss Stingray searches under the backdrop of the “long-term tracking” issues Jones raised.291 If police know the target’s number, a Stingray search could move fast. Indeed,

286 Andrews, 134 A.3d at 324.
287 This alone would not make the Stingray’s use an overly broad search that even a warrant could not cure, but it should bear heavily on whether the Stingray’s use was reasonable under the circumstances.
288 Mobile Fact Sheet, supra note 39.
291 United States v. Jones 565 U.S. 400, 419 (Alito, J., concurring); Id. at 415 (Sotomayor, J., concurring).
in *Patrick*, the police located Patrick one day after it obtained the location tracking warrant. But, police do not always know the target’s number. For example, a suspect may rely on pre-paid disposable phones commonly known as “burner phones,” which make tracking harder, but not impossible, to track. Police would then need use the Stingray to intercept data from an unknown quantity of devices, and eventually, through a process of elimination, the collected information would provide calling and messaging patterns that identify a suspect’s phone. In this scenario, the timeline and degree of intrusiveness greatly increases.

The majority’s analysis was not only limited, but it was also selective. Nowhere did the majority mention *Riley v. California*. Though factually different than *Patrick*, *Riley* suggested that the Court would highly scrutinize Stingray searches if the device searched the contents of the phone and data to determine the target location, for after *Riley*, police must obtain a warrant to search cell-phone data. As Chief Justice Wood explained, “the location warrant authorized only methods of fixing Patrick’s location that involved gathering information that would reveal his phone’s connection with cellphone towers,” and the “authorization of the collection of location data cannot be expanded to permit a search of the contents of Patrick’s cell

---

292 United States v. Patrick, 842 F.3d 540, 541 (7th Cir. 2016).
295 *Riley v. California*, 134 S. Ct. 2473, 2485 (2014); see also id. at 2493 (“We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.”).
If the Stingray gathered information from Patrick’s phone that went beyond his location, “such a ‘search’ of his phone would have been unauthorized.” But, the court had no information on whether the Stingray gathered information that went beyond his location information and whether it searched the contents of the cellphone itself to determine the location.

In its brief discussion on the issue, the majority conveyed a strange reluctance to find, as a general matter, that the use of a Stingray constitutes a “search.” Ultimately, it did not illicit what one would hope a court would express: a strong sense of unease regarding the factual holes, especially given the intrusive nature of the devices.

C. Warrants Requirements for Stingray Searches

Patrick raised two intertwined yet distinctive challenges to the Stingray use, both of which ultimately turn on whether a judge is entitled to know how a warrant will be executed. The majority took a stance wholly deferential to law enforcement, concluding that the Fourth Amendment forbids ex ante limitations and confines the judiciary only to the ex post assessments of whether the method of execution was reasonable.

Though the majority in Patrick relied heavily on United States v. Dalia, where the Court noted “the specificity required by the Fourth Amendment does not generally extend to how warrants are executed,” Chief Judge Wood rightfully pointed out that this statement must be understood in context. The Stingray device itself was at issue in Patrick, and because of its

---

296 Patrick, 842 F.3d at 547 ((Wood C.J. dissenting) (citing Riley, 134 S. Ct. at 2494–95)).
297 Id.
298 Id.
299 Id. at 544–45 (majority opinion).
300 Id. at 544 (citing Dalia v. United States, 441 U.S. 238, 256 (1979)).
301 Id. at 548 (Wood, C.J., dissenting) (citing Dalia, 441 U.S. at 257).
sophisticated capabilities, “the way it was used could affect the scope and location of the search itself.”  

Given their novel nature, only a handful of courts have had the occasion to address questions pertaining to Stingrays and warrants requirements. United States v. Rigmaiden was one of the first cases that dealt with Stingrays. In Rigmaiden, police suspected the defendant of perpetrating a fraudulent tax scheme where he used identity data of third parties to electronically file tax returns and claim tax refunds. Police obtained a tracking warrant that authorized a “mobile tracking device” to monitor the defendant’s aircard but failed to describe the specific technology and how it would generate the signal to fix the defendant’s location. Police ultimately used a device that functioned akin to a cell-site simulator to track and locate the location of the defendant’s aircard contained in his laptop. The defendant then filed a motion to suppress the evidence police obtained through their use of this parallel device, arguing the search exceeded the scope of the warrant issued.  

