# A HAILSTORM OF UNCERTAINTY: THE CONSTITUTIONAL QUANDARY OF CELL-SITE SIMULATORS

*Carrie Leonetti*∗



***Abstract***

*In a relatively short period of time, Stingray tracking by law-enforcement officers has become ubiquitous and shrouded in secrecy. These Stingrays engage not only their targeted phone, but also every phone near where they are operating, raising concerns about individualized suspicion and particularity.*

*From a practical standpoint, Stingray tracking is technologically superior to both cell-site location information and global-positioning satellite tracking because it is always done in real time without the involvement of the wireless service provider and does not require the hacking capability of GPS tracking. Up until now, the Supreme Court has avoided deciding the constitutionality of warrantless GPS tracking,*

∗ Associate Professor, Center for Cyber Security and Privacy & School of Law, University of Oregon.

*along with broader questions about the reasonableness of privacy interests in personal data. In the meantime, lower courts are divided on the constitutionality of the police acquiring CSLI from a cell-service provider using a subpoena.*

*Even if the Court ultimately finds that GPS tracking and CSLI acquisition are not searches for Fourth Amendment purposes, those decisions would not necessarily dictate the same result for warrantless Stingray tracking because GPS and CSLI tracking typically involve following a suspect primarily on public thoroughfares while Stingray tracking allows the police to track a suspect's phone inside of the individual's residence and because of the invasion into the phone by the Stingray tracking device to extract the location information.*

*The Court has recently shown a willingness to reign in traditional privacy exceptions when they apply to intrusive high-tech searches in the modern era in the context of searches incident to arrest. Much of the Court's reasoning regarding the difference between searches of cell phones and packs of cigarettes applies by analogy to the difference between visual surveillance and Stingray tracking.*

*The few lower courts that have ventured into this unchartered territory of warrantless Stingray searches have found them to be unconstitutional, but the constitutional dilemmas that Stingray tracking invokes are not new. Instead, Stingrays are just another iteration of the broader problem that the Katz test has failed to keep up with technological changes and developments in high-tech surveillance. The Supreme Court needs to address the applicability of Maryland v. Smith and Miller v. United States to high-tech data mining and analysis, and it needs to do so in a systematic way that addresses not only today's newest technology, but by providing a systematic framework by which tomorrow's searches can be judged, as well.*

## I. INTRODUCTION

I have previously written to call on the Supreme Court to adopt a broad framework of Fourth Amendment privacy[1] that can account for the collection, aggregation, and mining of personal data[2] and protect

1. The Fourth Amendment guarantees:

> 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.

U.S. CONST. amend. IV.

2. *See* Carrie Leonetti, *Bigfoot: Data Mining, the Digital Footprint, and the Constitutionalization of Inconvenience*, 15 J. HIGH TECH. L. 260 (2014) [hereinafter "Leonetti, *Data Mining*"].

against large-scale, "dragnet" investigatory sweeps.[3] What these previous proposals share in common is the critique that the Court's current application of the reasonable-expectation-of-privacy test from *Katz v. United States*[4] to high-tech forms of surveillance fails adequately to protect Americans from unwarranted intrusions into their private activities. This Article picks up where those left off with the most recent example of the *Katz* high-tech conundrum: how, if, and whether courts can regulate law-enforcement use of cell-site-simulator technology (also known as "IMSI (International Mobile Subscriber Identity) catchers" or by brand names including "StingRay," "Triggerfish," and "Hailstorm")[5] to intercept data traveling to and from individuals' cell phones. Part II briefly describes the way that Stingray technology tracks a suspect cell phone. Part III contrasts the operation of Stingray tracking with that of its two most constitutionally analogous alternate forms of tracking: cell-site location information (CSLI) tracking and Global Positioning Satellite (GPS) tracking. Part IV describes the Supreme Court's primary jurisprudence governing the Fourth Amendment's protection of privacy, the plain-view, third-party, and metadata doctrines. It discusses their application to GPS tracking, high-tech searches incident to arrest, and CSLI tracking, as well as how Stingray tracking fits in among these other constitutional controversies. Part V describes the few lower-court cases that have addressed the constitutionality of warrantless Stingray tracking. Part VI concludes that Stingray tracking is not meaningfully different, in a constitutionally significant way, from many other forms of warrantless high-tech surveillance. Rather, its treatment and use is another variation on the broader critique that the Supreme Court's current Fourth Amendment jurisprudence fails to address the critically important questions involving the viability and application of the third-party doctrine in the context of large-scale, suspicionless data mining programs.

## II. THE TECHNOLOGY

All base towers communicate periodically with nearby cell phones by sending intermittent signals, to which the cell phones respond, generally to the tower emitting the strongest signal, which also tends to be the

3. *See* Carrie Leonetti, *Motive & Suspicion:* Florida v. Jardines *and the Constitutional Right to Protection from Suspicionless Dragnet Investigations*, 14 OHIO ST. J. CRIM. L. 247; *see also* Carrie Leonetti, *A Grand Compromise for the Fourth Amendment*, 12 MD. J. BUS. & TECH. L. 1.

4. 389 U.S. 347 (1967).

5. *See* Jemal R. Brinson, *Data: Cell Site Simulators: How Law Enforcement Can Track You*, CHIC. TRIB. (Feb. 18, 2016), http://www.chicagotribune.com/news/plus/ct-cellphone-tracking-devices-20160129-htmlstory.html. This Article uses these names interchangeably.

closest tower to the phone.[6] As the phone moves around, the relative strength of the signal from different towers varies, and the cell phone changes the tower with which it is communicating accordingly, continuously "pinging" off of the strongest/nearest tower or towers. By tracking the towers through which a given cell phone is communicating and the relative signal strengths, the police can determine an approximate location of the phone (and usually, by extension, the suspect).[7]

Stingrays work by impersonating cell towers, sending a barrage of signals into a target area to engage a target cell phone, and forcing the phone to ping back to the simulator.[8] By doing so, the Stingray essentially tricks nearby mobile devices into communicating with them and transmitting their unique numerical identifiers that cell-service providers use to route the correct information to and from each phone—basically their electronic serial numbers.[9] The Stingray then collects this information from pings over a period of time and uses their relative strength to generate a precise location for the duped mobile device.[10]

## III. THE CONTROVERSY

### *A. Existing Technologies*

In order to understand the controversy surrounding warrantless Stingray tracking, it is important to place Stingray tracking in its proper place in comparison to location-tracking technologies that are commonly used by law enforcement, whose use the Court has largely failed to address.

#### 1. CSLI: Cell-Site Location Information

As long as a suspect cell phone is turned on, law-enforcement officers can plot the locations of the different cell towers off of which it is pinging and determine the approximate location of the phone (and therefore any individual who has the phone in his/her possession). From a practical standpoint, there are two major weaknesses with this type of

6. *See id.*

7. *See, e.g.*, Tracey v. State, 152 So. 3d 504, 507 (Fla. 2014).

