Boston College Law Review

Volume 57 | Issue 2 Article 8

3-31-2016

Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment

Jonathan Bard
Boston College Law School, jonathan.bard@bc.edu

UNPACKING THE DIRTBOX: CONFRONTING CELL PHONE LOCATION TRACKING WITH THE FOURTH AMENDMENT

Abstract: Surveillance technology has raced ahead of the Fourth Amendment, forcing courts to confront high-tech intrusions with rusty jurisprudence. The Dirtbox, an airborne cell-site simulator, allows the government to sweep entire cities and intercept individuals' cell phone location information without relying on cooperative intermediaries. This Note argues that the government's use of the Dirtbox and other cell-site simulators amounts to a Fourth Amendment search because it may pinpoint individuals within a constitutionally protected space. Although the Department of Justice issued policy guidelines requiring its agents to obtain a search warrant before using this device, this narrow and unenforceable protocol fails to adequately regulate the rising use of cell phone tracking devices. Until the U.S. Supreme Court accepts the opportunity to modernize the Fourth Amendment, Congress should enact legislation requiring all law enforcement agents to obtain a warrant before using the Dirtbox or other cell-site simulators.

INTRODUCTION

Anaheim, a small city in Southern California, is home to 350,000 residents, Disneyland, and an arsenal of military-grade spy equipment.[1] One of the devices used by the Anaheim Police Department is the Dirtbox, a plane-mounted surveillance system that impersonates a cell phone tower and

[1] Matthew Cagle, *Documents Reveal Anaheim, CA Has Surprisingly Robust Surveillance Arsenal for Small City*, AM. C.L. UNION: FREE FUTURE (Jan. 27, 2016, 6:45 PM), https://www.aclu.org/blog/free-future/documents-reveal-anaheim-ca-has-surprisingly-robust-surveillance-arsenal-small-city [https://perma.cc/3S4S-6PSC] (describing how local law enforcement in Anaheim has spent nearly a decade developing an inventory of powerful cell phone location monitoring technology); *see* Matt Ferner, *Anaheim Cops Have Had a Massive Spy Program for Years*, HUFFINGTON POST POL. (Jan. 28, 2016, 6:37 PM), http://www.huffingtonpost.com/entry/anaheim-cops-spy-program_us_56aa5ac3e4b0d82286d53737 [http://perma.cc/5A3N-XJWE] (noting that the police in Anaheim are using surveillance equipment thought to have only been used by the federal government and in larger cities). Documents obtained by the American Civil Liberties Union of California reveal that Anaheim law enforcement use at least three types of surveillance equipment. Ferner, *supra.* In 2009, Anaheim used a federal grant to purchase the Dirtbox, an airborne device capable of collecting information from thousands of cell phones. *Id.* Two years later, using a combination of federal grant money and local funds, Anaheim purchased the Stingray, a non-airborne Dirtbox. *Id.* Finally, in 2013, Anaheim acquired the Jugular, a hand-held monitoring device designed for covert location interception of cell phones within buildings. *Id.*

tricks targeted mobile phones into revealing their location within a ten-foot accuracy.[2]

Cell phone location tracking raises substantial privacy concerns and thus implicates the Fourth Amendment.[3] The Fourth Amendment guards against government encroachment on individuals' privacy, but its protections are not triggered unless a "search" has occurred.[4] The U.S. Supreme Court has determined that a search occurs when the government violates an individual's reasonable expectation of privacy.[5] Thus, if an individual has a reasonable expectation of privacy in his or her cell phone location information, the government must obtain a warrant before performing Dirtbox surveillance.[6] Courts and scholars are divided, however, as to whether people have a reasonable expectation of privacy in cellular location data and as

---

[2] Kim Zetter, *California Police Used Stingrays in Planes to Spy on Phones*, WIRED (Jan. 27, 2016, 6:28 PM), http://www.wired.com/2016/01/california-police-used-stingrays-in-planes-to-spy-on-phones/ [https://perma.cc/X27G-EA2J] (discussing how the Anaheim Police Department has owned the Dirtbox since 2009); *see* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL STREET J. (Nov. 13, 2014), http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533 [https://perma.cc/G78Z-5YMC] (revealing the aerial cell phone surveillance program operated by the U.S. Marshals and discussing the technological capacity of the Dirtbox). The Dirtbox (or DRTbox) is named after its maker, Digital Receiver Technology Inc., a Maryland-based subsidiary of Boeing that develops wireless surveillance and tracking equipment for the federal government and law enforcement. Barrett, *supra*; *see* News Release, Boeing, Boeing to Acquire Digital Receiver Technology to Enhance Capabilities in Intelligence Market (Nov. 14, 2008), http://boeing.mediaroom.com/2008-11-14-Boeing-Boeing-to-Acquire-Digital-Receiver-Technology-to-Enhance-Capabilities-in-Intelligence-Market [https://perma.cc/V5LW-DET5]. Secured to the underside of a soaring Cessna, the Dirtbox emits a phony signal that causes cell phones to recognize it as the closest cellular tower and transmit their location information. *See* Barrett, *supra*.