It was the defendant’s position that the tracking warrant police obtained authorized not the government, but Verizon Wireless, the carrier associated with his aircard, to track and locate the aircard. He argued that the warrant directed Verizon to assist the government by operating the tracking device and turning over information

302 Id.
305 Id. *14–*15.
306 Id. The court found that “[t]he mobile tracking device used by the FBI to locate the aircard functions as a cell site simulator” and the mobile tracking device mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard. Id. at *15.
307 See Id. at *15.
308 Id. at *14.
gathered. The government also stipulated that the tracking device it used sent signals to the defendant’s aircard that Verizon would not have sent in the normal course of its operation, meaning the government would not have found the defendant solely relying on Verizon. The government also admitted that it failed to disclose in its application for the warrant that “the mobile tracking device would capture signals from other cell phones and aircards in the area of Defendant’s apartment.” This was a “detail of execution” that the court in Rigmaiden said need not be specified. Though that court itself admitted the warrant was not “a model of clarity,” it still denied the defendant’s motion to suppress because the issuing judge found the requisite probable cause to authorize the use of a tracking device.

Following Rigmaiden’s lead, a New Jersey district court in United States v. Tutis held that the while it “might have been helpful to include the words ‘cell-site simulator’ in the warrant” it was not required under the Fourth Amendment. Tutis is distinguishable from Rigmaiden, however, because the government in Tutis did specifically describe the device’s capabilities in the warrant application. It provided that the only function of equipment is to obtain the listed unique identification numbers, and it also described how the technology would obtain data points. Since this sufficiently described how the technology operated, the court found it insignificant that the warrant did not explicitly refer to a “cell-site simulator.”

310 Id. at *15.
311 Id. at *20.
312 Id.
313 Id. at *19–*20.
315 Id. at *2.
316 Id. at *2.
317 Id. at *6.
But, courts that have taken a more thorough look at the high stakes implicated by Stingray searches and have held that the use of a cell-site simulator requires a search warrant “based on probable cause and describing with particularity the object and manner of the search, unless an established exception to the warrant requirement applies.”318 In State v. Andrews, the court concluded that an order authorizing the use of a cellular tracking device to locate a suspect’s cell phone did not constitute sufficient judicial authorization to use a cell-site simulator.319 In Andrews, the police’s use of a cell-site simulator revealed information about the defendant’s residence, specifically, that the defendant’s cellphone, and logically the defendant himself, were inside.320 The court observed that cell site simulators can locate and track the movements of a cellphone and its user across both public and private spaces.321 While it acknowledged that police frequently do not know whether officers will find a target phone in a constitutionally protected space, it nonetheless found it impractical to create a rule that prohibited a warrantless search only retrospectively when the search resulted in locating the cellphone inside a home or another constitutionally protected area.322 This provides “neither guidance nor deterrence, and would do nothing to thwart unconstitutional intrusions.”323 For these reasons, the court held the government must disclose the manner of execution if it intends to use a cell-site simulator to satisfy the Fourth Amendment requirements.324

Most recently, a court applied the exclusionary rule to suppress evidence police through the use of a Stingray in United States v.

319 Id. at 355. Police obtained a pen register order and a trap and trace order, which the court in Andrews held was not the functional equivalent of a warrant for a cell-site simulator. Id. at 358.
320 Id. at 348.
321 Id.
322 Id.
323 Id. at 350.
324 Id.
Lambis.\textsuperscript{325} DEA agents in Lambis had a warrant for the defendant’s cell-site location information ("CSLI").\textsuperscript{326} The CSLI provided the agents with a specific intersection of target phone’s location.\textsuperscript{327} But, this did not identify the precise information that police needed—the defendant’s specific apartment building and thus where he was located—to make the arrest.\textsuperscript{328} So, officers used a Stingray device to obtain this information and subsequently uncovered narcotics in the defendant’s apartment.\textsuperscript{329}

