Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 26 *Volume XXVI*
Number 4 *Volume XXVI Book 4*

Article 4

2016

The Fourth Amendment Implications on the Real-Time Tracking of Cell Phones Through the Use of "Stingrays"

W. Scott Kim
Fordham University School of Law

The Fourth Amendment Implications on the Real-Time Tracking of Cell Phones Through the Use of "Stingrays"

Cover Page Footnote

Associate Editor, Fordham Intellectual Property, Media & Entertainment Law Journal, Volume XXVII; J.D. Candidate, 2017, Fordham University School of Law; B.S., 2013, Seton Hall University.

I would like to thank Professor Olivier Sylvain for introducing me to this topic and for being an instrumental advisor throughout. I would also like to thank the Fordham IPLJ staff and editors, especially Liz Walker, Patrick O'Keefe, and Katie Rosenberg.

The Fourth Amendment Implications on the Real-Time Tracking of Cell Phones Through the Use of "Stingrays"

W. Scott Kim*

The rights secured to us by the Fourth Amendment were the driving force behind the American Revolution. Today, law enforcement seems to forget that fact when they use cell-site simulators, commonly referred to by the brand name "Stingray," without first securing a warrant. These devices mimic cell phone towers and force cell phones near them to connect to the cell-site simulator instead of a tower, thereby allowing the user of the simulator device to track a cell phone to its precise location.

Ninety-two percent of Americans own a cell phone and forty-six percent of smartphone users say they could not go a single day without them. Cell phones are not just another modern convenience, they are a part of modern life and people should not have to sacrifice a near necessity in today's world in order to secure their privacy. This Note analyzes the conflict between the Fourth Amendment and the use of cell-site simulator technology and argues that the use of a Stingray constitutes a Fourth Amendment search and should require a warrant prior to its use.

---

* Associate Editor, *Fordham Intellectual Property, Media & Entertainment Law Journal,* Volume XXVII; J.D. Candidate, 2017, Fordham University School of Law; B.S., 2013, Seton Hall University. I would like to thank Professor Olivier Sylvain for introducing me to this topic and for being an instrumental advisor throughout. I would also like to thank the Fordham IPLJ staff and editors, especially Liz Walker, Patrick O'Keefe, and Katie Rosenberg.

INTRODUCTION

Cell phone users know that when making a call from their cell phone, the phone has to connect to a cell tower.[1] They are also aware that they are conveying their cell tower location to their service provider, who may then give it to a law enforcement agency to track them.[2] What they do not know is that their cell phone may not be connecting to a cell tower at all, but instead to a device known as a "cell-site simulator," commonly referred to by the brand name "Stingray."[3] These devices send out signals of their own and force cell phones in the area to transfer their locations and identifying information to it instead of a cell tower, all without ever alerting the user of the phone.[4] With these devices, the government can determine at what time and to whom you are calling each time you place a call, the location of every phone in the area, and with certain devices, even listen in on your conversations and texts.[5]

Law enforcement agencies typically use Stingrays in three ways: (1) to find an individual whose cell phone number they have in order to determine his location;[6] (2) to follow an individual whose cell phone number they do not have to various locations in order to analyze the numbers at each location and determine the targeted individual's number;[7] or (3) to capture the cell phone data

---

1 *See* United States v. Davis, 785 F.3d 498, 510 (11th Cir. 2015).

2 *See id.*

3 *See Stingray Tracking Devices: Who's Got Them*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them [https://perma.cc/C85Q-SPPX] (last visited Feb. 24, 2016) [hereinafter *Who's Got Them*].

4 *Id.*

5 Hanni Fakhoury & Trevor Timm, *Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About*, ELECTRONIC FRONTIER FOUND. (Oct. 22, 2012), https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy [https://perma.cc/SYR4-529T]; *see also* Dina Rasour, *Protesters Beware: Don't Get Stung by Stingrays*, OCCUPY.COM (Sept. 17, 2014), http://www.occupy.com/article/protesters-beware-don%E2%80%99t-get-stung-stingrays [https://perma.cc/RC7Q-VB74].

6 *See* Larry Greenemeier, *What Is the Big Secret Surrounding Stingray Surveillance?*, SCI. AM. (June 25, 2015), http://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/?page=1[https://perma.cc/48CA-NLAA].

7 *See id.*

of everyone in attendance at rallies and protests.[8] Law enforcement's use of a Stingray typically begins with them driving around from place to place with the device in order to narrow in on the target cell phone's location by gathering the phone's signal strength at each point, resulting in a far more precise location than what could have been ascertained from cell tower records.[9] This process can lead law enforcement right to the doorstep of the phone's location, allowing law enforcement to switch to a handheld Stingray if necessary to walk through the building and hone in on the exact room where the target phone is located.[10]

However, even in those situations where law enforcement is only trying to locate one particular person, Stingrays do not only collect the data of the target.[11] Rather, they collect the data from every single phone near it, within a range of several kilometers, by making each phone connect to it every seven to fifteen seconds.[12] This means potentially thousands of innocent people's phones could be searched with no one but law enforcement knowing about it.[13] The safety of a person's home will not stop a Stingray either, as the device is able to track the location of a cell phone through walls.[14]

The Department of Justice ("DOJ") released a new policy on the use of Stingrays for federal officers in September 2015[15] but at least sixty-one law enforcement agencies in twenty-three states, plus the District of Columbia, also have Stingrays and most use

---

8 *See id.*

9 Kim Zetter, *The Feds Are Now Using 'Stingrays' in Planes to Spy on Our Phone Calls*, WIRED (Nov. 14, 2014, 2:14 PM), http://www.wired.com/2014/11/feds-motherfng-stingrays-motherfng-planes/ [https://perma.cc/UZE9-PWNA].

10 *See id.*

11 *See* Fakhoury & Timm, *supra* note 5; Timothy Williams, *Covert Electronic Surveillance Prompts Calls for Transparency*, N.Y. TIMES (Sept. 28, 2015), http://www.nytimes.com/2015/09/29/us/stingray-covert-electronic-surveillance-prompts-calls-for-transparency.html [https://perma.cc/J4AS-RYGC].

12 *See* Fakhoury & Timm, *supra* note 5; Rasour, *supra* note 5.

13 *See* Fakhoury & Timm, *supra* note 5.

14 *See Stingrays*, AM. CIV. LIBERTIES UNION VA. (Oct. 2014), http://acluva.org/wp-content/uploads/2014/10/140905-Stingray-one-pager.pdf [https://perma.cc/F22N-Q8KN].

15 *See* DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY (Sept. 3, 2015), http://www.justice.gov/opa/file/767321/download [https://perma.cc/7N4A-V22M] [hereinafter DOJ Policy].

them without any policy guidelines or statutes in place instructing law enforcement on how to use the devices in compliance with the Fourth Amendment.[16] This is where the problem lies—should law enforcement agencies be able to use Stingrays without at least obtaining a warrant first? Part I provides a background on the political landscape today. Part II discusses the evolution of the Fourth Amendment. Part III conducts an analysis on the use of a Stingray in the context of the Fourth Amendment. Lastly, Part IV provides a recommendation on the use of Stingrays in the future.

I. THE CURRENT USE OF STINGRAYS

This Part discusses how Stingrays are being used in present day. Section I.A explains the history behind the development and use of the Stingray. Section I.B examines the new federal policies in place. Section I.C discusses Stingray use at the state level. Lastly, Section I.D focuses on the differences between a Stingray and pen register, and the issue this presents.

A. A History on the Use of Stingrays

Originally created for the military and spy agencies,[17] Federal and state agencies began using cellular surveillance techniques as early as the 1990s. It is impossible to know the exact beginning of their use due to the secret nature of the devices, but the first indication of use by federal, state, and local law enforcement and intelligence agencies was in 1991 when they began using passive surveillance techniques.[18] Devices more similar to the Stingray, which

---

[16] *See Who's Got Them*, *supra* note 3. Approximately eleven states have laws regarding law enforcement's tracking of cell phones. Brandon Ellington Patterson, *Police Use This Secret Military Snooping Gadget to Track Cell Phones. But Is It Legal?*, MOTHER JONES (Apr. 4, 2016, 6:00 AM), http://www.motherjones.com/politics/2016/03/maryland-stingray-appeals-court-opinion [https://perma.cc/D2L8-HFND]. At least five states have enacted statutes mandating a warrant before their use. *See infra* notes 84–88.

[17] *See* John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 8, 2013), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ [https://perma.cc/6ND4-G9U6].

[18] *See* Glen L. Roberts, *Who's on the Line? Cellular Phone Interception at Its Best*, FULL DISCLOSURE (1991), http://67.225.133.110/~gbpprorg/2600/harris.txt [https://perma.cc/TU5X-QZEP] (describing the marketing of TriggerFish devices to law enforcement agencies at the National Technical Investigators Association conference in 1991). Passive

were capable of active surveillance, were used by the federal government and loaned to local and state law enforcement agencies starting as early as 1995.[19]

The precursor to the Stingray is generally believed to be an IMSI Catcher developed in 1996 by Rohde & Schwarz, a German manufacturer of radio equipment.[20] It was the first purpose-built active device capable of performing surveillance on cellphones by forcing phones to transmit their serial number to it.[21] As for the development behind the Stingray itself, which was developed by Harris Corporation ("Harris"), not much is known publicly. Harris is the exclusive manufacturer of the Stingray and discloses no details regarding the Stingray on its website.[22] The user manual provided with a Stingray warns that the device should only be distributed to persons eligible under 18 U.S.C. § 2512, which includes law en-

---

surveillance means the device "intercepts the signals sent between nearby phones and the wireless provider's network. . . . [T]hey can only detect signals of nearby phones when those phones are actually transmitting data." Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J. L. & TECH. 1, 9–13 (2014) (internal citations omitted).

19 *See FBI FOIA Releases, EPIC v. FBI, No. 12-0667 (D.D.C.)—Fifth Release*, ELECTRONIC PRIVACY INFO. CTR. 260 (Feb. 7, 2013), https://epic.org/foia/fbi/stingray/FBI-FOIA-Release-02072013-OCR.pdf [https://perma.cc/PYF4-8PXN] ("By Department Order 1945-95, dated January 18, 1995 (replacing Department Order 890-80, dated Apri1 29, 1980), the Attorney General delegated to the Federal Bureau of Investigation the authority to approve loans of electronic surveillance equipment to state and local law enforcement agencies for use in their investigations . . . ."). Active surveillance means the device "works by impersonating a wireless base transceiver station . . . the carrier-owned equipment installed at a cell tower to which cellular phones connect—and tricking the target's phone into connecting to it" allowing the device to "identify nearby phones, locate them with extraordinary precision, intercept outgoing calls and text messages, as well as block service, either to all devices in the area or to particular devices." Pell & Soghoian, *supra* note 18, at 11–12 (internal citations omitted).

20 *See* Daehyun Strobel, IMSI Catcher 13 (July 13, 2007) (unpublished seminar paper, Ruhr-Universitat Bochum), https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf [https://perma.cc/V7JZ-ZPZ4]. "IMSI" is short for International Mobile Subscriber Identity. *Id.* at 4.

21 *See* Pell & Soghoian, *supra* note 18, at 13–14.

22 *See* HARRIS CORP., http://harris.com/ [https://perma.cc/5JHC-HZ4E] (last visited Feb. 24, 2016).

forcement and communications service providers,[23] while the Federal Communications Commission ("FCC") requires local law enforcement to coordinate with the Federal Bureau of Investigation ("FBI") before acquiring a Stingray.[24] The FBI then requires the local agency to sign a non-disclosure agreement before acquiring a Stingray.[25] Due to all this secrecy, the earliest public indication of the invention of the Stingray is found at the Patent and Trademark Office when Harris trademarked the name "Stingray" in 2003.[26]

Despite this indication that Stingrays have been around since 2003, the use of Stingrays by law enforcement agencies did not surface until 2011, when Daniel David Rigmaiden combed through 15,000 pages of court documents in an attempt to find out how authorities located him.[27] Rigmaiden undertook numerous steps to avoid detection, including fake IDs, keeping a low public profile, and living in the woods.[28] Thus, when he was found, he suspected the only weak link in his attempt to remain anonymous was a cellular aircard he used to connect to the Internet.[29] This suspicion was confirmed when Rigmaiden discovered that the FBI was able to locate him precisely inside his apartment because a Stingray tracked the aircard connected to the laptop in his apartment.[30]

---

[23] *See* 18 U.S.C. § 2512(b) (2012); HARRIS ASSURED COMMC'NS, HARDWARE MANUAL 3 (2010), https://cryptome.org/2015/03/fcc-stingray-final.pdf [https://perma.cc/A25X-JACB]. A violation under § 2512 is punishable by up to five years in prison. *See* § 2512(a).

[24] Tim Cushing, *FCC Denies It Requires Law Enforcement to Sign a Non-Disclosure Agreement with the FBI Before Deploying Stingray Devices*, TECHDIRT (Oct. 10, 2014, 1:33 PM), https://www.techdirt.com/articles/20141008/13471728772/fcc-denies-it-requires-law-enforcement-to-sign-non-disclosure-agreement-with-fbi-before-deploying-stingray-devices.shtml [https://perma.cc/895L-4VP6].

[25] *See id.*

[26] STINGRAY, Registration No. 76,303,503.