[3] *See* Barrett, *supra* note 2; *see also* U.S. CONST. amend. IV (protecting against unreasonable searches by the government); United States v. Karo, 468 U.S. 705, 707 (1984) (applying the Fourth Amendment to location tracking devices); United States v. Knotts, 460 U.S. 276, 277 (1983) (same).

[4] *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) (regarding the determination of whether a search has occurred to be an "antecedent question"); United States v. Jacobsen, 466 U.S. 109, 136–37 (1984) (noting that the Fourth Amendment only applies to searches and seizures); Katz v. United States, 389 U.S. 347, 353 (1967) (explaining that the Fourth Amendment protects people from unreasonable searches and seizures).

[5] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (noting that a Fourth Amendment search occurs when the government violates an individual's reasonable expectation of privacy); *see also* California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing *Katz*, 389 U.S. at 360 (Harlan, J., concurring)) (describing the reasonable expectation of privacy as the standard for Fourth Amendment protection); *Knotts*, 460 U.S. at 281 (applying the reasonable expectation of privacy test).

[6] *See Katz*, 389 U.S. at 357 (noting that, with few exceptions, warrantless searches violate the Fourth Amendment); *see also* United States v. Jones, 132 S. Ct. 945, 953 (2012) (explaining that cases of non-physical electronic surveillance are subject to Fourth Amendment analysis under *Katz*'s reasonable expectation of privacy test).

to what constitutional limitations, if any, should be placed on Dirtbox surveillance.[7]

This Note argues that Dirtbox surveillance amounts to a Fourth Amendment search and therefore the government must be required to get a warrant before using this technology.[8] When the government uses a device to determine an individual's location with sufficient accuracy to pinpoint them within a constitutionally protected space, such as the home, the Fourth Amendment demands that this search be conducted pursuant to a warrant.[9] Part I explores the foundations of the Fourth Amendment and discusses its application to location tracking.[10] Part II examines new developments in location tracking, including the Dirtbox.[11] Part II also outlines the efforts by the Department of Justice and various legislatures to regulate the use of the Dirtbox and other cell-site simulators.[12] Part III argues that the government's use of the Dirtbox and other cell-site simulators amounts to a Fourth Amendment search and that the U.S. Supreme Court and Congress must provide individuals with greater protection against novel surveillance techniques.[13]

---

[7] *See* United States v. Davis, 785 F.3d 498, 531 (11th Cir.) (holding that the defendant had no reasonable expectation of privacy in his cell phone location records held by his cellular provider, which were subject to the third-party doctrine), *cert. denied*, 136 S. Ct. 479 (2015); United States v. Skinner, 690 F.3d 772, 775 (6th Cir. 2012) (holding that the defendant did not have a reasonable expectation of privacy in his cell phone location information); State v. Tate, 849 N.W. 2d 798, 805 (Wis. 2014), *cert. denied*, 135 S. Ct. 1166 (2015) (mem.) (noting that the State of Wisconsin had conceded that cell site location tracking constitutes a Fourth Amendment search). Furthermore, the source of the location data—whether directly intercepted or obtained from a cellular provider—affects the legal analysis. *See In re* the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012) (holding that the pen register statute does not apply to the interception of cell phone location data by a Stingray); Brian L. Owsley, *Spies in the Skies: Dirtboxes and Airplane Electronic Surveillance*, 113 MICH. L. REV. FIRST IMPRESSIONS 75, 81–82 (2015), http://michiganlawreview.org/wp-content/uploads/2015/08/113MichLRevFI75_Owsley.pdf [https://perma.cc/WJL9-ZKGZ] (arguing that Dirtbox surveillance amounts to a Fourth Amendment search and therefore requires a warrant supported by probable cause).

[8] *See infra* notes 140–186 and accompanying text.

[9] *See Kyllo*, 533 U.S. at 34 (holding that the acquisition by sense-enhancing technology of information about the inside of a home constitutes a Fourth Amendment search); *Karo*, 468 U.S. at 716 (holding that the government is not exempt from the warrant requirement when it uses an electronic device to determine whether an item or person is inside of an individual's home); *see also Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring) (applying the mosaic theory to location tracking).

[10] *See infra* notes 1–73 and accompanying text.

[11] *See infra* notes 74–113 and accompanying text.

[12] *See infra* notes 114–139 and accompanying text.

[13] *See infra* notes 140–186 and accompanying text.