The court in Lambis warned, and held that the original warrant application did not contemplate the use of a cell-site simulator, finding CSLI and cell-site similar generated location information not one in the same.\textsuperscript{330} The court rationalized that “if the Government had wished to use a cell-site simulator, it could have obtained a warrant,” adding “the fact that [the government] previously demonstrated probable cause and obtained a warrant for CSLI . . . suggests [it] could have obtained a warrant to use a cell-site simulator, if it had wished to do so.”\textsuperscript{331} The court concluded with a clear message: “[a]bsent a search warrant, the Government may not turn a citizen’s cell phone into a tracking device.”\textsuperscript{332}

In Patrick’s case, the warrant indicated that only location data was to be searched and obtained, not a search of the phone’s contents.\textsuperscript{333} If

\textsuperscript{325} United States v. Lambis, 197 F. Supp. 3d 606 (2016).
\textsuperscript{326} Id. at 608–09. The court defined CSLI as “a record of . . . location information from the service provider derived from ‘pings’ sent to cell sites by a target cell phone [which] allows the target phone’s location to be approximated by providing a record of where the phone has been used.” Id. at 608.
\textsuperscript{327} Id. at 609.
\textsuperscript{328} Id. at 609.
\textsuperscript{329} Id.
\textsuperscript{330} Id. at 611.
\textsuperscript{331} Id. at 611.
\textsuperscript{332} Id. See also State v. Andrews, 134 A.3d 324, 350, 256–57 (Md. Ct. Spec. App. 2016) (holding A pen register trap and trace order is not sufficient to authorize use of cell site simulator, which actively sends electronic signal and triggers cell phone to respond).
\textsuperscript{333} Id. at 547.
the Stingray gathered information from the phone that went beyond his location, such a search of his phone would have been unauthorized, and “suppression of the additional information (which might have pinpointed Patrick's location) would likely be required.”\(^{334}\) And the warrant in Patrick “authorize[d] the identification of the physical location of the target cellular phone,” in a context that implied that the service provider would release information that would then allow police to identify Patrick’s location.\(^{335}\) These were built-in qualifications that confined the grant of the warrant’s authority, as Chief Justice Wood explained, just like a physical limitation to the house, but not the shed, or vice versa, would do.\(^{336}\)

Though the Court has understood the manner of the warrant’s execution to fall within the officer’s discretion, such cases call into question whether the judiciary can sufficiently protect Fourth amendment rights with an after-the-fact review. How police conduct a search impacts the constitutionality of the search, at least when it comes to searches that utilize specialized technology, as Kyllo held. Stingrays can depart greatly from other information gathering methods, both in function and in their level of intrusiveness. Leaving the entirety of the manner in an officer’s discretion in the traditional sense means an officer can get a warrant for one technology and then use a different form, like a dragnet, but still argue this fell within his discretionary power to decide the manner of execution. It is difficult to see how an \textit{ex post} reasonableness assessment can sufficiently protect privacy rights when the damage has already been done, and with Stingrays, to a countless number of people.

To Judge Easterbrook’s surprise, a magistrate in the Northern District of Illinois recently imposed both \textit{ex ante} and \textit{ex post} restrictions on the government's use of a Stingray device “to bring the surveillance into compliance with the Fourth Amendment.”\(^{337}\) The

\(^{334}\) Id. at 548.
\(^{335}\) Id.
\(^{336}\) Id.
\(^{337}\) Rachel Levinson-Waldman, \textit{Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public}, 66 Emory L.J. 527,
judge was particularly concerned with the Stingray’s “inevitable collection of innocent third parties’ information.” It thus required the government to take three steps to limit the collection, retention, and use of the information gathered when it used the cell-simulator.