[27] *See* Cale Guthrie Weissman, *How an Obsessive Recluse Blew the Lid Off the Secret Technology Authorities Use to Spy on People's Cell Phones*, BUS. INSIDER (June 19, 2015, 5:04 PM), http://www.businessinsider.com/how-daniel-rigmaiden-discovered-stingray-spying-technology-2015-6 [https://perma.cc/566D-WA5M].

[28] *Id.*

[29] *See id.*

[30] *See* Response to Government's Memorandum Regarding Law Enforcement Privilege and Request for an Ex Parte and In Camera Hearing if Necessary at Exhibit 38, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC) [hereinafter Investigative Details Report] (detailing how agents of the FBI and U.S. Postal Inspection Service used a Stingray to track and pinpoint the signal of Rigmaiden's aircard after only a few hours).

Rigmaiden was ultimately charged with various counts of tax fraud arising from an alleged scheme he had concocted where he filed tax returns on behalf of various people who had passed away in order to recover the proceeds from their refunds.[31] However, without the use of the Stingray, the government would not have been able to narrow the location of Rigmaiden's aircard down to his specific apartment, but instead would have gotten no closer than knowing the aircard was in the Santa Clara/San Jose area through the use of historical cell tower data obtained from Verizon.[32] This illustrates the massive difference a Stingray's tracking ability can make in a man hunt because of its ability to generate "real time data during the tracking process."[33]

Prior to tracking the aircard with the Stingray, the government obtained a "tracking warrant," which is a search warrant issued pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure that authorizes the use of a cell-site simulator.[34] Rigmaiden filed a motion to suppress, raising several Fourth Amendment challenges, arguing that "the warrant is not supported by probable cause, that it lacks particularity, that the government's searches and seizures exceeded the warrant's scope, and that agents executed the warrant unreasonably because they failed to comply with inventory and return requirements."[35] The American Civil Liberties Union ("ACLU"), through an amicus brief, raised several issues with the warrant as well—"that the search exceeded the scope of the warrant because the warrant authorized Verizon, not the government, to locate the aircard, and that the warrant was misleading and incomplete because it failed adequately to describe the technology involved in the search."[36] Ultimately, the government stipulated arguendo for the purposes of the motion to suppress that the tracking of Rigmaiden with the device was a Fourth Amendment search

---

31 *Rigmaiden*, 844 F. Supp. 2d at 987.

32 *See* Investigative Details Report, *supra* note 30.

33 *See* United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013).

34 *See id.* at *14; *see also* FED. R. CIV. P. 41(b).

35 *See Rigmaiden*, 2013 WL 1932800, at *14.

36 *Id.*

and seizure.[37] Despite this concession, the federal government's position remained that the use of a Stingray, including its use here, is not a search or seizure under the Fourth Amendment.[38]

One potential reason for making such a concession was to prevent the disclosure of information that could have been exposed about the use of Stingrays through discovery, pre-trial motions, and related hearings had the government defended the Fourth Amendment issues with use of a Stingray factually. The FBI has always asserted that information about the use of cell-site simulators is "law enforcement sensitive" and that if such information was made public, it could easily impair the use of this investigative method.[39] The federal government in *United States v. Rigmaiden* made this exact argument.[40] This shows how important it is to the federal government to keep the cell-site simulator technology secret. Therefore, by conceding the factual argument on whether a Stingray constitutes a Fourth Amendment search and instead making an argument at the suppression stage, there were less demand-

---

[37] *See* Government's Memorandum re Motion for Discovery at 1, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC) [hereinafter Motion for Discovery].

[38] *Id.* at 1 n.1 ("The United States explained in its March 11, 2011, Memorandum Regarding Law Enforcement Privilege that Defendant does not have a reasonable expectation of privacy in his general location or in the cell site records he transmitted wirelessly to Verizon. Therefore, the use of the cell-site simulator is not a search under the Fourth Amendment. Nevertheless, in an attempt to simplify the analysis and to avoid unnecessary disclosure of privileged information, the United States will no longer argue in this case only that the aircard tracking operation was not a search or seizure under the Fourth Amendment, and will instead rely on its authority under the hybrid order and tracking warrant, Defendant's lack of standing, and, if necessary, the agents' good faith reliance on these court orders." (internal citations omitted)).

[39] *Affidavit of Bradley S. Morrison*, SAN DIEGO CITY ATT'Y OFF. 2 (Apr. 11, 2014), http://www.sandiego.gov/cityattorney/pdf/news/2014/nr141222c.pdf [https://perma.cc/2K5J-JMLB].

[40] *See Rigmaiden*, 844 F. Supp. 2d at 989 ("[T]he government contends that the technology used to locate Defendant's aircard, the manner in which the technology was employed, and the identities of the agents who operated the equipment all constitute sensitive law enforcement information subject to the qualified privilege recognized in *Roviaro* and *Van Horn*."). The court cited two cases that essentially hold that the government can shield information about sensitive investigative techniques when a court determines that such disclosure would not be relevant or helpful to the defense or "is essential to a fair determination of a cause." Roviaro v. United States, 353 U.S. 53, 60–61 (1957); *see also* United States v. Van Horn, 789 F.2d 1492, 1507 (11th Cir. 1986).

ing disclosure requirements.[41] This strategy reduced the likelihood that any information would become available to the public, which seems to be the federal government's main concern.

It is interesting to note nonetheless that the government still obtained a warrant in this case prior to using the Stingray.[42] The prosecutors of the case even recognized that the Supreme Court holding that when "the government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant" would likely apply to law enforcement's use of a Stingray in *Rigmaiden* had they sent a signal though the walls of his apartment to locate the aircard.[43] This is in opposition to the government's position taken in their motion for discovery and the DOJ's 2005 Guidance on Electronic Surveillance.[44] Ultimately, this inconsistency became essentially a moot point at the federal level as a result of the DOJ and Department of Homeland Security ("DHS") each releasing their respective policies on Stingrays.[45] However, whether the use of a Stingray requires a warrant remains an issue at the state and local levels.

---

[41] *See Rigmaiden*, 844 F. Supp. 2d at 990; *see also* United States v. Garey, No. 5:03-CR-83, 2004 WL 2663023, at *4 n.7 (N.D. Ga. Nov. 15, 2004) ("[T]he reasons for requiring disclosure of privileged information at the search warrant stage are less compelling than those for disclosure in preparation for trial." (citing McCray v. Illinois, 386 U.S. 300, 311 (1967)).

[42] *See* text accompanying *supra* note 34.

[43] *See* Pell & Soghoian, *supra* note 18, at 31 n.160 (quoting Kyllo v. United States, 533 U.S. 27, 40 (2001)).

[44] *See supra* note 38; *see also* ELEC. SURVEILLANCE UNIT, U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 48 (2005), http://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf [https://perma.cc/J2CC-23WE] ("The amended text of the pen/trap statute and the limited legislative history accompanying the 2001 amendments strongly suggest that the non-content information that passes between a cellular phone and the provider's tower falls into the definition of 'dialing, routing, addressing, and signaling information' for purposes of the definitions of 'pen register' and 'trap and trace device.' A pen/trap authorization is therefore the safest method of allowing law enforcement to collect such transmissions directly using its own devices.").

[45] *See infra* Section I.B.

B. Federal Policy on the Use of Cell-Site Simulator Technology

On September 3, 2015, the DOJ released a policy for its use of cell-site simulators, requiring federal officers to obtain warrants before using them and setting limits on what data can be collected and for how long.[46] Prior to this policy, the government had long asserted that it did not need to obtain a warrant to use Stingrays, claiming that the devices operate more like a pen register because neither device captures the content of phone calls or messages.[47]

The DOJ policy provides, in pertinent parts, that information collected by Stingrays is limited to the numbers being dialed and the signal direction of the cell phone, as opposed to GPS data.[48] The policy prohibits Stingrays from collecting the content of phone conversations, text messages, emails, or application data.[49] The collected information must be deleted no later than thirty days after its collection if law enforcement's target is not known, or as soon as the identity of the target is ascertained.[50] There are exceptions for "exigent circumstances" and "exceptional circumstances," with exigent being broadly defined and exceptional not defined at all.[51] This new policy does not apply to state and local law enforcement agencies or other federal agencies, unless a DOJ component is using the device "in support of other federal agencies and/or state and local law enforcement agencies."[52] Simply put, the policy only

---

[46] *See* DOJ POLICY, *supra* note 15.

[47] *See* Kim Zetter, *Florida Cops' Secret Weapon: Warrantless Cellphone Tracking*, WIRED (Mar. 3, 2014, 9:00 AM), http://www.wired.com/2014/03/stingray/ [https://perma.cc/5KPF-GL4M]. The Supreme Court held that use of a pen register is not a Fourth Amendment search. *See* Smith v. Maryland, 442 U.S. 735 (1979).

[48] *See* DOJ Policy, *supra* note 15, at 2.

[49] *See id.*

[50] *See id.* at 6.

[51] *Compare id.* at 3 ("An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable. When an officer has the requisite probable cause, a variety of types of exigent circumstances may justify dispensing with a warrant. These include the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice."), *with id.* at 4 ("There may also be other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable.").

[52] *Id.* at 6.

applies to federal law enforcement and situations such as task forces where federal and local agencies share resources.[53]

A little over a month after the DOJ released its policy, the DHS also released a policy providing similar guidelines on the use of Stingrays.[54] It applies to the DHS and agencies that fall under its umbrella, such as the Secret Service, Customs and Border Protection, and Immigration and Customs Enforcement.[55] Like the DOJ's policy, the DHS policy provides that search warrants must be obtained to use cell-site simulators and provides exceptions for "exigent circumstances" and "exceptional circumstances," with the explanation for each defined in the same manner as in the DOJ policy.[56] The DHS policy also only applies to criminal investigations, meaning when the "DHS is patrolling the 'border,' conducting certain immigration activities, or monitoring conferences—no protections apply."[57] Lastly, the DHS policy, like the DOJ policy, does not apply to state or local officials unless they are working with the DHS.[58] This leaves it up to each state to individually implement policies or guidelines restricting the use of Stingrays by their law enforcement agencies.

C. Stingray Use at the State and Local Level

Rigmaiden's discovery that the federal government was using technology capable of tracking him through his cell phone led to a public desire for information on how Stingrays were being used and

---

[53] *See* Tal Kopan, *DOJ Cracks Down on Use of Cell-Duping Stingrays*, CNN (Sept. 3, 2015), http://www.cnn.com/2015/09/03/politics/stingrays-cell-site-simulator-justice-department-rules/ [https://perma.cc/J7WL-BYC6].

[54] *See* DEP'T OF HOMELAND SEC., POLICY DIRECTIVE 047-02, DEPARTMENT POLICY REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY (2015), https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf [https://perma.cc/VX9C-N699] [hereinafter DOH Policy].

[55] *See id*. at 1.

[56] *See id.* at 4–5.

[57] Neema Singh Guliani, *The Four Biggest Problems with DHS's New Stingray Policy*, AM. CIV. LIBERTIES UNION (Oct. 22, 2015, 6:00 PM), https://www.aclu.org/blog/free-future/four-biggest-problems-dhss-new-stingray-policy [https://perma.cc/N787-ULA5]. "Border" is defined as one hundred air miles from any external boundary of the United States, including coastal boundaries, unless an agency official sets a shorter distance. *See* 8 C.F.R. § 287.1(b) (2015).

[58] *See* DOH Policy, *supra* note 54, at 8.

a battle between state officials and the public over the release of this information. Information regarding Stingrays has been hard to come by because the FBI, Harris, and state agencies continually fight any requests made for information. This starts with the FBI and Harris requiring the signing of non-disclosure agreements in order for local and state law enforcement agencies to obtain Stingrays.[59]

Through a Freedom of Information Act ("FOIA") request, a non-disclosure agreement between the Erie County Sheriff's Office and the FBI seems to indicate that the FCC is the agency requiring such agreements.[60] However, documents obtained through other FOIA requests reveal a different truth. These documents show Harris made a request to the FCC for licensing restrictions[61] based on concerns from the FBI "over the proliferation of surreptitious law enforcement surveillance equipment."[62] The FCC granted this request in 2012.[63] This means that the FCC does not *require* the signing of a non-disclosure agreement, as claimed by the FBI,[64] but instead requires local law enforcement only "*coordinate* with the FBI before the purchase and use of Stingray devices."[65] As a result, it is either the FBI or Harris who is requiring the sign-

---

[59] *See* Kim Zetter, *Police Contract with Spy Tool Maker Prohibits Talking About Device's Use*, WIRED (Mar. 4, 2014, 4:34 PM), http://www.wired.com/2014/03/harris-stingray-nda/ [https://perma.cc/Y83T-BB3V]; *see also FBI Now Says Stingray Surveillance Can Be Disclosed*, RT (May 15, 2015, 6:37 PM), https://www.rt.com/usa/259105-fbi-stingray-nondisclosure-agreement/ [https://perma.cc/JAJ2-EPFT].

[60] *See* Letter Agreement Between Fed. Bureau of Investigation and Erie Cty Sheriff's Office 1 (June 29, 2012), http://www.nyclu.org/files/20120629-renondisclsure-obligations(Harris-ECSO).pdf [https://perma.cc/5XEB-X3GX] [hereinafter Erie County Nondisclosure Agreement] ("Consistent with the conditions on the equipment authorization granted to Harris Corporation by the [FCC], state and local law enforcement agencies must coordinate with the [FBI] to complete this non-disclosure agreement prior to the acquisition and use of the equipment/technology authorized by the FCC authorization.").