8. *See* United States v. Lambis, 197 F. Supp. 3d 606., 609 (S.D.N.Y. 2016); State v. Andrews, 134 A.3d 324, 355 (Md. Ct. Spec. App. 2016).

9. *See* State v. Tate, 849 N.W.2d 798, 826 n.8 (Wis. 2014); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 142–46 (2013).

10. *See Lambis*, 197 F. Supp. 3d at 609; Pell & Soghoian, *supra* note 9, at 144–46.

phone tracking for law-enforcement officers. First, CSLI tracking is relatively imprecise. It can locate the general area in which a cell phone is being used (e.g., a particular city block or maybe an apartment complex), but it cannot pinpoint the exact location of the phone. Second, the police have to obtain CSLI from a third party (the suspect cell-service provider), typically by way of a grand jury subpoena.

#### 2. GPS Tracking

From a technical standpoint, GPS tracking is superior to CSLI for locating a suspect's cell phone. Because the phone's GPS chip communicates directly with a satellite, GPS tracking can locate a device more precisely than CSLI. GPS tracking can be done in real time, but courts generally require a warrant and probable cause for GPS tracking (although whether this is constitutionally required is the issue that the Supreme Court declined to reach in *United States v. Jones*).[11] GPS tracking also typically requires the police to attach physically a tracking device to a target (usually a car) because, even though most cell phones have internal GPS chips, law-enforcement officers generally do not have the ability to crack the phone's encryption to access the chips—at least, not without advanced hacking capability, as the most recent battle between the Federal Bureau of Investigation (FBI) and Apple aptly demonstrated.[12]

### *B. How Stingray is Different*

From a practical standpoint, Stingray tracking is technologically superior to both CSLI and GPS tracking. Unlike CSLI, Stingray tracking is always done in real time without the involvement of the wireless service provider, but it does not require the hacking capability (and legal hassles) of GPS tracking. Cutting out the wireless provider from the acquisition of the phone's location information not only speeds up the delivery of location information from the phone to the police, but it also heads off any risk that the service provider will move to quash a subpoena for historical phone-location records.

---

11. *See infra* Part IV.A.4.

12. *See Answers to Your Questions about Apple and Security*, APPLE, http://www.apple.com/customer-letter/answers/ (last visited July 20, 2016); Brian Barrett, *The Apple-FBI Battle is Over, but the New Crypto Wars Have Just Begun*, WIRED (Mar. 30, 2016), https://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/; Nathaniel Mott, *Take That, FBI: Apple Goes All in on Encryption*, GUARDIAN (June 15, 2016), https://www.theguardian.com/technology/2016/jun/15/apple-fbi-file-encryption-wwdc; Danny Yadron et al., *Inside the FBI's Encryption Battle with Apple*, GUARDIAN (Feb. 18, 2016), https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple.

## IV. THE CONSTITUTIONAL DILEMMAS

### *A. Privacy*

The framework for assessing whether an investigatory technique is a search, and therefore is subject to the requirements of the Fourth Amendment (usually a judicial warrant issued on probable cause), is the *Katz* reasonable-expectation-of-privacy test. *Katz* involved the surreptitious recording of conversations that Katz had during calls made in a public phone booth, but from outside of the phone booth without physical invasion of the booth by investigators.[13] The Government had defended the warrantless eavesdropping on the ground that it had occurred without a physical trespass into the phone booth.[14] The Supreme Court rejected that argument, holding:

> The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.[15]

The test that the Court adopted for determining whether a search had occurred for Fourth Amendment purposes post-*Katz* was the now well-known test which Justice Harlan proposed in his concurring opinion: "[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[16] Immediately following that test, however, Justice Harlan continued by noting:

> Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances

13. *See* Katz v. United States, 389 U.S. 347, 348 (1967).
14. *See id.* at 348–49.
15. *Id.* at 353.
16. *Id.* at 361 (Harlan, J. concurring).

would be unreasonable.[17]

This language about items in "plain view" would ultimately grow into what commentators generally refer to as the "plain-view exception" to the warrant requirement.

### 1. Plain View

*California v. Ciraolo*[18] offers a textbook example of how the plain-view exception plays out post-*Katz*. The police suspected Ciraolo of cultivating large amounts of marijuana. Probably adding to that suspicion was the fact that he had a large, opaque fence around his back yard. Not to be outdone, the police, acting without a warrant, used a helicopter and telephoto camera equipment to surveil Ciraolo's back yard from the air, finding a large number of marijuana plants growing behind the fence. Rejecting Ciraolo's argument that the warrantless surveillance of his well-protected back yard was a search for Fourth Amendment purposes, and thus requiring a warrant issued on probable cause, the Court held:

> The observations by [the police] in this case took place within public navigable airspace, in a physically nonintrusive manner; from this point they were able to observe plants readily discernible to the naked eye as marijuana. . . . Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed. On this record, . . . respondent's expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor.[19]

### 2. The Third-Party Doctrine

It is a central axiom of constitutional law that the Bill of Rights constrains only government action.[20] This principle, in conjunction with

17. *Id.*

18. 476 U.S. 207 (1986).

19. *Id.* at 213–14.

20. *See* Burdeau v. McDowell, 256 U.S. 465, 475–76 (1921) (holding that the protections of the Fourth Amendment applied only to governmental action and did not prohibit the admission of incriminating papers stolen from private files by private individuals); United States v. Benoit, 713 F.3d 1, 9 (10th Cir. 2013) (holding that the Fourth Amendment was wholly inapplicable to illegal searches and seizures by private individuals not acting as agents, or with the knowledge of, government officials); United States v. Goodale, 738 F.3d 917, 921 (8th Cir. 2013) (holding that the Fourth

the plain-view doctrine, has given rise to a principle that commentators refer to as the "third-party doctrine," which the Court first established in *United States v. Miller*.[21] Miller was a moonshiner who kept the proceeds from his bootlegging business in the bank. Pursuant to federal banking statutes, the bank retained certain records of Miller's financial transactions through his account. Tax-revenue agents subpoenaed Miller's bank records from the bank, hoping to uncover evidence of tax evasion, à la Capone, and the bank turned them over. In his subsequent criminal case, Miller moved to suppress the records on the ground that their warrantless acquisition had violated the Fourth Amendment. The