The first restriction indicated law enforcement “make reasonable efforts to minimize the capture of signals from cell phones used by people other than the target of the investigation.” The order also prohibited law enforcement from using the Stingray “when, because of the location and time, an inordinate number of innocent third parties’ information will be collected.” The second restriction directed law enforcement to delete all extraneous data, which is all data other than the data that identified the target’s cellphone, within 48 hours after its capture. The last restriction banned law enforcement from using any information beyond what was actually necessary to determine the target’s location. The court significantly noted “a cell-site simulator is simply too powerful of a device to be used and the information captured by it too vast to allow its use without specific authorization

582–84 (2017) (citing In re Application of the U.S. for an Order Relating to Tels. Used by Suppressed, No. 15 M 0021, 2015 WL 6871289, at *3 (N.D. Ill. Nov. 9, 2015). The guiding principle, as in all Fourth Amendment cases, is a “reasonable balance between the investigative needs of law enforcement and the privacy interests of the suspect and society at large.” David Gray & Danielle Citron, The Right to Quantitative Privacy, 98 MINN. L. REV. 62, 111 (2013) (citing United States v. Jones, 565 U.S. 400 (2012)). Applied to drones, GPS-enabled tracking, and similar technologies, an appropriate warrant requirement might mean setting limits on “when, how, and how long a device can be deployed. Id.

338 In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed, 2015 WL 6871289, at *3.

339 Id.

340 Id.

341 Id. As examples, the court stated it would be inappropriate for law enforcement to use the Stingray near a large arena while a sporting event or high school graduation takes place. Id.

342 Id. at *4.

343 Id.
from a fully informed court. Minimizing procedures . . . are necessary to protect the goals of the Fourth Amendment.\textsuperscript{344} The stress on a “fully informed court” falls directly in line with arguments made by both judges and scholarly commentators that government agents owe a “duty of candor” to judicial officers when presenting warrant applications.\textsuperscript{345} In United States v. Comprehensive Drug Testing, Inc., Chief Judge Kozinski, wrote a concurring opinion that offered guidelines to magistrates on how to deal with issuing search warrants for electronic data.\textsuperscript{346} The Chief Judge emphasized, “[a] lack of candor in any aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized [items].”\textsuperscript{347} This duty, the kind that Patrick raised, would require the government to fairly disclose in a warrant application aspects of the process and the scope of the intended search, including the implications on third parties.

By not knowing (or caring) how the Stingray specifically conducted a search, the court in Patrick should not have taken the approach “less is enough.”\textsuperscript{348} Lambis and Andrews rejected point-blank that the use of a cell-site simulator was “close enough” to a warrant for cell-site location information, noting the many ways the two devices are different in kind.\textsuperscript{349} As Chief Judge Wood noted, the Seventh Circuit was likely not dealing with “two interchangeable tools

\textsuperscript{344} Id.


\textsuperscript{346} United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, C.J., concurring).

\textsuperscript{347} Id.

\textsuperscript{348} United States v. Patrick, 842 F.3d 540, 544 (7th Cir. 2016) (“This means that the police could have sought a warrant authorizing them to find Patrick’s cell phone and kept silent about how they would do it.”).

for gathering exactly the same information.”

On the facts, the Seventh Circuit could not definitively provide an answer.

CONCLUSION

The Seventh Circuit in Patrick was undoubtedly presented with weighty questions. It confronted whether the use of a cell-site simulator Stingray device constitutes a search that falls within the Fourth Amendment and whether the Fourth Amendment requires the warrant to authorize specifically the use of such a device, all issues of first impression. Unfortunately, its analysis provided a painful bite at privacy rights. Though the Seventh Circuit got the first word, fortunately, it did not get the last.

The mystique surrounding Stingrays ultimately illuminates the harsh reality of this unregulated and technologically unmediated surveillance technology. As Chief Judge Wood pointed out, the government has gone so far as to dismiss cases, withdraw evidence, and negotiate lesser plea agreements rather than reveal that the technology was used.

Standing issues will continue to severely limit which law enforcement activities are challenged. As the court in Patrick briefly addressed, Patrick had no standing to challenge the Stingray search on the grounds that it was too broad: “if the problem with simulators is that they are too comprehensive, that would not lead to suppression—though it might create a right to damages by other persons whose interests were unreasonably invaded.”