[61] The restrictions requested were that: "(1) the marketing and sale of these devices shall be limited to federal/state/local public safety and law enforcement officials only; and, (2) state and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization." Cushing, *supra* note 24.

[62] *Id.*

[63] *Id.*

[64] *See* Erie County Nondisclosure Agreement, *supra* note 60.

[65] Cushing, *supra* note 24 (emphasis added).

ing of a boilerplate non-disclosure agreement, as indicated by executed agreements discovered in the District of Columbia,[66] Arizona,[67] Florida,[68] New York,[69] Maryland,[70] and elsewhere.[71]

Taking the Erie County Sheriff's Office agreement as an example representative of the group, we see that the Sheriff's Office is barred from discussing any information about the surveillance tool "to the public, including any non-law enforcement individuals or agencies."[72] The Sheriff's Office may only share information with other law enforcement or government agencies with the prior written approval of the FBI.[73] Additionally, the letter stated that the Sheriff's Office "shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology."[74] If the Sheriff's Office discovers that a prosecutor or court intends to disclose such information, the Sheriff's Office must "immediately notify the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise."[75] The FBI could then require the Sheriff's Office to "seek dismissal of the case in lieu of providing, or allowing others to provide, any such information."[76] Lastly, the Sheriff's

---

[66] *See* Letter Agreement Between Fed. Bureau of Investigation and Metro DC Police Dep't (Aug. 17, 2012), https://www.scribd.com/fullscreen/283244771?access_key=key-FKWtXK9zFChGaoOck6zD&allow_share=true&escape=false&view_mode=scroll [https://perma.cc/Z34F-4W49].

[67] *See* Zetter, *supra* note 59.

[68] *See FDLE-FBI Non-Disclosure Obligations/Guidelines*, FLA. DEP'T L. ENFORCEMENT (Mar. 8, 2012), https://assets.documentcloud.org/documents/1814785/hillsborough-county-sheriff-fl.pdf [https://perma.cc/YV6E-TVBM].

[69] Erie County Nondisclosure Agreement, *supra* note 60.

[70] *See* Letter Agreement Between Fed. Bureau of Investigation, Balt. Police Dep't, and Office of the State's Att'y for Balt. City (July 13, 2011), https://www.documentcloud.org/documents/1808819-baltimore-police-stingray-non-disclosure-agreement.html [https://perma.cc/AG6U-6J7Y].

[71] *See* Sean Robinson, *Group Sues Tacoma Police over Stingray Agreement*, NEWS TRIB. (Oct. 2, 2015), http://www.thenewstribune.com/news/local/politics-government/article37341000.html [https://perma.cc/RGP4-3VTT] ("[The] boilerplate agreement [has been] disclosed by twelve law enforcement agencies in eight states.").

[72] Erie County Nondisclosure Agreement, *supra* note 60, at 2.

[73] *See id.*

[74] *Id.*

[75] *Id.* at 3.

[76] *Id.*

Office is also required to notify the FBI if any FOIA requests, or the like, are made concerning the technology so that the FBI can attempt to prevent disclosure.[77]

Despite the plain language of the agreements, the FBI has stated that its non-disclosure agreements with local law enforcement agencies are "not intended to shield the technology's use."[78] Despite this claim, it is clear multiple efforts have been made to do just that. The standard tactic of stonewalling was made when local police in Florida neither denied nor confirmed the existence of relevant documents in response to a public records request about its use of cell phone location tracking instruments, despite the fact the city had already publicly acknowledged having a Stingray.[79] Additionally, numerous cases have been dropped when the prosecution is questioned on how law enforcement used the Stingray to obtain evidence in that case rather than turn over such information.[80]

---

[77] *See id.* at 4.

[78] *FBI Now Says Stingray Surveillance Can Be Disclosed*, *supra* note 59 ("The [non-disclosure agreement] should not be construed to prevent a law enforcement officer from disclosing to the court or a prosecutor the fact that this technology was used in a particular case.").

[79] *See* Nathan Freed Wessler, *Local Police in Florida Acting Like They're the CIA (But They're Not)*, AM. CIV. LIBERTIES UNION (Mar. 25, 2014, 10:00 AM), https://www.aclu.org/blog/local-police-florida-acting-theyre-cia-theyre-not [https://perma.cc/CT4P-RFSZ].

[80] *See, e.g.*, Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALT. SUN (Apr. 9, 2015), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html [https://perma.cc/U389-2S9V] (reporting that prosecutors in Baltimore withdrew evidence obtained through the use of a Stingray before a judge could hold a detective in contempt of court for not answering questions); Greenemeier, *supra* note 6 (finding that the Baltimore Police Department signed a nondisclosure agreement with the FBI that instructed prosecutors to drop cases rather than reveal the department's use of the stingray); 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 [https://perma.cc/3ZRL-RTEC] (reporting that after a state judge ordered the police to show the Stingray device to the defense attorneys, the state offered one of the defendants six months probation when a usual sentence for the charge receives at least four years in jail); *St. Louis Prosecutors Drop Charges Before Spy Tool Used in Arrests Is Revealed in Court*, RT (Apr. 20, 2015, 6:37 PM), https://www.rt.com/usa/251345-missouri-stingray-charges-dropped/ [https://perma.cc/8X4N-PJFL] ("Prosecutors in St. Louis, Missouri have dropped more than a dozen charges against three defendants accused of

Perhaps the most startling attempt to withhold information occurred in Florida. After a public records request pertaining to cell phone surveillance was made, the local police department responded they had such records.[81] These records showed how a local detective had obtained authorization for Stingray use under the state "trap and trace" statute.[82] However, before the documents could be inspected, the U.S. Marshals Service deputized the local detective, claimed the records therefore became the property of the federal government, and instructed the local police not to release the records.[83]

Such tactics indicate states, either of their own accord or under the direction of the FBI and Harris, are still trying to hide their use of Stingrays. Washington,[84] Utah,[85] Virginia,[86] California,[87] and

---

participating in a string of robberies in late 2013 on the eve of a court hearing on the police department's use of a controversial spy tool.").

[81] *See* Nathan Freed Wessler, *U.S. Marshals Seize Local Cops' Cell Phone Tracking Files in Extraordinary Attempt to Keep Information From Public*, AM. CIV. LIBERTIES UNION (June 3, 2014, 12:15 PM), https://www.aclu.org/blog/us-marshals-seize-local-cops-cell-phone-tracking-files-extraordinary-attempt-keep-information [https://perma.cc/9E5V-XVAZ].

[82] *See id.*

[83] *See id.*

[84] H.B. 1440, 64th Leg., 1st Spec. Sess. (Wash. 2015) ("The state and its political subdivisions shall not, by means of a cell-site simulator device, collect or use a person's electronic data or metadata without (1) that person's informed consent, (2) a warrant, based upon probable cause, that describes with particularity the person, place, or thing to be searched or seized, or (3) acting in accordance with a legally recognized exception to the warrant requirements.").

[85] UTAH CODE ANN. § 77-23c-102(1)(a) (West 2014) ("[A] government entity may not obtain the location information, stored data, or transmitted data of an electronic device without a search warrant issued by a court upon probable cause.").

[86] VA. CODE ANN. § 19.2-70.3(K) (2015) ("An investigative or law-enforcement officer shall not use any device to obtain electronic communications or collect real-time location data from an electronic device without first obtaining a search warrant authorizing the use of the device if, in order to obtain the contents of such electronic communications or such real-time location data from the provider of electronic communication service or remote computing service, such officer would be required to obtain a search warrant pursuant to this section.").

[87] The California law, approved in October 2015, "require[s] police agencies to get city council approval before employing" the use of a cell-site simulator. *See* Williams, *supra* note 11; *see also* S.B. 741, 2015–2016 Leg., Reg. Sess. (Cal. 2015), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160SB741 [https://perma.cc/XT5J-B92D].

Minnesota[88] all have statutes with guidelines on Stingray use and require warrants prior to their use. However, these states are the minority. At least sixty-one agencies in twenty-three states and the District of Columbia use Stingrays, and most of these states have no such guidelines.[89] State law enforcement typically obtains Stingrays with federal money on the basis of anti-terror grants, but then actually use the Stingrays for purposes other than combating terrorism.[90]

For example, the Michigan Police Department paid more than $200,000 for cellular tracking equipment, including a Stingray, with a DHS grant.[91] The department justified the purchase on the basis of "allow[ing] the state to track the physical location of a suspected terrorist who is using wireless communications as part of their operation."[92] This justification proved to be completely false, as evidence shows that the department never used it to track a terrorist.[93] Instead, out of 128 investigations where the department used Stingrays in 2014, most were for homicides, burglaries and robberies, assaults, and missing persons, as well as for minor offenses such as drug crimes, obstructing police, and fraud.[94] The Baltimore Police Department is another example of a local agency without any guidelines that used a Stingray to track a range of criminals from killers to petty thieves.[95]

Without legislative guidelines, Maryland, Michigan, and other states typically employ the use of Stingrays without any judicial

---

[88] MINN. STAT. § 626A.42(2) (2014) ("[A] government entity may not obtain the location information of an electronic device without a tracking warrant. A warrant granting access to location information must be issued only if the government entity shows that there is probable cause the person who possesses an electronic device is committing, has committed, or is about to commit a crime.").

[89] *See Who's Got Them*, *supra* note 3; *supra* note 16 and accompanying text.

[90] *See* Kelly, *supra* note 17.

[91] *See* Nathan Freed Wessler, *Police Citing "Terrorism" to Buy Stingrays Used Only for Ordinary Crimes*, AM. CIV. LIBERTIES UNION (Oct. 23, 2015, 9:00 AM), https://www.aclu.org/blog/free-future/police-citing-terrorism-buy-stingrays-used-only-ordinary-crimes [https://perma.cc/665Z-TJSY].

[92] *See id.*

[93] *See id.*

[94] *Id.*

[95] *See Surveillance Log*, BALTIMORE POLICE DEPARTMENT'S ADVANCED TECHNICAL TEAM, https://assets.documentcloud.org/documents/2287407/cell-site-data-request-060815-bds-2.pdf [https://perma.cc/ZW2Q-GUU2] (last visited Feb. 24, 2016).

application.[96] Some local agencies even use the devices through deceptive means.[97] For example, some will draft surveillance requests to use Stingrays and make them appear as pen register applications instead.[98] A template for a pen register request used by the San Bernardino Sheriff's Department to deploy a Stingray was obtained through a FOIA request.[99] Nowhere in the application do the words Stingray, IMSI catcher, or anything of the like appear.[100] One ACLU attorney believes this application template is very unusual and "likely to mislead judges who receive applications based on it because it gives no indication that the Sheriff's Department intends to use a Stingray."[101] Notably, pen registers are far different than Stingrays.

D. How Stingrays are Different from Pen Registers and Why This Matters

A pen register records the numbers dialed in incoming and outgoing calls to and from a targeted number,[102] while a Stingray col-

---

[96] *See* Zetter, *supra* note 47.

[97] *See* Clarence Walker, *New Hi-Tech Police Surveillance: The "Stingray" Cell Phone Spying Device*, GLOBAL RES. (May 19, 2015), http://www.globalresearch.ca/new-hi-tech-police-surveillance-the-stingray-cell-phone-spying-device/5331165 [https://perma.cc/NLG8-WY9P].

[98] *See id.*

[99] *See* Tim Cushing, '*Insert Probable Cause': Pen Register Boilerplate Hides Sheriff's Department's Hundreds Of Stingray Deployments*, TECHDIRT (June 3, 2015, 4:15 AM), https://www.techdirt.com/articles/20150525/17150031098/insert-probable-cause-pen-register-boilerplate-hides-sheriffs-departments-hundreds-stingray-deployments.shtml [https://perma.cc/4TRP-2E5B]. The agency has used a Stingray at least 303 times. *Id.*

[100] *See id.*

[101] Cyrus Farivar, *County Sheriff Has Used Stingray over 300 Times with No Warrant*, ARS TECHNICA (May 24, 2015, 1:00 PM), http://arstechnica.com/tech-policy/2015/05/county-sheriff-has-used-stingray-over-300-times-with-no-warrant/ [https://perma.cc/ZQK8-G36A].

[102] *See* Matt Blaze, *How Law Enforcement Tracks Cellular Phones*, EXHAUSTIVE SEARCH BLOG (Dec. 13, 2013), http://www.crypto.com/blog/celltapping/ [https://perma.cc/8MH3-56DJ]. The statutory definition of a pen register is:

> [T]he term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication

lects information from every cell phone in its vicinity, leaving the disposal of the information collected from the non-targeted phones to the discretion of the user.[103] In other words, a pen register simply allows for the electronic delivery of call information from a telephone company to law enforcement for only the numbers specified in law enforcement's requests,[104] while a Stingray can track the precise location of every cell phone near it and provide the identifying information of each of those phones.[105] This means that Stingrays "subject [a] potentially unlimited number[] of innocent people to dragnet surveillance" with absolutely no indication that such a search occurred or that the search may have intruded into their private residence or other "constitutionally protected spaces."[106]

The Supreme Court has held use of a pen register is not a "search" under the Fourth Amendment.[107] Furthermore, individuals have no expectation of privacy in the telephone number they dial.[108] Accordingly, "[t]he judicial role in approving [the] use of trap and trace devices is ministerial in nature."[109] A federal court merely needs to find that "the attorney for the government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[110] As explained previously though, Stingrays are being used to do much more than merely record the numbers dialed and received on cell phones; they are used to track people.[111] This leads

---

> service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

18 U.S.C. § 3127(3) (2012).

103 Cushing, *supra* note 99.

104 *See* Blaze, *supra* note 102.