Amendment did not apply to private searches that were "neither instigated by nor performed on behalf of a governmental entity"); United States v. Lee, 723 F.3d 134, 139 (2d Cir. 2013) (holding that the Fourth Amendment applied only to government action, not that of private individuals); United States v. Tosti, 733 F.3d 816, 821 (9th Cir. 2013) (holding that Fourth Amendment prohibitions were "inapplicable to private action"); United States v. Cameron, 699 F.3d 621, 637 (1st Cir. 2012) (holding that the Fourth Amendment did not apply to searches and seizures conducted by private individuals without the knowledge or participation of government agents); United States v. Oliver, 630 F.3d 397, 406 (5th Cir. 2011) (holding that the Fourth Amendment did not protect against searches "conducted by private individuals acting in a private capacity"); United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010) (holding that the Fourth Amendment exclusionary rule did not apply to the fruits of illegal private searches); United States v. Bruce, 396 F.3d 697, 705 (6th Cir. 2005) (holding that the Fourth Amendment did not apply to unreasonable searches or seizures conducted by private individuals not acting as governmental agents), *vacated in part on reh'g*, 405 F.3d 1034 (6th Cir.); United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003) (holding that searches by private individuals did not implicate the Fourth Amendment unless they were acting as agents or instruments of the government); United States v. Crowley, 285 F.3d 553, 558 (7th Cir. 2002) (holding that searches and seizure by private individuals did not implicate the Fourth Amendment unless they were acting as agents or instruments of the government); Clark v. State, 562 N.E.2d 11, 14 (Ind. 1990) (holding that the Fourth Amendment did not apply to searches performed by private actors); State v. Brittingham, 294 P.3d 263, 266–67 (Kan. Sup. Ct. 2013) (holding that neither the Fourth Amendment nor the analogous provision of the Kansas Constitution applied to the conduct of private individuals acting independently of the State); State v. Collins, 790 A.2d 660, 664 (Md. 2002) (holding that the Fourth Amendment did not protect individuals from unreasonable searches and seizures by private individuals); Commonwealth v. Augustine, 4 N.E.3d 846, 855–56 (Mass. 2014) (holding that the Fourth Amendment did not govern the methods used by private parties to discover and seize evidence unless state officials instigated or participated in the search or seizure); State v. Jorgensen, 660 N.W.2d 127, 131 (Minn. 2003) (holding that the Fourth Amendment did not apply to searches by private individuals conducted without knowledge of, or acquiescence by, State officials); State v. Rivera, 241 P.3d 1099, 1104 (N.M. 2010) (holding that the Fourth Amendment prohibition against unreasonable searches and seizure did not extend to searches conducted by private citizens); State v. Seglen, 700 N.W.2d 702, 706 (N.D. 2005) (holding that the Fourth Amendment only applied to governmental actions); Commonwealth v. Harris, 817 A.2d 1033, 1047 (Pa. 2002) (holding that neither the Fourth Amendment nor the analogous provision of the Pennsylvania Constitution applied to searches and seizures conducted by private individuals); State v. Thunder, 777 N.W.2d 373, 378 (S.D. 2010) (holding that the Fourth Amendment offered no protection from private nongovernmental searches); State v. Carter, 85 P.3d 887, 890 (Wash. 2004) (holding that neither federal nor state protections against unreasonable searches and seizures were implicated without State action); State v. Smith, 702 S.E.2d 619, 628 (W. Va. 2010) (holding that constitutional protections against unreasonable searches and seizures did not apply to searches by private individuals unless they were acting as instruments or agents of the State); State v. Payano-Roman, 714 N.W.2d 548, 553 (Wis. 2006) (holding that private searches were not subject to the restrictions of the Fourth Amendment because they applied only to governmental action).

21. 425 U.S. 435 (1976).

Court rejected Miller's argument, holding that the acquisition of the records was not a search for Fourth Amendment purposes, reasoning:

> [C]hecks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. . . . The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . . [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[22]

The Court employed similar reasoning in *California v. Greenwood*.[23] In Greenwood, the police, who suspected Greenwood of drug trafficking, arranged, without a warrant, for her garbage company to turn over her garbage to them after it had been collected from the curb on her regular collection day. Rejecting Greenwood's argument that the warrantless acquisition of her garbage had been unconstitutional, the Court reasoned:

> [R]espondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection. It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so. Accordingly, having deposited their garbage "in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it," respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded.[24]

22. *Id.* at 442–43.

23. 486 U.S. 35 (1988).

24. *Id.* at 40–41.

### 3. Metadata

At the same time that the Court was developing principles to limit the possessory scope of the Fourth Amendment by holding that items in plain view and items entrusted to third parties who chose to turn them over to the police as part of a criminal investigation do not deserve the protection of the Fourth Amendment, it was also developing principles to limit the typological scope of the Fourth Amendment's restrictions. Most notably for the purposes of Stingray tracking, in *Smith v. Maryland*,[25] the Supreme Court held that the use of "pen registers"[26] was not a search for Fourth Amendment purposes. The facts of *Smith* were a bit odd. A woman was robbed, and her identification was taken from her. After the robbery, she began to receive harassing and threatening phone calls from someone identifying himself as the robber. The police arranged for her phone company to attach a pen register to her phone, which would trap and trace the phone numbers, time, and duration of all incoming calls to her phone. When she received the next harassing phone call, the police were able to use the pen register to determine that it had originated from Smith's telephone. Rejecting Smith's argument that the warrantless trace of his phone call was unconstitutional, the Court held:

> In applying the *Katz* analysis to this case, it is important to begin by specifying precisely the nature of the state activity that is challenged. The activity here took the form of installing and using a pen register. Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his "property" was invaded or that police intruded into a "constitutionally protected area." Petitioner's claim, rather, is that, notwithstanding the absence of a trespass, the State, as did the Government in *Katz*, infringed a "legitimate expectation of privacy" that petitioner held. Yet a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.
>
> . . . .
>
> Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search"

25. 442 U.S. 735 (1979).

26. A "pen register" is a device that records dialing, routing, addressing, or signaling information from electronic communications. *See* MD. CODE ANN., CTS. & JUD. PROC. § 10–4B–01(c)(1) (West 2016). Pen registers have largely been supplanted by "trap-and-trace" devices, which capture the originating number, routing, addressing, and signaling information to identify the source of an electronic communication. *See id.* § 10–4B–01(d)(1).

> necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.
>
> This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. . . . Telephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.
>
> . . . .
>
> . . . Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.[27]

This distinction between contents and metadata is often at the heart of the Government's defense of various warrantless data-mining programs.[28]

### 4. The GPS-Tracking Analogy

Unfortunately, the Supreme Court dodged its opportunity to decide the constitutionality of warrantless GPS tracking a few years ago, along with broader questions about the reasonableness of privacy interests in personal data, in *United States v. Jones*.[29] In *Jones*, the police had placed a GPS tracking device on Jones's car, without a valid warrant, because it was parked in his front driveway. The police then used the device to track his movement and tie him to a drug-trafficking scheme. The Government defended the warrantless tracking on the basis of an earlier case, *Knotts v. United States*,[30] which had found warrantless tracking of a vehicle using a radio beacon to be constitutional under the plain-view doctrine, reasoning:

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from

27. *Smith*, 442 U.S. at 741–43.

28. *See* Leonetti, *Data Mining*, *supra* note 2, at 267.

29. 565 U.S. 400 (2012).

30. 460 U.S. 276 (1983).