If the secrecy lingers, and courts decline to remand the issues for further fact finding, third

---

350 Patrick, 842 F.3d at 549 (Wood, C.J., dissenting).
351 See generally Pell & Soghoian, supra note 4. Police track thousands of cellphones every year, and generally, neither the target nor the public ever learns of a tracking order. Rothstein, supra note 30, at 491 (2012). Requests to track cellphones are sealed, and the judges who consider tracking requests rarely publish opinions. Id. In fact, “one federal magistrate judge has estimated that federal courts alone approve 20,000-30,000 tracking requests annually, and the number is rising.” Id.
352 Patrick, 842 F.3d at 546 (Wood, C.J., dissenting).
353 United States v. Patrick, 842 F.3d 540, 545 (7th Cir. 2016).
parties will find it extremely difficult, if not impossible, to discover whether their information was collected.

This creates a paradoxical question: how can courts deter unlawful police conduct if those that have standing never know they have a viable claim? The uncomfortable reality is that if a Stingray search was unreasonably sweeping, those that have standing to invoke a Fourth Amendment claim will likely never know, because the defendant before the court likely does not have standing to explore the question. Indeed, a court will deem these issues as irrelevant unless the defendant can successfully allege the conduct violated his own constitutional rights. And since the Court does not extend the interest of the exclusionary rule’s deterrent function to unconstitutional police conduct affecting third parties, Stingrays that collaterally searched third parties’ phones and scooped up their data will proceed uncontested. The collection of innocent third party information unfortunately then becomes tolerable collateral damage.

The Seventh Circuit’s attitude in Patrick evokes questions of whether devices such as Stingrays should prompt a change in what a warrant requires, both in substance and in procedure, to satisfy the Fourth Amendment’s requirements. Judicial review after-the-fact is no longer an effective safeguard. The Stingray device, by its very nature, calls for greater supervision.

The solution may rest with the legislature. All three states within the Seventh Circuit, Illinois, Indiana and Wisconsin, now require police to get a warrant to conduct real-time cellphone tracking. Nine other states—California, Maine, Maryland, Minnesota, Montana, New Hampshire, Utah, Virginia, and Washington—require the same.

354 Id.
355 See 725 ILL. COMP. STAT. ANN. 168/10 (West 2017); IND. CODE ANN. § 35-33-5-12 (West 2014); WIS. STAT. ANN. § 968.373(2) (West 2014). Wisconsin’s statute was enacted in April of 2014, after the search in Patrick’s case, which occurred in October 2013.
356 CAL. PENAL CODE § 1546 (West 2017); ME. REV. STAT. tit. 16, § 648 (2014); MD. CODE ANN., CRIM. PROC. 1-203.1(b)(1) (West 2014); MINN. STAT. ANN. §§ 626A.28(3)(d), 626A.42(1)(d) (West 2014); MONT. CODE ANN. § 46-5-110(1)(a)
Still, courts should approach questions regarding Stingray searches with increased caution. As an initial matter, courts should find that the use of a Stingray is a search under the Fourth Amendment, which then triggers the requirements of a warrant supported by probable cause. To be clear, this Note does not question law enforcement discretion regarding the use of the Stingray nor does it pass judgment on the propriety of these devices as a matter of public policy. But, as Stingrays confirm, surveillance technology no longer operates in the clean vacuum as it once did, directed only at a target. Numerous third parties enter the equation with Stingrays. The manner in which police gather information now becomes relevant with Stingrays because the collection of the data itself can invoke a Fourth Amendment violation. Of course, this disclosure can vary on a case-by-case basis, but a judicial officer cannot protect who he or she does not know is vulnerable. With Stingrays, the manner of the search implicates constitutional rights in a way that information gathering methodologies in the past have not.

Ultimately, we know little about Stingray devices, and until more information surfaces, its veil of secrecy precludes courts from meaningfully resolving constitutional questions. Until then, the question remains, who is pinging your phone?