105 *See Stingrays*, *supra* note 14.

106 Justin Fenton, *ACLU Joins Md. Federal Case over Cellphone Tracking*, BALT. SUN (Nov. 26, 2014, 6:55 PM), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-aclu-stingray-brief-20141125-story.html [https://perma.cc/LX6E-XV6L].

107 *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

108 *Id.* at 743.

109 United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).

110 18 U.S.C. § 3123(a)(1) (2012).

111 *See* text accompanying *supra* notes 3–8.

to the question of whether or not use of a Stingray constitutes a search under the Fourth Amendment and should therefore be subject to the more stringent requirements of a warrant prior to its use.

II. THE DEVELOPMENT OF THE FOURTH AMENDMENT

This Part discusses the origin and development of the Fourth Amendment. Section II.A provides a brief history of the Fourth Amendment. Section II.B discusses the Fourth Amendment's implications on the use of historical location data before being compared to real-time tracking in Section II.C. Then Section II.D. discusses the mosaic theory and its potential impact on the Fourth Amendment. Lastly, Section II.E looks into the advance of technology and the Supreme Court's response.

A. The History Behind the Fourth Amendment

The Framer's disdain for the "general warrants" and "writs of assistance" from the colonial era, which allowed British officers to go through all the contents of a person's home looking for evidence, resulted in the drafting of the Fourth Amendment.[112] Their contempt for these searches was a "driving force[] behind the Revolution itself."[113] The Framers consequently did not want to confer any discretionary authority to officers that would allow them to conduct such general searches.[114] This is why the Fourth Amendment was specifically aimed at barring Congress from having the ability to allow the issuance of general warrants; it was not, howev-

---

[112] Riley v. California, 134 S. Ct. 2473, 2494 (2014); *see* Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978) ("The general warrant was a recurring point of contention in the Colonies immediately preceding the Revolution."); United States v. Chadwick, 433 U.S. 1, 7–8 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991) ("It cannot be doubted that the Fourth Amendment's commands grew in large measure out of the colonists' experience with the writs of assistance and their memories of the general warrants formerly in use in England."); *see also Riley*, 134 S. Ct. at 2494 (noting how a young John Adams listened to James Otis's speech against general warrants and later said that it was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.").

[113] *Riley*, 134 S. Ct. at 2494.

[114] *See* Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 201, 212 (1993); *see also* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 578 (1999).

er, aimed at creating the broad reasonableness standard that is in place today.[115]

The Framers assumed that the common-law background protecting warrantless intrusions and explaining when warrants were required would remain in place, thereby making it unnecessary to implement text into the Fourth Amendment regarding such procedures.[116] This is why the Framers were content in stating only the standards necessary for a valid warrant as common law already placed restraints on the discretionary authority of officers conducting searches and seizures.[117] However, this foundation became blurred when legislative codes began undermining the notion of a "permanent common law."[118] This shift in policy, coupled with concerns about crime and social disorder during the nineteenth century, expanded the authority of the warrantless officer.[119]

The foundation of the modern Fourth Amendment is rooted in *Weeks v. United States*.[120] *Weeks* extended the Fourth Amendment to the actions of a warrantless officer acting "under color of his office."[121] This had the effect of constitutionalizing the requirement of a warrant to search a house,[122] and introduced the exclusionary rule to illegally obtained evidence.[123] The next step was the inser-

---

115 Davies, *supra* note 114, at 557–60, 724.

116 *See id.* at 724.

117 *Id.*

118 *Id.* at 725.

119 *See id.* ("New concerns about crime and social disorder during the nineteenth century gave rise to a perception that the common-law structure of law enforcement was inadequate to meet the needs of an increasingly complex and urban society. Contemporaneously with the advent of police departments and career officers, courts and legislatures drastically expanded the ex officio authority of the warrantless officer.").

120 *See id.* at 729.

121 *See* Weeks v. United States, 232 U.S. 383, 393–94, (1914) ("[T]he [Fourth] Amendment was intended to secure the citizen in person and property against unlawful invasion of the sanctity of his home by officers of the law, acting under legislative or judicial sanction. This protection is equally extended to the action of the government and officers of the law acting under it. To sanction such proceedings would be to affirm by judicial decision a manifest neglect, if not an open defiance, of the prohibitions of the Constitution, intended for the protection of the people against such unauthorized action." (internal citations omitted)).

122 *See id.* at 398 (finding that the taking of letters from the defendant's house is "in direct violation of the constitutional rights of the defendant").

123 By characterizing the act of the officer as "in direct violation of the constitutional rights of the defendant," the Court placed a warrantless search in the same category as

tion of a "reasonableness" standard into a warrantless search.[124] *Carroll v. United States* accomplished this when the Court upheld the warrantless search of an automobile on the basis that the Fourth Amendment only prohibits searches that are "unreasonable," and it was "'not unreasonable' for the police to conduct a warrantless search of a car for contraband in the circumstances."[125] This concept of "reasonableness" would become the central principle of the Fourth Amendment in the late nineteenth and early twentieth centuries.[126]

The reasonableness standard used today was articulated in *Katz v. United States*.[127] In this case, the defendant violated a federal statute by using a telephone to transmit wagering information, and at trial, the prosecution used evidence obtained through an electronic listening and recording device attached to the outside of a public telephone booth that the defendant had used.[128] The Court recognized that "the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures."[129] This interpretation makes it clear that whether or not a "search" has occurred under the Fourth Amendment "cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[130] Therefore, the previous requirement of a physical trespass for a "search" to occur was bad law in modern times as "reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[131]

---

the "void" court order in *Boyd v. United States*. *See id.*; Boyd v. United States, 116 U.S. 616 (1886). The Court in *Boyd*, in excluding an invoice produced under unconstitutional statutory authority, relied upon a conclusion in *Marbury v. Madison* that the Court has no authority to recognize a "void" government act. *See Boyd*, 116 U.S. at 638; Marbury v. Madison, 5 U.S. 137, 180 (1803). Under this string of logic, exclusion is a necessary consequence of a government search that violates constitutional authority. *See* Davies, *supra* note 114, at 730.

124 *See* Davies, *supra* note 114, at 731.

125 *Id.*; *see also* Carroll v. United States, 267 U.S. 132, 147 (1925) ("The Fourth Amendment does not denounce all searches or seizures, but only such as are unreasonable.").

126 *See* Davies, *supra* note 114, at 732.

127 389 U.S. 347 (1967).

128 *See id.* at 348.

129 *Id.* at 353.

130 *Id.*

131 *Id.* at 362 (Harlan, J., concurring).

As a result, Justice Harlan came up with a two-prong test to determine whether or not a Fourth Amendment search or seizure occurred. First, a court determines whether a person has "exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[132] Using this test, it was determined that someone who goes into a telephone booth, shuts the door, and pays to make a phone call "is surely entitled to assume that his conversation is not being intercepted."[133] The booth "is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable."[134] Justice Harlan's concurrence from *Katz* has become known as the "*Katz* test" and is the touchstone analysis of any Fourth Amendment question.[135] This analysis was recently applied to the use of cell phones in *United States v. Davis*.[136]

B. The Acquisition and Use of Historical Cell Tower Records

The Eleventh Circuit decision in *Davis* involved a review of whether or not a statutorily-prescribed judicial order to a third party cellular telephone service provider to turn over "historical cell tower location information" to the federal government on one of its users constituted a search under the Fourth Amendment.[137] This data was beneficial because MetroPCS, Davis' cell phone provider, used it to identify the locations of their cell towers, allowing the police to compare the locations of the robberies to those of

---

[132] *Id.* at 361. Even though this is a concurring opinion, the Supreme Court has subsequently applied Justice Harlan's principle to hold that a Fourth Amendment search occurs when "'the individual manifest[s] a subjective expectation of privacy in the object of the challenged search' and 'society is willing to recognize that expectation as reasonable.'" Kyllo v. United States, 533 U.S. 27, 33 (2001).

[133] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[134] *Id.*

[135] *See* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (stating the *Katz* test has come to mean the test enunciated by Justice Harlan's concurrence); Smith v. Maryland, 442 U.S. 735, 740 (1979) (expressly adopting Justice Harlan's "reasonable expectation of privacy" formula as the rule of *Katz*).

[136] 785 F.3d 498 (11th Cir. 2015).

[137] *Id.* at 503. "Historical cell tower location information" is historical telephone records for a number requested, which shows, among other things, "the number assigned to the cell tower that wirelessly connected the calls from and to Davis" and "the sector number associated with that tower." *Id.* at 502–03.

the cell towers connecting Davis' calls around the time of the robberies.[138] This showed the cell tower sites were near the robbery locations.[139] Therefore, the prosecution was able to argue that Davis must have also been near the robberies.[140]

The main doctrine relied upon in *Davis* for admitting the historical location data was the third party doctrine.[141] This doctrine holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[142] Using this line of reasoning, the *Davis* court held that since cell phone users know their phone must connect to a cell tower, that the signal is only transmitted when they make or receive a call, and that this signal is also sent to their service provider, the cell user is aware that he is "conveying cell tower location information to the service provider and voluntarily does so."[143] Consequently, there is no expectation of privacy in telephone records that show past cell tower locations.[144] This line of reasoning is different when courts look at real-time location tracking.

C. Real-Time Tracking Through the Use of Physical Tracking Devices

The Supreme Court first confronted the use of a tracking device in *United States v. Knotts*, where law enforcement agents placed a beeper,[145] without a warrant, in a drum of chloroform purchased by one of the defendants.[146] The agents subsequently monitored the progress of a car carrying the chloroform and traced the drum from its place of purchase in Minnesota to the defendant's cabin in Wisconsin.[147] It is important to note that the "surveillance amounted principally to the following of a car on public streets and

---

138 *See id.* at 501.
139 *See id.*
140 *Id.* at 502.
141 *See generally id.*
142 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
143 *Davis*, 785 F.3d at 510.
144 *See id.*
145 A beeper is "[a] radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver." United States v. Knotts, 460 U.S. 276, 277 (1983).
146 *See id.* The beeper was placed in the drum with the consent of Hawkins Chemical Company who subsequently sold it to the defendants. *See id.* at 278.
147 *See id.* at 277.

highways" because a person travelling in an automobile on public roads has no reasonable expectation of privacy in his movements from one place to another.[148] While travelling on public streets, a person "voluntarily convey[s] to anyone who want[s] to look . . . that he is travelling over particular roads in a particular direction," the locations of any stops he makes, and "his final destination when he exit[s] from public roads onto private property."[149] While the owner of the cabin had an expectation of privacy within the cabin, that notion did not carry over into law enforcement's observation of the car arriving to the cabin, nor did it extend to the transportation of the drum in the "open fields" outside the cabin.[150] Law enforcement's use of the beeper to supplement their visual surveillance makes no difference as "[n]othing 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."[151] Furthermore, even though the police would not have been able to locate the final resting place of the chloroform without the beeper in this case,[152] had an agent wanted to, he could have followed the defendant in a car without the use of a beeper and determined the final resting place of the chloroform.[153] Therefore, the Court reasoned, the scientific enhancement used here raised "no constitutional issues which visual surveillance would not also raise," so no Fourth Amendment violation occurred.[154]

United States v. Karo addresses two issues left unresolved by *Knotts*: (1) whether tracking a container through the placement of a beeper in a container with the consent of the original owner, but not with the buyer's consent, is a search under the Fourth Amendment; and (2) whether acquiring information that could not have been obtained through normal, visual surveillance makes the

---

148 *Id.* at 281.

149 *Id.* at 281–82.

150 *Id.* at 282.

151 *Id*. *But see infra* Section II.E (noting how sense-enhancing technology can be prohibited by the Fourth Amendment).

152 *See Knotts*, 460 U.S. at 278. When the defendant "began making evasive maneuvers . . . the pursuing agents ended their visual surveillance." *Id*.

153 *See id.* at 282.

154 *See id.* at 285.

monitoring of the beeper a Fourth Amendment violation.[155] The facts in *Karo* are very similar to those in *Knotts*.[156]

In answering the first question, the Court held that "[t]he mere transfer to [the defendant] of a can containing an unmonitored beeper infringed no privacy interest" because "it conveyed no information at all. . . . [I]t created a potential for an invasion of privacy," but a potential, as opposed to an actual, invasion of privacy does not constitute a search under the Fourth Amendment.[157] It is only when these "technological advances" are actually exploited that Fourth Amendment privacy interests come into play.[158]

This brings us to the second question. Employing the same analysis used in *Knotts*,[159] the Court first recognized the basic Fourth Amendment principle that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."[160] Therefore, had the agents gone into one of the residences to check if the ether was there without a warrant because they had no beeper to monitor, it surely would have been an illegal search under the Fourth Amendment.[161] Consequently, when law enforcement employs an electronic device to obtain information from inside a house that it could not have obtained by observation from outside the area surrounding the house, it too must be an illegal search.[162] This occurred in *Karo* because even though visual surveillance

---

155 United States v. Karo, 468 U.S. 705, 707 (1984).

156 After a Drug Enforcement Administration ("DEA") agent learned that the defendants had ordered fifty gallons of ether to extract cocaine from clothing they had imported, the government obtained a court order to install and monitor a beeper in one of the cans of ether, with the informant's consent. *Id.* at 708. Thereafter, agents saw one of the defendants pick up the ether from the informant, followed him to his house, and determined by using the beeper that the ether was inside the house where it was then monitored. *Id.* at 708–09. After being moved to various locations, the agents determined that the can with the beeper in it was inside a house rented by the defendants and obtained a warrant to search the house based in part on information derived through use of the beeper. *Id.* at 709–10.