> one place to another. When [the source] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.
>
> . . . .
>
> Visual surveillance from public places along [the source]'s route or adjoining Knotts' premises would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but on the use of the beeper to signal the presence of [the source]'s automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.[31]

A majority of the Court in *Jones* found the use of the GPS tracking device to be unconstitutional, but on the narrow ground that the police had trespassed onto Jones's property to place it on his car (rendering the subsequent tracking fruit of the poisonous trespass tree), reasoning: "The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment . . . ."[32]

If the Court had reached the merits of the warrantless GPS tracking issue itself (i.e., the question of the continued viability of *Knotts* and the constitutionality of the GPS tracking if the police had instead placed the device on Jones's car without trespassing—e.g., when it was parked on a public road or in a parking lot), as Justice Sotomayor proposed,[33] the decision might have shed light on the constitutional status of warrantless Stingray tracking.[34] Instead, the constitutionality of warrantless GPS

---

31. *Id.* at 281–82.

32. *Jones,* 565 U.S. at 404–405.

33. *See id.* at 416–17 (Sotomayor, J., concurring) ("I would take [the] attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on . . . . More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g.,* [*Smith*, *Miller*]. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

34. *See, e.g.*, *In re* the Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F.Supp.2d 747, 752 (S.D. Tex. 2012) (finding that

tracking (in the absence of a trespass during the placement of the device) remains an open question. Even if the Court ultimately finds that using GPS to track suspects is not a search for Fourth Amendment purposes, that would not necessarily dictate the same result for warrantless Stingray tracking. GPS tracking typically involves following a suspect primarily on public thoroughfares (because the tracking device is typically attached to a vehicle), while Stingray tracking allows the police to track a suspect's phone inside of the individual's residence. In fact, its in-home-location precision is the primary reason why police prefer it to GPS tracking. The penetration of the walls of the suspect's home or other protected place, however, could create a unique constitutional problem even if the act of tracking itself does not.[35]

A few years after the Supreme Court decided *Knotts*, permitting warrantless radio-beacon-tracking of suspects on public streets, it decided *United States v. Karo*.[36] *Karo*'s facts were very similar to those of *Knotts*, except that, in *Karo*, the police used the radio beacon to track Karo in his private residence. Distinguishing *Knotts*, the Court held that tracking within a home required a warrant:

> [We] reject the government's contention that it would be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime . . . will be committed . . . . If agents are required to obtain warrants prior to monitoring a beeper when it has been withdrawn from public view, the government argues, for all practical purposes they will be forced to obtain warrants in every case in which they seek to use a beeper, because they have no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises. The argument that a warrant requirement would oblige the government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.[37]

### 5. High-Tech Searches Incident to Arrest

The Court has recently shown a willingness to reign in traditional privacy exceptions when they apply to intrusive high-tech searches in

---

a sitesite simulator was more akin to a tracking device than a pen register).

35. *See. e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the warrantless use of a thermal-imaging device to penetrate the walls of Kyllo's residence and detect the heat signature from a high-intensity marijuana-growing light installation inside violated the Fourth Amendment).

36. 468 U.S. 705 (1984).

37. *Id.* at 717–18.

another context: searches incident to arrest. The Court announced the search-incident-to-arrest exception to the warrant requirement in *Chimel v. California*,[38] when it held:

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. . . . In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. And the area into which an arrestee might reach in order to grab a weapon or evidentiary items must, of course, be governed by a like rule. . . . There is ample justification, therefore, for a search of the arrestee's person and the area "within his immediate control"—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.[39]

Post-*Chimel*, search-incident-to-arrest cases tended to involve items like wallets and cigarette packs. With the increasing ubiquity of cell phones, however, the Court addressed the Government's argument that the *Chimel* principle extended to the search of the contents of a modern cell phone, including voice messages, email, and text messages. In *Riley v. California*,[40] the Court held that it did not—that the search of a cell phone found in a suspect's pocket was quantitatively and qualitatively different than the search of the pocket itself, requiring its own justification (a warrant and probable cause, unless an applicable exception to the warrant requirement existed).[41] The Court reasoned:

> The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of

38. 395 U.S. 752 (1969).
39. *Id.* at 762–63.
40. 134 S. Ct. 2473 (2014).
41. *See id.* at 2489–94.

that reasoning to digital data has to rest on its own bottom.

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.

. . . .

The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

. . . .

Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

. . . .

. . . [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.[42]

Much of this reasoning regarding the difference between searches of cell phones and packs of cigarettes applies by analogy to the difference

42. *Id.* at 2488–91.

between visual surveillance and Stingray tracking.

### 6. Warrantless CSLI Acquisition

Lower courts are divided on the constitutionality of warrantless CSLI acquisition—i.e., the constitutionality of the police acquiring CSLI from a cell-service provider using a subpoena (rather than a judicial warrant issued after a showing of probable cause). Some courts reason, in cases such as *Miller*, *Greenwood*, and *Smith*, that, by turning their CSLI over to their phone companies (pursuant to service contracts, typically for billing purposes), cell-service customers have relinquished a reasonable expectation of privacy that those providers will not in turn reveal the information to the police. Other courts reason, similarly to *Riley* and Justice Sotomayor's concurring opinion in *Jones*, that there is a qualitative difference between simply reviewing billing records and the creation of a twenty-four hour per day log of a person's movements through space and time. These opinions also reason that voluntarily allowing a phone company to communicate with one's phone through towers does not relinquish a reasonable expectation that such information will not be seized by the government for the purpose of tracking. To the extent that a pattern has emerged, courts tend to be more receptive to the acquisition of historical (past-tense) CSLI without a warrant than to warrantless, real-time tracking.[43]

Two recent federal appeals court opinions demonstrate the split in reasoning among lower courts. In *United States v. Davis*,[44] law-enforcement agents were investigating a string of robberies at six local businesses. During the investigation, the agents subpoenaed Davis's telephone communications records during the time period of the robberies from MetroPCS, his cellular service provider (without a judicially issued search warrant). The records showed the telephone numbers that Davis called on each of his outgoing calls during the time period and the location of the cell tower that connected each call. The calls to and from Davis's cell phone were all connected through cell towers located near robbery locations. Davis challenged the admissibility of the CSLI at trial, arguing that it had to be suppressed

43. *See, e.g.*, *In re* Application of the United States for an Order Authorizing Installation and Use of a Pen Register, 415 F.Supp.2d 211, 219 (W.D.N.Y. 2006) (holding that the Government needed to show "that there exists probable cause to believe that the data sought will yield evidence of a crime" in order to collect real-time CSLI); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F.Supp.2d 747, 765 (S.D. Tex. 2005) (holding that the Government had to obtain a search warrant based on probable cause to obtain real-time CSLI); *cf.* MD. CODE ANN., CRIM. PROC. § 1–203.1(b)(1) (West 2016) (requiring a court order issued on the basis of probable cause for the acquisition of real-time location information from an electronic device).

44. 785 F.3d 498 (11th Cir. 2015).

because its warrantless acquisition violated the Fourth Amendment. The United States Court of Appeals for the Eleventh Circuit rejected Davis's challenge, reasoning:

> [L]ike the bank customer in *Miller* and the phone customer in *Smith*, Davis can assert neither ownership nor possession of the third-party's business records he sought to suppress. Instead, those cell tower records were created by MetroPCS, stored on its own premises, and subject to its control. Cell tower location records do not contain private communications of the subscriber. This type of *non-content evidence*, lawfully created by a third-party telephone company for legitimate business purposes, does not belong to Davis, even if it concerns him.
>
> . . . .
>
> More importantly, like the bank customer in *Miller* and the phone customer in *Smith*, Davis has no subjective or objective reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls at or near the time of six of the seven robberies.
>
> . . . .
>
> Admittedly, the landscape of technology has changed in the years since these binding decisions in *Miller* and *Smith* were issued. But their holdings did not turn on assumptions about the absence of technological change. To the contrary, the dispute in *Smith*, for example, arose in large degree due to the technological advance from call connections by telephone operators to electronic switching, which enabled the electronic data collection of telephone numbers dialed from within a home. The advent of mobile phones introduced calls wirelessly connected through identified cell towers. This cell tower method of call connecting does not require "a different constitutional result" just "because the telephone company has decided to automate" wirelessly and to collect the location of the company's own cell tower that connected the calls. . . . The longstanding third-party doctrine plainly controls the disposition of this case.
>
> The use of cell phones is ubiquitous now and some citizens may want to stop telephone companies from compiling cell tower location data or from producing it to the government. . . . "[T]he recourse for these desires is in the market or the political process; in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact

statutory protections."[45]

Almost simultaneously, the United States Court of Appeals for the Fourth Circuit addressed the same issue in *United States v. Graham*,[46] under nearly identical circumstances. Graham involved a string of six attempted robberies of several business establishments in Baltimore. Law-enforcement agents sought cell-phone information from Sprint/Nextel, the service provider for two cell phones recovered during a search of Graham's truck, including CSLI for calls and text messages transmitted to and from the phones around the time of the robberies. At the time when Sprint/Nextel turned over the CSLI to investigators, it had a privacy policy in effect, which was included in Graham's service contract, which stated, in pertinent part:

> Information we collect when we provide you with Services includes when your wireless device is turned on, how your device is functioning, device signal strength, where it is located, what device you are using, what you have purchased with your device, how you are using it, and what sites you visit.[47]

The privacy policy notwithstanding, a three-judge panel of the Fourth Circuit reached the opposite conclusion than the one that the Eleventh Circuit reached—namely, that the warrantless acquisition of Graham's CSLI violated the Fourth Amendment. The court reasoned:

> [T]he government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI for an extended period of time. Examination of a person's historical CSLI can enable the government to trace the movements of the cell phone and its user across public and private spaces and thereby discover the private activities and personal habits of the user. Cell phone users have an objectively reasonable expectation of privacy in this information.
>
> . . . .
>
> . . . Much like long-term GPS monitoring, long-term location information disclosed in cell phone records can reveal both a comprehensive view and specific details of the individual's daily life.
>
> . . . .
>
> [*Miller* and *Smith*] do not categorically exclude third-party

45. *Id.* at 511–12.

46. 796 F.3d 332 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

47. *Id.* at 345.

> records from Fourth Amendment protection. They simply hold that a person can claim no legitimate expectation of privacy in information she voluntarily conveys to a third party. It is that voluntary conveyance—not the mere fact that the information winds up in the third party's records—that demonstrates an assumption of risk of disclosure and therefore the lack of any reasonable expectation of privacy. We decline to apply the third-party doctrine in the present case because a cell phone user does not "convey" CSLI to her service provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement.
>
> . . . .
>
> We cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person.[48]

### 7. Stingrays

Stingrays actively locate phones in a two-step process. First, they mimic a cellular tower in a way that tricks nearby cell phones into connecting with it. Second, it forces phones to transmit their unique electronic identifiers while using those transmissions to pinpoint the location of the target phone.[49] Because the constitutional status of warrantless CSLI and GPS tracking is itself uncertain, the constitutional status of warrantless Stingray tracking is even more tenuous. Even if the Supreme Court ultimately were to decide that warrantless, real-time CSLI tracking is constitutional, that determination would not necessarily dictate the same result for Stingray tracking because of the two primary differences between CSLI and Stingray tracking: the real-time nature of Stingray tracking and the invasion into the phone by the Stingray tracking device to extract the location information (which is what allows the police to dispense with the assistance of the service provider in performing the tracking),[50] as opposed to acquiring information already in the hands of the third-party provider.[51]

---

48. *Id.* at 344–55.

49. *See* State v. Andrews, 134 A.3d 324, 341 (Md. Ct. Spec. App. 2016).

50. *See id.* at 339–40.

51. *See* United States v. Lambis, 197 F. Supp. 3d 606, 615. (S.D.N.Y. 2016) ("[T]he arguments that can be made for the application of the third party doctrine to CSLI do not extend to the distinct technology used by a cell-site simulator, which has an additional layer of involuntariness. Unlike CSLI, the 'pings' picked up by the cell-site simulator are not transmitted in the normal course of the phone's operation. Rather, 'cell site simulators actively locate phones by forcing them to repeatedly transmit

Additionally, the added precision of Stingray tracking, in comparison to CSLI, may itself create an independent constitutional concern since it allows the police to track a suspect phone within the target's home, as opposed to CSLI which would only reveal the more general location of the suspect.[52] Even GPS tracking, which is highly precise, typically does not reveal a suspect's movements inside his or her home because the tracking device is traditionally placed on an automobile, rather than on the suspect's person, where a cell phone is typically carried.[53]

### *B. Ubiquity*

Stingray tracking by law-enforcement officers has become ubiquitous in two senses. First, a surprising number of law-enforcement agencies own and deploy IMSI catchers, typically without judicial oversight in the form of warrants, despite their relative newness and the dubious constitutional status of such use.[54] Second, the agencies that employ IMSI catchers do not employ them selectively, in only the most serious or urgent cases. Instead, agencies that have invested in Stingrays use them frequently and without regard to the seriousness of the investigation or the availability of other means of locating a suspect.[55]

---

their unique identifying electronic serial numbers, and then calculating the signal strength until the target phone is pinpointed.'") (citing *Andrews*, 134 A.3d at 340–41).

52. *See Andrews*, 134 A.3d at 349 ("Moreover, because the use of the cell site simulator in this case revealed the location of the phone and Andrews inside a residence, we are presented with the additional concern that an electronic device not in general public use has been used to obtain information about the contents of a home, not otherwise discernable without physical intrusion.").

53. An additional controversy stems from the fact that Stingrays are technologically capable of intercepting not just phone location information, but also the contents of wireless communications. Up until now, however, law-enforcement agencies have forsworn using Stingrays warrantlessly to intercept the contents of phone calls, text messages, emails, etc., *see*, Brinson, supra note 5; *see, e.g.*, *Andrews*, 134 A.2d at 332, likely because the warrantless interception of the contents of wireless communications would almost certainly be unconstitutional, at least in the absence of an exception to the warrant requirement (like exigent circumstances or consent). Because it appears that Stingrays are not presently being used to intercept the contents of these communications, this Article does not address the constitutionality or other ramifications of such disclaimed use. *But see* Carrie Leonetti, *If a Tree Falls: Bulk Surveillance, the Exclusionary Rule, and the Firewall Loophole*, 13 OHIO ST. J. CRIM. L. 211 (2015) (discussing the inability of the Fourth Amendment to provide a remedy for illegal searches that do not result in derivative evidence offered subsequently during a criminal trial).