157 *Id.* at 712.

158 *Id.*

159 *See supra* notes 152–54 and accompanying text.

160 *Karo*, 468 U.S. at 714.

161 *See id.* at 715.

162 *See id.*

alone may have been enough to witness the ether entering the residence, the beeper confirmed what law enforcement saw and the continual monitoring of the beeper provided verification that the beeper had not left the residence.[163] Thus, the case is not like *Knotts*, where the beeper only provided information that could have also been obtained through visual surveillance.[164] In *Karo*, the monitoring indicated a fact that could not have been obtained through visual surveillance—that the beeper was inside the house.[165]

Based upon this reasoning, the Court held that the Government cannot:

> [B]e completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.[166]

It does not matter that a warrant requirement in this situation would require the government to get warrants in a large number of cases[167] nor does it matter that it will be difficult to meet the Fourth Amendment's particularity requirement in such instances.[168] The search of a house must be conducted with a warrant.[169]

---

163 *Id.*

164 *See supra* notes 146–49 and accompanying text.

165 *See Karo*, 468 U.S. at 715.

166 *Id.* at 716.

167 *See id.* at 718. The prosecution argued that "[i]f agents are required to obtain warrants prior to monitoring a beeper when it has been withdrawn from public view . . . 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." *Id.* The Court found this argument to be hardly compelling. *See id.*

168 *See id.* The prosecution also argued that "it would be impossible to describe the 'place' to be searched, because the location of the place is precisely what is sought to be

The final and most recent case on the use of a tracking device is *United States v. Jones*.[170] Again, the facts are very similar to *Knotts* and *Karo*.[171] The Court found that "the attachment of a [GPS] tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search within the meaning of the Fourth Amendment."[172] The different outcome is a result of the analysis employed by the majority of the Court. Justice Scalia, writing for the majority, focused on the trespass involved with the placing of the beeper and declared that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."[173] Therefore, because "the government physical-

---

discovered through the search. However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance." *Id.* (internal citations omitted); *see also infra* Section III.D (discussing the issues presented by the particularity requirement).

169 *See id.*

170 132 S. Ct. 945 (2012).

171

> Jones . . . was made the target of an investigation . . . . Officers employed various investigative techniques, including visual surveillance of the nightclub, installation of a camera focused on the front door of the club, and a pen register and wiretap covering Jones's cellular phone.
>
> Based in part on information gathered from these sources, in 2005 the Government applied . . . for a warrant authorizing the use of an electronic tracking device on the [vehicle] registered to Jones's wife. A warrant issued, authorizing installation of the device in the District of Columbia and within [ten] days.
>
> On the [eleventh] day, and not in the District of Columbia but in Maryland, agents installed a GPS tracking device on the undercarriage of the Jeep while it was parked in a public parking lot. Over the next [twenty-eight] days, the Government used the device to track the vehicle's movements, and once had to replace the device's battery when the vehicle was parked in a different public lot in Maryland. By means of signals from multiple satellites, the device established the vehicle's location within [fifty] to [one hundred] feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the [four]–week period.

Id. at 948.

172 *Id*. at 948, 954.

173 *Id.* at 952.

ly occupied private property for the purpose of obtaining information," the Court had no doubt that such an intrusion was a "search" within the original meaning of the Fourth Amendment.[174] The *Katz* test remains applicable to "[s]ituations involving merely the transmission of electronic signals without trespass."[175]

Knotts is distinguishable from *Jones* because *Knotts* only conducted a *Katz* analysis, there was no challenge to the physical installation of the beeper, and the Court declined to consider the installation's effect on its Fourth Amendment analysis.[176] However, the conclusion in *Karo*—that installation with the consent of the original owner, then delivered to a buyer having no knowledge of the beeper, does not constitute a search—was determined to be consistent with the Court's holding in *Jones*.[177]

It is important to note that Justice Scalia and the three justices who joined the majority opinion did not find it necessary to determine whether or not using strictly electronic surveillance over a four-week period, which may have been possible through traditional, visual observation, without an accompanying trespass is an unconstitutional search.[178] While Justice Sotomayor agreed that the trespassory analysis should be employed first and that its analysis alone was sufficient to decide this case,[179] she also recognized and agreed with Justice Alito's concurrence, joined by three other justices, finding that "physical intrusion is now unnecessary to many

---

174 *Id.* at 949.

175 *Id.* at 953.

176 *See id.* at 952. The Court found that *Knotts* might have been applicable "if the government were making the argument that what would otherwise be an unconstitutional search is not such where it produces only public information. The government does not make that argument, and we know of no case that would support it." *Id.*

177 *See id.* ("Karo accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to monitor the container's location.").

178 *See id.* at 953–54.

179 *See id.* at 954–55 (Sotomayor, J., concurring) ("The government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection . . . . [T]he trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: when the government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case.").

forms of surveillance" and "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"[180]

Justice Alito's approach made a *Katz* analysis similar to those done in *Knotts*[181] and *Karo*.[182] Justice Alito reasoned that in most cases, long term GPS monitoring infringes upon reasonable expectations of privacy, as society has long held the belief that law enforcement would not have the resources to discreetly monitor a person's every movement.[183] The exact point at which the monitoring became a search in this case is not necessary to determine as that "line was surely crossed before the four-week mark," although "[o]ther cases may present more difficult questions."[184] In those situations where it is not clear whether or not GPS surveillance will amount to a Fourth Amendment search, the police can always play it safe by getting a warrant first.[185]

This shows that a majority of the Supreme Court (through the majority and concurrence opinions) deemed the duration of the GPS monitoring as a critical factor in their analysis due to the fact that no reasonable person would expect law enforcement to use the resources necessary to conduct such a long surveillance through traditional means.[186] GPS surveillance intrudes on expectations of privacy because the information in its totality reveals intimate details of a person's life.[187] This line of reasoning is an articulation of the mosaic theory.

---

[180] *Id.* at 955 (quoting *id.* at 964 (Alito, J., concurring)).

[181] *See supra* notes 152–54 and accompanying text.

[182] *See supra* notes 160–65 and accompanying text.

[183] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

[184] *See id.*

[185] *See id.*

[186] *See id.* at 956. (Sotomayor, J., concurring) ("And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"); *supra* notes 183–85 and accompanying text.

[187] *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

D. The Mosaic Theory

The mosaic theory[188] holds that "the aggregation of vast amounts of metadata should be considered a 'search' within the meaning of the Fourth Amendment because it can reveal a great deal about a person's life, even if each piece of data may reveal little when viewed in isolation."[189] It provides an opportunity for the courts to protect against the privacy intrusions presented by the ever-evolving technological landscape in the era of big data.[190] Under this theory, a court would determine Fourth Amendment interests on a case-by-case basis, "assessing the quality and quantity of information about a suspect gathered in the course of a specific investigation."[191]

Justice Sotomayor in *Jones*, while not explicitly using the term "mosaic theory," suggested that the Court may need to adopt such an approach in the near future.[192] She forewarned that the Court would eventually need to recognize the growing concern of how easily technology enables law enforcement to acquire personal in-

---

[188] While the Supreme Court justices never explicitly used the term "mosaic theory" in *Jones*, the Court of Appeals used this term. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) ("As with the 'mosaic theory' often invoked by the government in cases involving national security information, 'What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene.' Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." (internal citations omitted)).

[189] Jonathan Hafetz, *Bulk Data Collection and the Mosaic Theory: A More Balanced Approach to Information*, JUST SECURITY (Jan. 17, 2014, 9:00 AM), https://www.justsecurity.org/5758/guest-post-bulk-data-collection-mosaic-theory/ [https://perma.cc/RAG2-JYWC].

[190] *Id.*

[191] David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 101 (2013).

[192] *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

formation and how such unrestrained power is susceptible to abuse by the government.[193] She specifically mentioned that physical intrusion is no longer necessary to conduct GPS tracking because GPS-enabled smartphones permit law enforcement to conduct non-trespassory surveillance.[194] Law enforcement's ability to ascertain information about a person, including his political affiliation, religion, and sexual habits, through the sum of his public movements should be taken into account in determining a person's expectation of privacy.[195]

Justice Alito used a similar line of reasoning in *Jones*, stating that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue *every single movement* of an individual's car for a very long period."[196] He was specifically concerned about the ease in which the tracking occurred and how it was continuous and precise.[197] Essentially, Justice Alito suggested the adoption of the mosaic theory through his concern with how much information the continuous tracking revealed—indicating five Justices on the Supreme Court may be ready to adopt the mosaic theory.[198]

Two years later, in *Riley v. California*, the Court held that police generally cannot search an arrestee's cell phone at the time of an arrest without obtaining a warrant.[199] Explaining why the arrestee's wallet could be searched but his cell phone could not be, the Court offered an argument resembling the mosaic theory:

> [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

---

193 *See id.* at 956.

194 *See id.* at 955.

195 *See id*. at 955–56.

196 *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (emphasis added).

197 *See id.* at 963–64.

198 Justice Sotomayor in her concurrence in *Jones*, along with Justice Alito's concurrence in the same case, joined by Justice Ginsburg, Justice Breyer, and Justice Kagan, indicate a willingness by the Court to adopt the mosaic theory. *See* text accompanying *supra* notes 192, 196–97.

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

> record. . . . 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. [Finally], 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.[200]

The Court also echoed Justice Sotomayor's concern about cell phone location data in that it can be used to reconstruct someone's movements down to the minute and within a specific building, reflecting intimate details of that person's life.[201] *Riley* provides us with hints that nearly all of the Justices may be open to mosaic theory reasoning in regards to the Fourth Amendment.[202] This can be seen as an important recognition by the Court as a way to protect the public from advances in technology. Another is laid out in *Kyllo v. United States*.[203]

E. The Advance of Technology and the Court's Response

Advances in technology, such as the Stingray, have made intrusions into the home easier and affected the degree of privacy secured to citizens by the Fourth Amendment.[204] Prior to the advent of smartphones, iPads, and every other technological innovation that has shaped the world we live in today, the greatest safeguards to our privacy were not found in the Constitution but were practic-

---

[200] *Id.* at 2489. *But see id.* at 2489 n.1 ("Because the United States and California agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.").

[201] *See id.* at 2490 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

[202] Every Justice but Justice Alito, who filed a concurring opinion, joined Chief Justice Robert's opinion. *See id.* at 2480 (majority opinion).

[203] 533 U.S. 27 (2001).

[204] *See id.* at 33–34.

al.[205] Maintaining surveillance through conventional means over a long period of time was costly and laborious and therefore rarely done.[206] Technological advances have made what used to take "a large team of agents, multiple vehicles, and perhaps aerial assistance . . . relatively easy and cheap."[207] Society's reasonable expectations of privacy will be continually transformed and shaped according to the accessibility and use of these advances.[208] A new surveillance technique, such as Stingrays, must be "judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[209]

Kyllo v. United States put these expectations to the test. In this case, agents used a thermal-imaging device to scan the defendant's home to ascertain whether or not the heat measurements coming from the home were consistent with levels given from the sort of lamps typically used for indoor marijuana growth.[210] Based in part on the results of the scan showing that parts of the home were warmer than others, a Federal Magistrate Judge issued a warrant to search the defendant's home where agents found marijuana growing.[211] The Court ultimately held that:

> [O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.[212]

In order to get to this conclusion, the Court first rejected recognizing a difference between "off-the-wall" observations and

---

[205] *Jones*, 132 S. Ct. at 963 (Alito, J., concurring); *see also* Boyd v. United States, 116 U.S. 616, 628 (1886) ("[T]he eye cannot by the laws of England be guilty of a trespass.").

[206] *See id.*

[207] *Jones*, 132 S. Ct. at 963–64.

[208] *Id.* at 963.

[209] Delaware v. Prouse, 440 U.S. 648, 654 (1979).

[210] Kyllo v. United States, 533 U.S. 27, 29 (2001).

[211] *See id.* at 30.

[212] *Id.* at 34 (internal citations omitted).

"through-the-wall surveillance."[213] The fact that thermal imaging only detects heat radiating from the exterior of the house is immaterial because recognizing such a difference would "leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home."[214] The "proposition that inference insulates a search" must be rejected as well because it is contrary to *Karo*, "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home."[215]

The next argument made by the government was that the thermal imaging was constitutional because it did not detect private activities occurring in private areas.[216] Supreme Court cases show that all details are intimate details when inside the home though,[217] so the detail of how warm—or even how relatively warm—Kyllo was heating his residence is also an intimate detail because it is in his home.[218] Therefore, because all details are intimate details when inside the home and the Government used a device, not in general public use, to procure information inside the home that could not have been knowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.[219]

The dissent points out two fair criticisms. First, the majority does not discuss how much use constitutes general public use.[220] The dissent was the first of many to criticize this portion of the opinion.[221] Unfortunately, this portion of the standard has not be-

---

213 *See id.* at 35.

214 *Id.* at 35–36.

215 *Id.* at 36.

216 *See id*. at 38.

217 For example, a can of ether and the registration number of a phonograph turntable have been found to be intimate details when inside a home. *See generally* Arizona v. Hicks, 480 U.S. 321 (1987); United States v. Karo, 468 U.S. 705 (1984).

218 *Kyllo*, 533 U.S. at 38.

219 *Id.* at 40.

220 *See id.* at 47 (Stevens, J., dissenting).

221 *See, e.g.*, Mary Kim, *Investigation and Police Practices*, 90 GEO. L.J. 1099 (2002); Daniel McKenzie, *What Were They Smoking?: The Supreme Court's Latest Step In A Long, Strange Trip Through The Fourth Amendment*, 93 J. CRIM. L. & CRIMINOLOGY 153 (2002); Reginald Short, Comment, *The Kyllo Conundrum: A New Standard to Address Technology*

come any clearer. Since the standards were first articulated, no thermal imaging device has been declared "in general public use" and therefore free to be used without a warrant.[222] Federal courts have avoided even attempting to interpret this portion of the standard and instead have simply decided cases without commenting specifically on the "general public use" portion of the standard.[223]

The second main criticism by the dissent was that "the category of 'sense-enhancing technology' covered by the new rule is far too broad."[224] Justice Stevens argued that this rule would prohibit mechanical substitutes for dog sniffs despite the fact that the Court had already held that "a dog sniff that 'discloses only the presence or absence of narcotics' does 'not constitute a "search" within the meaning of the Fourth Amendment.'"[225] This fear proved to be unfounded when, in *Illinois v. Caballes*, the Court reasoned that it was critical to the *Kyllo* decision that the device was capable of detecting lawful activity, whereas a dog sniff can only detect unlawful activity.[226] There is an accepted, reasonable expectation that private, lawful activity will remain private, but that assumption is inapposite to the expectation that contraband in the trunk of your car will also remain private.[227] Therefore, the Court concluded that "[a] dog sniff conducted during a lawful traffic stop that reveals no information other than the location of a substance that no individual has any right to possess does not violate the Fourth Amendment."[228]

That Represents A Step Backward For Fourth Amendment Protections, 80 DENV. U. L. REV. 463, 482–83 (2002).

[222] Derek T. Conom, *Sense-Enhancing Technology and the Search in the Wake of Kyllo v. United States: Will Prevalence Kill Privacy?*, 41 WILLAMETTE L. REV. 749, 765 (2005).

[223] *See* Conom, *supra* note 222, at 765; *see also* Baldi v. Amadon, No. CIV. 02-313-M, 2004 WL 725618, at *4 (D.N.H. Apr. 5, 2004) (distinguishing *Kyllo* and the general public use standard by instead holding that since the scan with the night vision was done outside Baldi's curtilage and in the open fields of the area, MacKenzie did not see anything "regarding the interior of the home that could not have been otherwise obtained without physical intrusion").

[224] *Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting).

[225] *Id.* (citing United States v. Place, 462 U.S. 696, 707 (1983)).

[226] Illinois v. Caballes, 543 U.S. 405, 409–10 (2005).

[227] *Id.* at 410.

[228] *Id.*

III. THE FOURTH AMENDMENT'S IMPLICATIONS ON THE USE OF A STINGRAY BY LAW ENFORCEMENT

This Part discusses the Fourth Amendment implications of the use of a Stingray, and concludes that the Fourth Amendment requires, at minimum, law enforcement to obtain a warrant prior to using a Stingray. Section III.A discusses modern Fourth Amendment cases dealing with different surveillance techniques and the protection of the home versus public places. Section III.B explains how the use of a Stingray is a Fourth Amendment search under a traditional *Katz* analysis. Then, Section III.C distinguishes how the real-time tracking of cell phone location data is different from historical cell phone location data. Lastly, Section III.D discusses the possibility that use of Stingrays should be banned altogether because approval to use one may equate to a general warrant.

A. Warrantless Searches and the Courts' Responses

While it is clear that the Framers of the Constitution could not have predicted modern law enforcement needs,[229] the discretionary authority of officers today is far greater than what the Framers could have ever imagined or wanted.[230] This Section first discusses how courts have reacted to the different surveillance methods and techniques used by modern law enforcement and the applicability of these decisions to a Stingray; particularly sense-enhancing technology and real-time tracking of automobiles. It then closes with the modern view of the Supreme Court on the "mosaic theory" and its applicability to Stingray use.

1. The Court's Protection of the Home from Sense-Enhancing Technology

People have always been able to be "free from unreasonable governmental intrusion" under the protection of their own home.[231] One's home is a place where an "individual normally ex-

---

[229] *See* Nathan H. Seltzer, *When History Matters Not: The Fourth Amendment in the Age of the Secret Search*, 40 NO. 2 CRIM. LAW BULL. ART 1 (Summer 2004).

[230] Davies, *supra* note 114, at 557.

[231] Payton v. New York, 445 U.S. 573, 590 (1980) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)). The Court re-affirmed this statement in *Kyllo v. United States*, 533 U.S. 27, 31 (2001).

pects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."[232] As such, without a warrant, the government cannot use surveillance devices to determine whether or not a particular item, like a cell phone, or a person, is in a private residence.[233] The "[i]ndiscriminate monitoring of property [within one's home] . . . present[s] far too serious a threat to privacy interests . . . to escape entirely some sort of Fourth Amendment oversight."[234]

It does not matter that law enforcement agencies will not know when they are monitoring devices in a private place, thus compelling them to obtain a warrant in almost all cases.[235] Nor does it matter that they may not be able to depict the "place" they are trying to search, because the location is what they are after.[236] This perfectly articulates why the use of a Stingray would intrude on a person's reasonable expectation of privacy in nearly all situations. Law enforcement typically uses Stingrays to find suspects whose locations they do not know, and therefore may track them into private places.[237] As a result, law enforcement must be required to obtain a warrant prior to its use of a Stingray or risk violating the Fourth Amendment. The federal government admitted as much in a failed defense in *Karo*.[238]

This potential for an invasion of privacy has only increased with the advance of technology and when new technologies come before a court they are typically analyzed through a *Kyllo* analysis.[239] Applying such an analysis to Stingrays supports the inference that Stingrays, like thermal imaging devices, should also be found to be

---

[232] United States v. Karo, 468 U.S. 705, 714 (1984).

[233] *Id.* at 716.

[234] *Id.*

[235] *See id*. at 718.

[236] *Id.*

[237] *See* text accompanying *supra* note 30.

[238] The federal government argued in *Karo* that requiring a warrant prior to monitoring a beeper in a private residence would require them to obtain a warrant in almost all situations. *Karo*, 468 U.S. at 718. Since the location is precisely what agents are after, it is impossible for agents to predict whether the beeper will be at some point transmitting its signals from inside private premises. *See id.*; *supra* note 167 and accompanying text.

[239] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

a search under the Fourth Amendment. A main concern of the Court in *Kyllo* was protecting the home from "advancing technology."[240] This is why even a mere inference from the use of technology that produces information on the interior of a home is still considered a search.[241] Therefore, use of a Stingray that goes through walls to produce information on the interior of a home, such information being an inference that the suspect will be in the home next to his cell phone,[242] should surely be found to be a search as well.[243] The fact that the information produced is only an inference is immaterial.[244] Nor does it matter that the information produced is merely the location of a cell phone—if a phonograph table, a can of ether, and how warm a house is are considered intimate details of a home,[245] the location of a cell phone within a home is assuredly an intimate detail as well.

As for the criticisms of *Kyllo* concerning the "general public use" standard and the potential for the category of "sense-enhancing technology" that is covered by the new rule being too broad,[246] they do not present much of a problem in regards to Stingrays. Stingrays cannot be considered in general public use because the public barely knows anything about them and are actively pre-

---

[240] *See id.* at 35–36, 40.

[241] *See id.* at 36.

[242] *See, e.g.*, Matthew Keys, *Sting Operation: Police Tracked Cellphones with 'Stingrays,'* BLOT MAG. (June 5, 2014), http://www.theblot.com/documents-reveal-police-track-cell-phones-stingrays-7720535 [https://perma.cc/YV6H-Z2BF] (reporting that the police used a Stingray to find and force themselves into a suspect's apartment without a warrant); Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED (Apr. 9, 2013, 6:30 AM), http://www.wired.com/2013/04/verizon-rigmaiden-aircard/ [https://perma.cc/5B66-ZLFC] (reporting that the FBI used a Stingray to find the suspect in apartment 1122).

[243] A potential counter is that the agents will have "probable cause to believe that incriminating evidence will be found within" the home, such as a wanted suspect. Payton v. New York, 445 U.S. 573, 588 (1980). The Court shot down this argument because "the constitutional protection afforded to the individual's interest in the privacy of his own home is equally applicable to a warrantless entry for the purpose of arresting a resident of the house; for it is inherent in such an entry that a search for the suspect may be required before he can be apprehended." *Id.*

[244] *See Kyllo*, 533 U.S. at 36.

[245] *See* text accompanying *supra* notes 217–18.

[246] *See Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting); text accompanying *supra* notes 220, 224.

vented from learning more.[247] Additionally, only sixty-one state and federal agencies are known to use Stingrays[248] as compared to the thermal imaging device at issue in *Kyllo*, which had nearly one thousand manufactured units.[249] On top of that, the device in *Kyllo* could be rented by anyone who wanted one from several national companies, was predated by a device which had anywhere from 4,000 to 5,000 units, and had a competitor ranging from 5,000 to 6,000 units.[250] If the device in *Kyllo* was found to not be in general public use, then clearly Stingrays are in even less general public use.

Were Stingrays to get to a point that they could arguably be considered in general public use, then courts may finally be forced to address this language. Federal courts have been reluctant to analyze what constitutes "general public use" so far,[251] while states may avoid the question altogether by formulating their own standards based upon their state constitutions.[252] Relying upon the more protective terms of their own constitutions, states may instead decide on the issue by relying upon a privacy analysis that does not incorporate the objective expectations of society into it,[253] or simply leave out the general public use language in a similar adoption of *Kyllo*. As for the federal courts, the blind affirmation of the public use standard needs to come to an end.[254] Whatever options the lower courts select in providing meaning to the language "will ultimately and inevitably lead to further consideration by the Supreme Court regarding this question,"[255] but until then, district courts need to attempt to provide clarification.

---

247 *See supra* Section I.A.

248 *See Who's Got Them*, *supra* note 3.

249 *See Kyllo*, 533 U.S. at 47 n.5 (Stevens, J., dissenting).

250 *Id.*

251 *See* Conom, *supra* note 222, at 765.

252 *See id*. at 766; *see also* State v. Young, 867 P.2d 593, 601 (Wash. 1994) ("We hold the infrared surveillance not only violated the defendant's private affairs, but also constituted a violation of the Washington State Constitution's protection against the warrantless invasion of his home.").

253 Conom, *supra* note 222, at 773. "In *Young*, the Washington Supreme Court found both the private affairs clause and invasion of the home clause [of their state constitution] violated." *Id.* at 768.

254 *See* Conom, *supra* note 222, at 773.

255 *Id*.

As to the second criticism of *Kyllo*, that the standard was far too broad,[256] its concern is unfounded here relying upon the reasoning laid out in *Illinois v. Caballes*.[257] Simply having a cell phone on your person is lawful activity[258] and very different than a dog sniff or any other future surveillance technique that is only capable of procuring unlawful activity. Therefore, because a Stingray is not in general public use at the moment and it detects legal activity, when the use of one produces information inside a private residence that was not knowable without the use of the device, in that instance it should be considered a search under the Fourth Amendment. Much of this line of analysis is confirmed and supplemented by GPS tracking cases.

2. Tracking People in Public Areas with Stingrays is Also a Search

Looking at the real-time tracking cases[259] together provides another useful indicator on how courts could analyze the use of Stingrays if they were to accept the opportunity. First, it appears a court would apply a *Katz* analysis because Stingrays involve no physical trespass but an electronic one.[260] If the use of a Stingray is found to have procured information from inside a private residence, that ends the analysis because the Fourth Amendment protects one's home.[261] It does not matter that electronic surveillance is less intrusive than traditional means—the Fourth Amendment protects the information a search reveals inside a home and a court cannot abandon the notion of being free from government intrusion just because a search is less intrusive.[262]

---

[256] *See* text accompanying *supra* note 224.

[257] *See* Illinois v. Caballes, 543 U.S. 405, 409–10 (1983); *supra* text accompanying notes 226–28.

[258] "[N]early three-quarters of smart phone users report being within five feet of their phones most of the time . . . ." Riley v. California, 134 S. Ct. 2473, 2490 (2014); *see also* Lee Rainie & Kathryn Zickuhr, *Americans' Views on Mobile Etiquette*, PEW RES. CTR. (Aug. 26, 2015), http://www.pewinternet.org/2015/08/26/americans-views-on-mobile-etiquette/ [https://perma.cc/D6KK-AUQ5].

[259] *See supra* Part II.C.

[260] *See* United States v. Jones, 132 S. Ct. 945, 953 (2012).

[261] *See* United States v. Karo, 468 U.S. 705, 714 (1984).

[262] *See Karo*, 468 U.S. at 715 ("The monitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal a critical fact about

If the search never intruded into a private place, which is very unlikely as the average American spends sixty nine percent of his or her time in a residence,[263] a court will likely then ask whether the surveillance done by the Stingray could have reasonably been done through traditional, visual surveillance as a way to determine the reasonableness of the search.[264] With a Stingray, the user is often trying to find a suspect's location. That means law enforcement does not have a car to place a tracking device on nor the means to conduct traditional surveillance methods, such as tracking the car by simply following it. Therefore, even if a suspect is tracked in and to public places, the tracking was only made possible through the use of the Stingray and should still be considered an illegal search.