54. *See Stingray Tracking Devices: Who's Got Them?*, .ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited July 24, 2016); John Diedrich, *Judge Wants Police to Disclose Use of "Stingray" in Murder Case*, MILWAUKIE-WISCONSIN J. SENTINEL (July 15, 2016), http://www.jsonline.com/news/crime/judge-wants-police-to-disclose-use-of-stingray-in-murder-case-b99762352z1-386997111.html (describing a Milwaukie Circuit Court judge's order for an evidentiary hearing regarding police use of a Stingray to locate a murder defendant).

55. *See* Cyrus Farivar, *New E-mails Reveal Feds Not "Forthright" About Fake Cell Tower Devices*, ARS TECHNICA (Mar. 27, 2013), http://arstechnica.com/tech-policy/2013/03/new-e-mails-reveal-feds-not-forthright-about-fake-cell-tower-devices/; Brad Heath, *Police Secretly Track Cell*

The end result of such widespread use of Stingrays in such a short period of time without judicial scrutiny is that police agencies may routinely be violating the Fourth Amendment rights of suspects, raising the prospect not only of suppression of evidence, but also potentially of civil liability for civil-rights violations.[56]

### *C. Collateral Damage*

An additional concern with the widespread use of Stingrays is that they do not engage only the targeted phone belonging to a suspect. They engage every phone within a certain radius of where they are operating.[57] If Stingray tracking of a suspect's phone is not a search for Fourth Amendment purposes, and a warrant and probable cause is not needed to engage in it, then the inadvertent tracking of other "innocent" phones in the vicinity would not change the constitutional calculus.

The more interesting question would arise if (1) a warrant is constitutionally required because the Court deems Stingray tracking to be a search for Fourth Amendment purposes and (2) the police with a valid warrant deployed a Stingray to track a suspect's phone, and, in executing the warrant, inadvertently obtained Stingray evidence from a bystander's phone. One possibility would be that the evidence obtained from the nearby phone would be covered by the plain-view doctrine, in the same way that an individual in a residence that is being searched pursuant to a search warrant is sometimes simply unlucky to be on the premises and engaged in their own illegal activity[58] (although searching

*Phones to Solve Routine Crimes*, USA TODAY (Aug. 24, 2015), http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

56. *See, e.g.*, 42 U.S.C. § 1983 (2012) (creating a statutory cause of action for civil-rights violations by state actors); Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) (recognizing a federal cause of action in tort for damages against federal officers, in their individual capacities, who allegedly violated the constitutional rights of a citizen). *But see* Pearson v. Callahan, 555 U.S. 223 (2009) (recognizing a qualified immunity defense for officers who violate federal civil rights that are not clearly established at the time of the violation).

57. *See Andrews*, 134 A.3d at 329 n.4; *cf.* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014), http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533 (describing the government's regular use of airplanes as large-scale Stingrays that can "scoop data from tens of thousands of cellphones in a single flight, collecting their identifying information and general location").

58. *Cf.* Horton v. California, 496 U.S. 128 (1990) (holding that the Fourth Amendment did not prohibit the warrantless seizure of evidence of a crime discovered in plain view, even if the discovery of the evidence was not inadvertent); Texas v. Brown, 460 U.S. 730, 737–39 (1983) (holding that, when the police were lawfully in premises, they could seize any evidence in plain view or take further action supported by any consequent probable cause); Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (explaining how the plain-view doctrine applies when the police have a warrant to search a given area for specified objects and, in the course of the search, came across some other article of incriminating character and when they are not searching for evidence against a particular individual but nonetheless

three cell phones on the authority of a warrant authorizing the search of only one because the police lack the technological means to narrow their searches does not seem quite analogous). The more apt plain-view analogy would be the interception of phone information from one individual who was communicating with a second individual whose phone was subject to a Stingray warrant, in the same way that a wiretap warrant for one phone will inevitably lead to the "plain-view" seizure of the conversation of the caller on the other end of the listened-to calls.[59]

In addition to judicial authorization and probable cause, the Fourth Amendment also requires that warrants comply with a separate particularity requirement: that the warrant state the items to be searched and seized specifically, in advance of issuance.[60] Traditionally, particularity issues have arisen when the police obtained a warrant to search one individual's residence but, on execution, also searched the residence of another individual, who was not named in the warrant (and, therefore, for whom probable cause was lacking)—perhaps because the suspect and the second individual were roommates or lived in separate units of a single building or the police simply misunderstood the nature of the suspect's living arrangements.[61] More recently, courts have struggled with applying the particularity requirement to computers, since it can be difficult to predict exactly what will be found where in a computer's hard drive prior to executing a warrant to search it.[62] Similar

inadvertently come across an incriminating object). *But cf.* Ybarra v. State of Illinois, 444 U.S. 85 (1979) (holding that a search warrant, issued on probable cause, gave police officers the authority to search the premises of a public tavern and to search the bartender for narcotics, but not to seize and pat down a tavern patron in the absence of a reasonable belief that he was involved in any criminal activity or was dangerous); Bragg v. State, 536 So.2d 965 (Ala. Crim. App. 1988) (holding that a search warrant that designated specific people and premises to be searched did not authorize officers to conduct search of unnamed people present on the premises when the warrant was executed); Hayes v. State, 234 S.E.2d 360 (Ga. Ct. App. 1977) (holding that a warrant to search premises did not justify officers in engaging in a personal search of a suitcase belonging to a person not named in the warrant); State v. Vandiver, 891 P.2d 350 (Kan. 1995) (holding that the police, when executing a search warrant of premises, could only search a nonresident visitor or the visitor's belongings if there is additional justification to support the search); State v. Wynne, 552 N.W.2d 218 (Minn. 1996) (holding that the search of Wynne's purse, which was taken from her and carried into her mother's home when she arrived there during the execution of a search warrant, was beyond the scope of what the warrant authorized).

59. *See, e.g.*, United States v. Baranek, 903 F.2d 1068, 1070–71 (6th Cir. 1990). The Wiretap Act requires agents to employ "minimization procedures" to avoid interception of non-relevant conversations, but does not prohibit their incidental interception. *See* 18 U.S.C. § 2518(5) (2012); *see generally* United States v. Manfredi, 488 F.2d 588 (2d Cir. 1973); United States v. Armocida, 515 F.2d 29, 42 (3d Cir. 1975); United States v. Clerkley, 556 F.2d 709, 716 (4th Cir. 1977); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994); United States v. Quintana, 508 F.2d 867 (7th Cir. 1975); United States v. Chavez, 533 F.2d 491 (9th Cir. 1976); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000); United States v. Scott, 516 F.2d 751 (D.C. Cir. 1975).