Such tracking of people in public places also impinges on expectations of privacy under the mosaic theory. Since Stingrays allow for the continuous, precise tracking of a person, it is, therefore, a very real concern that law enforcement may use a Stingray to obtain an aggregate of information that paints an intimate portrait of a person's life. When law enforcement uses a Stingray to follow an individual, whose cell phone number they do not have, to various locations in order to determine the targeted individual's number, the police create a powerful social and behavioral analysis map that will not only reveal the intimate details of the targeted person but also of innocent people who live and interact around those loca-

---

the interior of the premises that the government is extremely interested in knowing and that it could not have otherwise obtained without a warrant.").

[263] *See* Neil E. Klepeis et al., *The National Human Activity Pattern Survey (NHAPS): A Resource for Assessing Exposure to Environmental Pollutants*, 11 J. OF EXPOSURE ANALYSIS AND ENVTL. EPIDEMIOLOGY 231, 239 (2001), http://www.nature.com/jes/journal/v11/n3/pdf/7500165a.pdf [https://perma.cc/JN9E-VVVQ].

[264] Even though the majority in *Jones* did not employ such a technique, the opinion did indicate were they to have employed a *Katz* analysis, they would have looked at whether the electronic surveillance could have been done through traditional means. *See Jones*, 132 S. Ct. at 953–54 ("Thus, even assuming that the concurrence is correct to say that '[t]raditional surveillance' of Jones for a four-week period 'would have required a large team of agents, multiple vehicles, and perhaps aerial assistance,' our cases suggest that such visual observation is constitutionally permissible. It 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." (internal citations omitted)).

tions.[265] One U.S. Magistrate Judge has already taken note of this issue and has prohibited federal agents from using Stingrays when "an inordinate number of innocent third parties' information will be collected."[266] Judge Iain Johnston stated the devices are "simply too powerful" and invasive "to allow its use without specific authorization from a fully informed court."[267]

In the scenarios where the police are tracking an individual whose cell phone number they do have, the mosaic theory may not be as applicable because law enforcement will presumably not track them for as long and, therefore, not obtain as much information. Nonetheless, the concern remains that law enforcement may give in to the temptation to use a Stingray because of how easy it makes the tracking of suspects, resulting in "abuse, overreach, or misuse" by law enforcement.[268] This potential abuse of authority by law enforcement is the twenty-first century version of the fear that the Framers had and why they wanted to curb the discretionary authority of officers.[269] Additionally, the public does not agree that the length of the tracking should be the decisive factor in deciding a reasonable expectation of privacy on the real-time tracking of an individual's cell phone.[270] Society is prepared to recognize that the short term tracking of a person's location is a violation as well.

B. A Traditional Katz *Analysis*

This Part conducts a traditional *Katz* analysis of the use of Stingray devices. It argues first that society is prepared to recognize an expectation of privacy in real-time cell phone location data, and second that people actually have such an expectation.

---

[265] *See* AM. CIV. LIBERTIES UNION MICH., A TASTE OF ITS OWN MEDICINE: MICHIGAN HOLDS FIRST PUBLIC HEARING ON SECRETIVE HAILSTORM AND STINGRAY SURVEILLANCE DEVICES 3 (2014), http://www.aclumich.org/sites/default/files/ATasteOfItsOwnMedicine_Hailstorm_Stingray_Surveillance_2014.pdf [https://perma.cc/9ZKK-D94E] [hereinafter ACLU Michigan Stingray Report].

[266] *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 *3 (N.D. Ill. Nov. 9, 2015) [hereinafter Cell-Site Simulator Use Order].

[267] *Id*. at *4.

[268] ACLU Michigan Stingray Report, *supra* note 265, at 3.

[269] *See* Davies, *supra* note 114, at 578.

[270] *See* text accompanying *infra* note 280.

1. People Have an Objective Expectation of Privacy in Their Real-Time Cell Phone Location Data

Harlan's concurrence in *Katz* requires that for Fourth Amendment protection an expectation of privacy must "be one that society is prepared to recognize as 'reasonable.'"[271] Therefore, we must determine if society is prepared to recognize the real-time tracking of a person's location through his cell phone (i.e., use of a Stingray) as reasonable or to be a violation of that person's expectation of privacy.

The Supreme Court recognizes that society is concerned about the government's increasing use of electronic surveillance.[272] Ninety-two percent of Americans own cell phones and ninety percent of those users say their phone is frequently with them[273]—meaning law enforcement could track eighty-three percent of Americans with a Stingray on a daily basis if they wanted to. Forty-six percent of smartphone users say they couldn't live without their phones.[274] The Court recognizes that:

> Modern cell phones are not just another technological convenience. With all they . . . may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.[275]

The Court has already found that there is an expectation of privacy in telephone conversations conducted in public phone

---

[271] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[272] *See, e.g.*, *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms."); United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 312 (1972) (stating that the employment of electronic surveillance by government causes "a deep-seated uneasiness and apprehension that this capability will be used to intrude upon the cherished privacy of law-abiding citizens").

[273] *See* Rainie & Zickuhr, *supra* note 258.

[274] *See* Monica Anderson, *6 Facts About Americans and Their Smartphones*, PEW RES. CTR. (Apr. 1, 2015), http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/ [https://perma.cc/45GY-4QBD].

[275] Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (internal citations omitted).

booths[276] and the Sixth Circuit, relying upon principles laid out in *Katz*, found a reasonable expectation of privacy in emails as well.[277] The Sixth Circuit has recognized that "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[278] The use of Stingrays is precisely the kind of situation where the Fourth Amendment must keep pace with technology or we risk losing its protection altogether. Therefore, there needs to be a recognition of an objective expectation of privacy in real-time cell phone location data, especially when obtained through surveillance techniques that could not have been conducted without the use of the device.

Justice Alito's concurrence in *Jones* suggests that such an expectation will only be reasonable if it is over a long period of time because the duration of the tracking is the decisive factor.[279] The public simply does not agree with this opinion. In a study about Americans' privacy expectations, the results show that the percentage of respondents who believed that surveillance either definitely or likely violated a reasonable expectation of privacy rose by just three percentage points when the surveillance's duration was described as month-long rather than day-long.[280] Therefore, the relative short term tracking that may occur with the typical use of a Stingray should not be of a concern to a court. People are just as worried about their location being tracked for a day as they are for a month.

---

276 *See Katz*, 389 U.S. at 353 (majority opinion).

277 *See* United States v. Warshak, 631 F.3d 266, 289 (6th Cir. 2010).

278 *Id.* at 285.

279 *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in judgment) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.").

280 Matthew B. Kugler & Lior Jacob Strahilevitz, *Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory* 6 (Coase-Sandor Inst. for Law & Econ., Working Paper No. 727, 2015), http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2419&context=law_and_economics [https://perma.cc/Q2KH-5ERD]. The results went from 56% to 59% who believed tracking through GPS surveillance would definitely or likely violate a reasonable expectation of privacy, with 25% and 24% respectively believing such tracking definitely or likely did not violate a reasonable expectation of privacy. *Id.* at 34.

2. People Have a Subjective Expectation of Privacy in Their Real-Time Cell Phone Location Data

In order to constitute a search under Harlan's concurrence in *Katz*, a person must exhibit an actual or subjective expectation of privacy as well.[281] Citizens are right to, and in fact do, assume that their belongings "are not infected with concealed electronic devices."[282] This is precisely what a Stingray does though; it secretly forces a user's phone to connect to it and then gathers the information and location of the phone. Statistics support this inference as well—that people have an actual expectation of privacy in their phones and location.

In a 2014 survey, 82% of people considered their physical location to be sensitive material.[283] In a separate survey, 85.5% of respondents disagreed with *Knotts*, in which the Supreme Court upheld the warrantless installation of a tracking device on a vehicle.[284] Lastly, in a poll of Californians, 73% of the people favored "a law that required the police to convince a judge that a crime has been committed before obtaining location information from the cell phone company."[285] All of this indicates people have an actual expectation of privacy in their location and cell phones, despite what the Eleventh Circuit said in *Davis*.

---

[281] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[282] United States v. Karo, 468 U.S. 705, 735 (1984) (Stevens, J., concurring in part and dissenting in part).

[283] *See* MARY MADDEN, PEW RES. CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 34 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf [https://perma.cc/P4Y6-6EE4] (noting that fifty percent of adults feel that their physical location data is "very sensitive" and that another thirty-two percent of adults consider this data "somewhat sensitive").

[284] *See* Henry F. Fradella, et al., *Quantifying Katz: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 366 (2011).

[285] *See* Jennifer King & Chris Jay Hoofnagle, *A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Location Information* 8–9 (Apr. 18, 2008), https://www.ftc.gov/sites/default/files/documents/public_comments/beyond-voice-mapping-mobile-marketplace-534331-00005/534331-00005.pdf [https://perma.cc/49J7-5QM5].

C. *The Use of a Stingray is Different from the Acquisition of Historical Cell Tower Records*

The overarching difference between the Eleventh Circuit decision in *Davis* and the use of a Stingray is that when law enforcement uses a Stingray, they are not obtaining historical location data but instead are tracking cell phones in real-time. The *Davis* court specifically mentioned that this case does not involve "real-time or prospective cell tower location information."[286] While historical cell site location data only shows the user's "general vicinity,"[287] the tracking with a Stingray is precise. When looking at the step-by-step analysis taken by the *Davis* court, it only further illustrates the differences between historical and real-time cell phone location data.

The court's first consideration in *Davis* was that cell phone users have no expectation of privacy in their historical cell site locations under the third party doctrine because cell phone users know when making a call that their phone has to connect to a cell tower.[288] This changes with the use of a Stingray. When a Stingray is being used, a cell phone no longer connects to a cell tower but instead connects to the Stingray without alerting the user. The *Davis* court also identified that cell phones only emit such a signal when a person makes or receives a call.[289] This too changes when law enforcement uses a Stingray, as the device forces a connection with the phone even if no call is in progress.

The third consideration in *Davis* was that people know their phone's signal is sent to their service provider.[290] As just mentioned, with a Stingray the phone's signal is no longer being sent to a user's service provider but instead to the Stingray device unknowingly. In its final step, the *Davis* court determined that the cell phone user is aware that he is conveying cell tower location information to the service provider, and voluntarily does so.[291] In contrast, when a Stingray is in use, the cell phone user is not aware

---

286 *See* United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015).
287 *See id.* at 516.
288 *See id.* at 511.
289 *See id.*
290 *See id.*
291 *See id*.

that he is conveying his location to the Stingray device, nor is he voluntarily sending a cell signal to it at all; the Stingray forces the connection. Therefore, the third party doctrine that is so heavily relied upon in *Davis* is not applicable to Stingrays.

D. Approval to Use a Stingray May Constitute a General Warrant

In determining whether a particular government action violates the Fourth Amendment, a court is first to inquire "whether the action was regarded as an unlawful search or seizure under the common law when the Amendment was framed."[292] The Fourth Amendment prohibits general warrants.[293] The problem with general warrants is not necessarily of an intrusion, but of "a general, exploratory rummaging in a person's belongings."[294] This is exactly what the Framers were concerned with when writing the Fourth Amendment and is addressed by the Amendments' particularity requirement.[295]

This would seem to suggest that Stingrays are in direct conflict with the original meaning of the Fourth Amendment because they gather information from every cell phone within their range, whether or not there is a warrant for each phone it forces a connection with.[296] The particularity requirement requires a warrant to describe the person and things to be searched[297] but this simply is

---

[292] Wyoming v. Houghton, 526 U.S. 295, 299 (1999).

[293] *See* Andresen v. Maryland, 427 U.S. 463, 480 (1976).

[294] *Id.* (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)).

[295] *See id.*; *see also* U.S. CONST. amend. IV ("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." (emphasis added)).

[296] *See* Frank Knaack, *Stingrays—Bringing Dragnet Surveillance to a Town Near You*, AM. CIV. LIBERTIES UNION VA. (Sept. 26, 2014, 4:13 PM), https://acluva.org/16123/stingrays-bringing-dragnet-surveillance-to-a-town-near-you/ [https://perma.cc/VRL4-8EZ5]. This article also suggests that use of a Stingray should be banned all together because of First Amendment concerns as well. *Id.* While the Supreme Court held in *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958), that the government "cannot force a private association to turn over its membership list to the government, the introduction of Stingrays has provided law enforcement with a tool to get around this constitutional limitation." Knaack, *supra*. Law enforcement can stand near a meeting and collect information and identities from all nearby phones. *Id.*

[297] U.S. CONST. amend. IV.

not possible because of the fact that a Stingray searches every phone near it, not just of the person or thing law enforcement described in the warrant, were law enforcement to obtain one.[298]

However, one problem with this historical approach is that between the 1990 and 2001 terms, the Supreme Court ruled on twenty cases addressing the Fourth Amendment, yet only discussed the original meaning of the Amendment in four of these cases—suggesting they do not always begin with a historical analysis.[299] A second problem is that modern judges have struggled "in recounting the content of framing-era law."[300] Nonetheless, a historical argument of the Fourth Amendment is one to consider when discussing the possibility that approval to use a Stingray may constitute an illegal general warrant.