60. *See* U.S. CONST. amend IV.

61. *See, e.g.*, Maryland v. Garrison, 480 U.S. 79 (1987).

62. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (reviewing the execution of warrants during the course of the Government's investigation into the Bay

particularity issues could arise with a warrant to target one cell phone in a situation in which it is almost inevitable that other, nearby "innocent" phones would get caught up in the surveillance net.[63]

### *D. Secrecy*

Another aspect of Stingrays that distinguish them from other forms of location tracking is the secrecy shrouding their use. The primary manufacturer of IMSI catchers for American law-enforcement agencies is the Harris Corporation (Harris).[64] It is a poorly kept secret that Harris insists on a nondisclosure agreement (NDA) as a condition of selling IMSI catchers to law-enforcement agencies.[65] The NDAs that Harris requires were instigated, in turn, at the insistence of the FBI, required by the Federal Communications Commission.[66] While the language varies across contracts, these extraordinary NDAs generally require not only that the law-enforcement agency protect the operation and even *existence* of the IMSI technology from disclosure, but also that law-enforcement agencies immediately notify the FBI if they receive a request, motion, or court order seeking or ordering disclosure of information relating to the technology, in time for the FBI to intervene to block disclosure. If the FBI requests it, local prosecutors must dismiss charges or agree to suppression of evidence[67] if doing so is

---

Area Laboratory Collective for providing steroids to Major League Baseball players, rejecting the Government's argument that data of hundreds of players who were not targets of the investigation were in plain view during its legal search for records pertaining to the ten initial targets, and suppressing the other players' information because of the Government's failure to segregate information as to which it had probable cause from the other records that were swept up during the seizures); *see generally* Carrie Leonetti, *Code 9: Digital Data as a Fourth-Amendment Analogue for "Abandoned" DNA*, 17 COLUMBIA SCI. & TECH. L. REV. 1, 17 (2015).

63. *See* Diedrich, *supra* note 54.

64. *See* State v. Andrews, 134 A.3d 324, 338 (Md. Ct. Spec. App. 2016); Robert Kolker, *What Happens When the Surveillance State Becomes an Affordable Gadget*, BLOOMBERG BUS. WEEK (Mar. 10, 2016), http://www.bloomberg.com/news/articles/2016-03-10/what-happens-when-the-surveillance-state-becomes-an-affordable-gadget; David Z. Morris, *Maryland Court Says Phone Tracking Unconstitutional*, FORTUNE (Apr. 3, 2016), http://fortune.com/2016/04/03/maryland-court-phone-tracking/.

65. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 1-18 (2015); Brinson, *supra* note 5.

66. *See* Brinson, *supra* note 5.

67. When a defendant has a good-faith basis to suspect that evidence being offered at trial was illegally obtained, he or she can file motion to suppress the evidence, usually pursuant to the exclusionary rule for evidence derived from violations of the Fourth Amendment. *See* U.S. CONST., amend. IV. If a court believes that the claim of illegality is colorable, it will typically order a hearing to determine: (1) whether a government search or seizure was illegal, (2) if so, what subsequent evidence was derived from the illegal search or seizure, and (3) whether an exception to the exclusionary rule nonetheless permits introduction of some or all of the derivative evidence. If the search or seizure being challenged was conducted without a warrant, the prosecution bears the burden at each step of the proceedings—i.e., to prove either that the search or seizure was legal, the evidence at issue was not

necessary to protect the secrecy behind the devices, their operation, or their use.[68] Even searches on the Harris public website, which advertises a broad array of cyber products for militaries and law-enforcement agencies, searches for "IMSI," "Stingray," and "Hailstorm" produces no results.[69] One investigation revealed that police departments in Florida intentionally and deceptively had concealed their use of Stingrays in court documents, characterizing them as "confidential source[s]."[70]

Adherence to the NDAs have resulted in several reported cases in which a local prosecutor's office has agreed to the suppression of evidence, dismissed charges, or suffered sanctions for refusing to disclose information relating to Stingrays when ordered to do so by a court, often after the court has rejected a claim that the information is protected by a trade- or state-secrets privilege.[71] Dismissal, however, does not end the constitutional controversy. The secrecy surrounding the operation and use of Stingrays by law-enforcement agencies has created subsidiary legal controversies surrounding the extent to which the targets (intentional or inadvertent) of Stingray searches have a legal right to obtain information about the investigatory procedures by which the police accessed their phone location information.[72]

Courts are often divided between sympathy for and outrage with law-enforcement attempts to conceal their use of Stingrays. A federal court in California recently issued a blistering criticism of the United States Department of Justice's (DoJ) refusal to reveal whether, when, and how law-enforcement agents used Stingray tracking in 2013 to locate the defendant, Purvis Ellis, in a federal gang-related attempted-murder case involving the shooting of an Oakland Police Department officer.[73] In

---

derived, in a causal sense, from the illegality, and/or that the evidence is nonetheless admissible. *See Andrews*, 134 A.3d at 340 n.11; Jones v. State, 775 A.2d 421, 428–29 (Md. Ct. Spec. App. 2001). To meet these burdens, the prosecution inevitably calls a lead investigator to describe the challenged search or seizure procedure in detail and to explain its putative legal justification.

68. *See, e.g.*, *Andrews*, 134 A.3d at 338.

69. *See* HARRIS, https://www.harris.com (last visited July 19, 2016).

70. *See* Cyrus Farivar, *Legal Experts: Cops Lying About Cell Tracking "Is a Stupid Thing to Do*," ARS TECHNICA (June 20, 2014), http://arstechnica.com/tech-policy/2014/06/legal-experts-cops-lying-about-cell-tracking-is-a-stupid-thing-to-do/ [hereinafter "Farivar, *Cops Lying*"].

71. *See, e.g.*, Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, BALT. SUN (Nov. 17, 2014), http://bsun.md/1xdVWJR; Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH. POST (Feb. 22, 2015), https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html.

72. *See, e.g.*, Diedrich, *supra* note 54 (describing a Milwaukee Circuit Court judge's order for an evidentiary hearing regarding police use of a Stingray to locate a murder defendant); Farivar, Cops *Lying*, *supra* note 70.