Even if you were not to base an analysis on the historical understanding of the Fourth Amendment, at the core of the Amendment is the right for any person to be free from governmental intrusion in his own home.[301] No warrant would allow the police to search every house in a neighborhood, but a Stingray allows the police to do just that.[302] Police can use a Stingray to search "every home, vehicle, purse and pocket in a given area,"[303] meaning that tens of thousands of innocent bystanders can potentially have information from their phones taken by law enforcement without anyone being the

---

[298] *See* Knaack, *supra* note 296.

[299] Seltzer, *supra* note 229.

[300] Davies, *supra* note 114, at 742 ("Justice Scalia repeated Chief Justice Taft's historically false claim that the allowance of warrantless ship searches in the 1789 Collections Act revealed the Framers' understanding of the Fourth Amendment's 'reasonableness' standard. Likewise, Justice Thomas has recently mischaracterized a statement by Blackstone as though it were relevant to the knock-and-announce rule for serving warrants.").

[301] *See* Kyllo v. United States, 533 U.S. 27, 31 (2001); Payton v. New York, 445 U.S. 573, 589–90 (1980).

[302] *See* Fenton, *supra* note 106; *see also* Tim Cushing, *Baltimore PD Hides Its Stingray Usage Under a Pen Register Order; Argues There's Really No Difference Between The Two*, TECHDIRT (Jan. 9, 2015, 6:10 PM), https://www.techdirt.com/articles/20150103/14461029590/baltimore-pd-hides-its-stingray-usage-under-pen-register-order-argues-theres-really-no-difference-between-two.shtml [https://perma.cc/FR9N-LH8C] (noting that since a Stingray searches the phones of anyone in the vicinity, a warrant to use such a device at the very least is an illegal general search warrant).

[303] Fenton, *supra* note 106.

wiser.[304] The fact that such a sweep may only pick up the identifying information of bystanders' cell phones does not matter because chances are that some of those bystanders will be in their homes, and all details in the home are intimate.

Additionally, there is a concern that the federal government will collect these innocent bystanders' numbers and then maintain those numbers in a database.[305] Such third party bystanders have greater privacy interests and are provided with more safeguards from the courts than litigants though.[306] In order to address this issue, one judge has limited the use of Stingrays, and in some situations banned their use altogether.[307] Therefore, while it may be unlikely that the use of a Stingray will be banned in all situations, they may be banned in certain situations on the basis that they are "fundamentally at odds with the Constitution."[308]

The legality of dragnet surveillance was recently looked at in *American Civil Liberties Union v. Clapper*.[309] In this case, the ACLU challenged the legality of the National Security Agency's ("NSA") telephone metadata[310] collection program,[311] arguing that the col-

---

[304] *See* Lisa Bartley, *Investigation: Law Enforcement Use Secret 'Stingray' Devices to Track Cell Phone Signals*, ABC7 (Dec. 3, 2014), http://abc7.com/news/investigation-law-enforcement-use-secret-devices-to-track-cell-phone-signals/421190/ [https://perma.cc/M6N8-YQA9].

[305] *See* Cell-Site Simulator Use Order, *supra* note 266, at *3.

[306] *Id*.

[307] *Id.* at *3–4.

[308] *See* Knaack, *supra* note 296.

[309] *See* ACLU v. Clapper, 785 F.3d 787 (2d. Cir. 2015).

[310] Telephone metadata are:

> [D]etails about telephone calls, including, for example, the length of a call, the phone number from which the call was made, and the phone number called. Metadata can also reveal the user or device making or receiving a call through unique "identity numbers" associated with the equipment . . . and provide information about the routing of a call through the telephone network, which can sometimes (although not always) convey information about a caller's general location. According to the government, the metadata it collected did not include cell site locational information, which provides a more precise indication of a caller's location than call-routing information does.

Id. at 793–94.

[311] In this program, the NSA "collect[ed] in bulk 'on an ongoing daily basis' the metadata associated with telephone calls made by and to Americans, and aggregated those metadata into a repository or data bank that can later be queried." *Id.* at 792.

lection program violated the Fourth Amendment.[312] The Second Circuit found that the language of section 215 of the PATRIOT Act did not authorize the program.[313] The court noted that the program was "shrouded in . . . secrecy . . . and only a limited subset of members of Congress had a comprehensive understanding of the program or of its purported legal bases."[314] Since there was "no opportunity for broad discussion in the Congress or among the public of whether the [federal government]'s interpretation of section 215 was correct," the program was not legislatively ratified.[315] Once the Second Circuit found the program to be illegal on statutory grounds, it did not rule on the constitutional issues.[316]

One issue with using *Clapper* as a corollary to Stingray use is that *Clapper* involved the authorization of the collection of data from millions of people in the interest of national security and counter-terrorism,[317] while Stingrays are typically used by state agencies to track anyone from killers to petty thieves and involve the alleged searches of tens of thousands of people, not millions. These are very different interests to be balanced by a court in weighing a person's reasonable Fourth Amendment interests against the legitimate interests of the government.

Nonetheless, the argument made by the ACLU in *Clapper*[318] provides an interesting theory and convinced the court to admit, in

---

312 *See id.* at 810.

313 *See id.* at 818.

314 *Id*. at 820.

315 *Id.* at 821.

316 *See id.* at 824.

317 *See generally id*.

318 Appellants argue that the telephone metadata program provides an archetypal example of the kind of technologically advanced surveillance techniques that, they contend, require a revision of the third-party records doctrine. Metadata today, as applied to individual telephone subscribers, particularly with relation to mobile phone services and when collected on an ongoing basis with respect to all of an individual's calls (and not merely, as in traditional criminal investigations, for a limited period connected to the investigation of a particular crime), permit something akin to the 24–hour surveillance that worried some of the Court in *Jones*. Moreover, the bulk collection of data as to essentially the entire population of the United States, something inconceivable before the advent of high-speed computers, permits the development of a government database with a

dicta, that the seriousness of the constitutional concerns raised had some bearing on what they held.[319] The court stated that the legislative process should serve the primary role "in deciding, explicitly and after full debate, whether such programs are appropriate and necessary. Ideally, such issues should be resolved by the courts only after such debate, with due respect for any conclusions reached by the coordinate branches of government."[320] This notion was confirmed when Congress subsequently amended the language of section 215 to create a 180-day transition period, which the Second Circuit upheld.[321] The court again declined to consider whether bulk collection of metadata violates the Fourth Amendment on the grounds that the transition period will soon expire and any violation of Fourth Amendment rights will be "temporary."[322] This suggests that legislators should be the ones to resolve the use of Stingrays as well.

IV. STATE LEGISLATORS NEED TO PROVIDE STATUTORY GUIDANCE ON THE USE OF STINGRAYS AND IF THEY DO NOT, COURTS SHOULD RULE ON THEM INSTEAD

As suggested in *Clapper* and elsewhere, in circumstances involving dramatic technological change, the best solution to privacy concerns are likely legislative.[323] Like the DOJ, DHS, Washington,

---

> potential for invasions of privacy unimaginable in the past. Thus, appellants argue, the program cannot simply be sustained on the reasoning that permits the government to obtain, for a limited period of time as applied to persons suspected of wrongdoing, a simple record of the phone numbers contained in their service providers' billing records.

Id. at 824.

319 *See id.*

320 *See id.* at 825.

321 *See* ACLU v. Clapper, 804 F.3d 617, 618 (2d Cir. 2015).

322 *Id.* at 626.

323 *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in judgment) ("A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."); United States v. Davis, 785 F.3d 498, 520 (11th Cir. 2015) ("If the rapid development of technology has any implications for our interpretation of the Fourth Amendment, it militates in favor of judicial caution, because Congress, not the judiciary, has the institutional competence to evaluate complex and evolving technologies.").

Utah, Virginia, California, and Minnesota, states and agencies need to implement their own guidelines or legislation on the use of Stingrays.

The remaining states should look to follow California's template and provide statutory guidance on the use of Stingrays. The California Electronic Communications Privacy Act is "the most comprehensive digital privacy law in the nation."[324] It ensures that law enforcement is granted a warrant prior to:

> [Obtaining] access to electronic information about who we are, where we go, who we know, and what we do. It requires a probable cause warrant for all digital content, location information, metadata, and access to devices like cell phones. The law's notice and enforcement provisions make sure that there is proper oversight and mechanisms to ensure that the law is followed . . . [and] still includes appropriate exceptions to ensure that the police can continue to effectively and efficiently protect public safety.[325]

While a legislative call to action across federal and state governments may be the ideal solution, it is not going to happen overnight, and courts need to provide a solution in the meantime. Therefore, when the use of a Stingray comes before a court, and where there is no statutory guidance in place, courts need to step in and decide whether evidence obtained as a result of Stingray use should be suppressed.[326] If courts are not allowed or choose not to

---

[324] *California Electronic Communications Privacy Act (CalECPA)—SB 178*, AM. CIV. LIBERTIES UNION N. CAL., https://www.aclunc.org/our-work/legislation/calecpa [https://perma.cc/VZ79-ZRHQ] (last visited Feb. 24, 2016) [hereinafter ACLU on CalECPA].

[325] *Id*. Most importantly, the Act has an exception for "an emergency involving danger of death or serious physical injury to any person." S.B. 178, 2015–2016 Leg., Reg. Sess. § 1546.1(c)(5) (Cal. 2015), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160SB178 [https://perma.cc/G43J-HEZ9].

[326] *See* Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843, 898 (2014); *see also* Johnson v. United States, 333 U.S. 10, 13–14 (1948) ("The 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

step in, the government essentially has total control over the legality of Stingray use with no oversight by acting as judge and jury on their use behind closed doors.[327]

Courts can and should step in to rule upon new investigative methods, as the legality of searches is significant for both defendants and society as a whole.[328] The protection provided by the courts "is one of the few ways in which the law can keep up with rapidly evolving technologies [when the legislators have declined to do so]—like the wiretapping in *Katz*, the thermal imaging in *Kyllo*, the GPS tracking in *Jones*, or the NSA's bulk collection of phone records today."[329] Thus, to allow the government to continue to hold unilateral control over the legality of Stingrays by withholding its use from the courts would clearly be detrimental to the privacy interests of society.[330]

Were a court given the chance to rule on the legality of a Stingray under the Fourth Amendment, the court should look to *Clapper* for guidance. Despite the Second Circuit not ruling on the Fourth Amendment issue (and the differences between the NSA data collection program and Stingrays), the court still made use of general doctrinal principles relevant to modern warrantless searches under the Fourth Amendment.[331] In discussing the Fourth Amendment implications of the case, the *Clapper* court made reference to the concern of "dragnet" surveillance in *Knotts*, the "mosaic" of information revealed through the surveillance in *Jones*, and that five of the Justices in *Jones* were suggesting that "there might be a Fourth Amendment violation even without the technical trespass upon which the majority opinion relied."[332]

---

competitive enterprise of ferreting out crime . . . . 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.").

327 *See* Toomey & Kaufman, *supra* note 326, at 898.

328 *See id*. at 898–99.

329 *See id.* at 899.

330 *See id.*

331 ACLU v. Clapper, 785 F.3d 787, 822 (2d Cir. 2015) ("Appellants' argument invokes one of the most difficult issues in Fourth Amendment jurisprudence: the extent to which modern technology alters our traditional expectations of privacy.").

332 *See id.* at 823.

It was argued that the telephone metadata program provided "an archetypal example of the kind of technologically advanced surveillance techniques that . . . require a revision of the third-party records doctrine."[333] As discussed previously, such a revision to the third party doctrine is not necessary to find Stingray use illegal under the Fourth Amendment.[334] Therefore, despite the fact that Stingrays do not invade upon the privacies of millions of people like the surveillance program in *Clapper*, they do conduct a sort of invasion of privacy that, as with the NSA's data collection program, was "unimaginable in the past."[335] If guidelines on the use of Stingrays are not going to be put forth by legislators in all jurisdictions, courts need to formulate their own guidelines on the use of Stingrays in order to protect the public's Fourth Amendment interests.[336]

CONCLUSION

The public should not be forced to sacrifice the modern convenience—some would even say necessity—of a cell phone in favor of privacy. The practice of tracking suspects of petty crime with Stingrays obtained through federal anti-terror grants needs to stop. Currently, those people found through the use of Stingrays have no idea such a device was used to find them, thereby leaving the opportunity to challenge that search within government control. Such a unilateral control over society's privacy interests is untenable. The real-time tracking of cell phone location data through a Stingray is illegal without a warrant and courts need to be given the opportunity to make such a ruling if legislators everywhere are not going to proactively implement their own statutory guidance on Stingrays.

---

333 *See id.* at 824.

334 *See supra* Section III.C.

335 *See Clapper*, 785 F.3d at 824.

336 The Seventh Circuit has finally taken up the issue in *United States v. Patrick* and will examine the Fourth Amendment implications of Stingray use. *See* Cyrus Farivar, *Warrantless Stingray Case Finally Arrives Before Federal Appellate Judges*, ARSTECHNICA (Jan. 29, 2016, 7:00 AM), http://arstechnica.com/tech-policy/2016/01/warrantless-stingray-case-finally-arrives-before-federal-appellate-judges/ [https://perma.cc/JHE5-4J2T]. In this case, Damian Patrick was located in a car by the Milwaukee Police Department, with strong evidence he was located through the use of a Stingray. *Id.* This case should finally provide some clarity to the warrantless use of Stingrays.