73. *See* Cyrus Farivar, *Judge Blasts DOJ's Refusal to Explain Stingray Use in Attempted Murder Case*, ARS TECHNICA (Aug. 10, 2016), http://arstechnica.com/tech-policy/2016/08/judge-blasts-dojs-

another case, however, a state judge in Florida allowed the United States Marshals Service to seize Stingray records from a local police department in order to shield them from disclosure under open-records laws.[74]

## V. FIRST FORAYS

A few courts have ventured into this unchartered territory of warrantless Stingray searches, and they have so far come down on the side of finding them to be unconstitutional. In *State v. Andrews*,[75] the Maryland Court of Special Appeals addressed the question of whether Kerron Andrews had a reasonable expectation of privacy in his real-time cell-phone location information, such that a warrant and probable cause were required before the police could obtain it using a Hailstorm. The Baltimore Police Department (BPD) had an arrest warrant for Andrews for attempted murder and a warrant for his cell phone authorizing CSLI from his service provider and the use of a pen register to track its metadata, but it did not have a warrant specifically authorizing it to employ a cell-site simulator to locate him.[76] Andrews's cell-service provider gave BPD the unique identifier for Andrews's cell phone and real-time CSLI.[77] The police were able to use the CSLI to identify the apartment complex in which Andrews cell phone was located, but not the precise apartment.[78] BPD then used its Hailstorm to track his cell phone (which was in his pants pocket) and locate him in the living room of a specific apartment, where officers arrested him.[79] A subsequent search of the apartment uncovered a gun in the cushions of the couch on which Andrews had been sitting.[80]

On appeal, the State defended the warrantless use of the Hailstorm as analogous to the radio-beacon tracking in *Knotts*.[81] The Maryland Court

refusal-to-explain-stingray-use-in-attempted-murder-case/ [hereinafter "Farivar, *Refusal to Explain*"].

74. *See* Farivar, *Cops Lying*, *supra* note 70.

75. 134 A.3d 324 (Md. Ct. Spec. App. 2016).

76. *Id.* at 327–28. Under *Smith*, the Fourth Amendment does not require a warrant before the police use a pen-register device. Smith v. Maryland, 442 U.S. 735 (1979). Maryland requires judicial authorization for such devices; however, the statute does not require a "warrant" in the Fourth Amendment sense, and the authorization can be granted on a showing of less than probable cause. *See* Maryland Pen Register, Trap and Trace Statute, MD. CODE ANN., CTS. & JUD. PRO., §§ 10–4B–02 to -04. Nonetheless, in issuing the pen-register warrant for Andrews's phone, the magistrate judge specifically found that probable cause existed to believe that Andrews's cell phone was relevant to the ongoing investigation of Andrews for attempted murder. See *Andrews*, 134 A.3d at 328.

77. *Andrews*, 134 A.3d at 331.

78. *Id.* at 329.

79. *Id.* at 326–29.

80. *Id.* at 329.

81. *Id.* at 347.

of Appeals rejected the analogy,[82] upholding the trial court's suppression of the evidence found in the residence as a result of the Hailstorm search, holding:

> We conclude that people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement, and—recognizing that the Fourth Amendment protects people and not simply areas—that people have an objectively reasonable expectation of privacy in real-time cell phone location information. Thus, we hold that the use of a cell site simulator requires a valid search warrant, or an order satisfying the constitutional requisites of a warrant, unless an established exception to the warrant requirement applies.[83]

The court also addressed what it described as the "extensive prohibition on disclosure of information to the court" contained in Harris's NDA with BPD, which it characterized as "prevent[ing] the court from exercising its fundamental duties under the Constitution."[84]

In *United States v. Lambis*,[85] under facts very similar to those of *Andrews*, the United States District Court for the Southern District of New York granted Raymond Lambis's motion to suppress drug-trafficking evidence the Drug Enforcement Agency (DEA) seized during a search of his apartment, which the DEA had located by way of warrantless Stingray tracking of his cell phone.[86] Like the BPD in *Andrews*, the DEA had warrants to place a pen register and acquire real-time CSLI from Lambis's phone. Once the CSLI had narrowed Lambis's location to several apartment complexes in Washington Heights, however, the DEA used a Stingray, without an additional warrant, to narrow Lambis's location to a specific building and then specific apartment.[87] The DEA knocked on the door and received consent from Lambis's father to search his bedroom, where they discovered evidence of drug trafficking.[88]

The court granted Lambis's motion to suppress the evidence that resulted from the Stingray tracking, holding: "The use of a cell-site simulator constitutes a Fourth Amendment search within the contemplation of *Kyllo*. Absent a search warrant, the Government may

82. *Id.* at 347–48.

83. *Andrews*, 134 A.3d. at 327.

84. *Id.* at 338.

85. 197 F. Supp. 3d 606 (S.D.N.Y. 2016).

86. *Id.* at 608–09.

87. *Id.* at 609.

88. *Id.*

not turn a citizen's cell phone into a tracking device."[89] The court also rejected the Government's defense of the warrantless Stingray tracking under the third-party doctrine, for two reasons. First, cell-phone users do not voluntarily give their location information to service providers in the same way that Smith voluntarily gave his call information to his phone company. Second, the Government acquired the location information directly from Lambis's phone, not via a third-party service provider.[90]

## VI. CONCLUSION

The uncertainty surrounding the constitutionality of Stingray tracking has caused some criminal-justice agencies to begin self-regulating its use. Most notably, DoJ and the Department of Homeland Security recently announced new Stingray policies for federal law-enforcement officers, requiring them to seek warrants supported by probable cause before employing cell-site simulators.[91] Of course, because this policy is an internal one, it is temporary and discretionary (as opposed to the mandatory operation of a court's constitutional ruling on the subject), does not govern local (state, county, municipal) police agencies, and its violation would not necessarily (or likely) give rise to a suppression remedy.[92] Earlier this year, Vermont also passed a sweeping privacy statute that, *inter alia*, bans the use of cell-site simulators for any use other than catching dangerous fugitives,[93] and California requires a warrant for their use.[94]

While Stingray technology is new, the constitutional dilemmas that it invokes are not. At the end of the day, Stingrays are just the variation du jour of the broader theme that the *Katz* test has failed to keep up with technological changes, and the queue of constitutionally questionable high-tech surveillance grows longer with each passing term. Did *Miller* and *Smith* authorize the National Security Agency's warrantless collection of communications metadata from Americans? Do they authorize the warrantless collection of historical CSLI from service providers? If they do, do they reach to real-time CSLI, as well? Can the

89. *Id.* at 611.

90. *Id*. at 614–16; Farivar, *Refusal to Explain*, *supra* note 73.

91. *See Lambis*, 197 F. Supp. 3d at 611; State v. Andrews, 134 A.2d 324, 357 n.20 (Md. Ct. Spec. App. 2016). This policy was not in place at the time that the alleged tracking occurred in the *Ellis* case. *See* Farivar, *Refusal to Explain*, *supra* note 73.

92. *Cf.* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Could Change Computer Crime Law*, 54 HASTINGS L.J. 805, 806 (2003) (explaining the absence of a suppression remedy for surveillance techniques that violate statutes but not the Fourth Amendment).

93. *See* 2015 Vt. Adv. Legis. Serv. 169 (LexisNexis).

94. *See* Farivar, *Refusal to Explain*, *supra* note 73.

government engage in warrantless GPS tracking of suspects as long as its agents do not trespass to install the device on the suspect's car? If warrantless GPS tracking and CSLI acquisition are constitutional, is Stingray just another means of accomplishing the same data collection? The Supreme Court needs to address the applicability of *Smith* and *Miller* to high-tech data mining and analysis, and it needs to do so in a systematic way that addresses not only today's newest technology, but by providing a systematic framework by which tomorrow's searches can be judged, as well.