I. THE EVOLUTION OF THE FOURTH AMENDMENT

The Fourth Amendment protects against unreasonable searches by requiring the government to obtain warrants for almost all searches.[14] To trigger this protection, however, a court must determine that a search has taken place.[15] Section A of this Part explores the evolution of the Fourth Amendment.[16] Section B examines the Fourth Amendment in the context of location monitoring.[17]

A. The Fourth Amendment Search, from Places to People

The definition of search, under the Fourth Amendment, has evolved substantially over the past fifty years.[18] At the time of the Fourth Amendment's ratification, a search was best understood as a physical trespass by the government on one's private property.[19] In the latter half of the twenti-

---

[14] U.S. CONST. amend. IV (providing "[t]he right of the people to be secure . . . against unreasonable searches and seizures"); *Jones*, 132 S. Ct. at 953 (applying "an 18th-century guarantee against unreasonable searches"); United States v. Sharpe, 470 U.S. 675, 682 (1985) (explaining that the Fourth Amendment does not "guarantee against *all* searches and seizures, but only against *unreasonable* searches and seizures"). Subject to a few exceptions, a search is reasonable only when it is conducted pursuant to a warrant. Kentucky v. King, 563 U.S. 452, 459 (2011) (citing Brigham City v. Stuart, 547 U.S. 398, 398 (2006)) (noting that the Fourth Amendment requires that searches be reasonable, though not necessarily executed under warrant). *But see Katz*, 389 U.S. at 357 (emphasizing that, with a narrow class of exceptions, warrantless searches are per se unreasonable). Although the Court has recently favored the reasonableness requirement over the warrant requirement, scholars continue to debate the precise mandate of the language of the Fourth Amendment. *Compare* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 736 (1999) (arguing that although history does not clearly support either a warrant-preference or a generalized-reasonableness construction, the former is more consonant with the framers' intent), *with* Akhil R. Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 759 (1994) (arguing that a search need only be reasonable, but not necessarily warranted, to comply with the Fourth Amendment). When the government obtains evidence in violation of the Fourth Amendment, the exclusionary rule allows for suppression of that evidence at trial. *See* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 118 (2007) (citing Mapp v. Ohio, 367 U.S. 643, 655 (1961)).

[15] *See Kyllo*, 533 U.S. at 31 (regarding the determination of whether a search has occurred to be an "antecedent question"); *Jacobsen*, 466 U.S. at 136–37 (noting that the Fourth Amendment only applies to searches and seizures); *Katz*, 389 U.S. at 353 (explaining that the Fourth Amendment protects people from unreasonable searches and seizures); *see also* Widgren v. Maple Grove Twp., 429 F.3d 575, 578 (6th Cir. 2005) (describing the word "search" as a complex legal term of art).

[16] *See infra* notes 18–43 and accompanying text.

[17] *See infra* notes 44–73 and accompanying text.

[18] *Compare* Olmstead v. United States, 277 U.S. 438, 457 (1928) (equating a "search" with a physical trespass), *with Katz*, 389 U.S. at 351, 353 (concluding that a "search" is violation of an individual's reasonable expectation of privacy).

[19] *See Olmstead*, 277 U.S. at 464 (holding that no Fourth Amendment search had occurred when the government conducted wiretapping without physically trespassing on the defendants' property); Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 998 (1982) (describing how the Fourth Amendment was historically construed as providing property protec-

eth century, the U.S. Supreme Court expanded the scope of the term, considering a search to occur when the government violates an individual's reasonable expectation of privacy.[20] Although this new model generally expanded privacy protection, the subsequent third-party doctrine carved out swaths of information from the scope of the Fourth Amendment.[21]

In 1886, in *Boyd v. United States*, the U.S. Supreme Court provided the first interpretation of the term "search."[22] In *Boyd*, the Court examined pre-Revolutionary cases to determine that the compelled production of private papers constituted a search under the Fourth Amendment, analogizing forced document production to the physical invasion of one's home.[23] In doing so, the Court expressed a clear preference for a liberal interpretation of the Fourth Amendment.[24]

In 1928, in *Olmstead v. United States*, the Court retreated from its liberal interpretation of the Fourth Amendment in *Boyd* to the physical trespass model of colonial times.[25] The Court considered the activities of federal agents who had placed a wiretap on the phone lines of various bootlegging suspects.[26] The Court held that no search had occurred because the officers never physically trespassed on the defendants' property.[27]

---

tion). The framers of the Constitution enacted the Fourth Amendment as a direct response to intrusive home searches carried out by the British government under broad, unspecified warrants. *See* Stanford v. Texas, 379 U.S. 476, 482 (1965) (noting that the Fourth Amendment arose from the colonists' revulsion against general writs of assistance); Davies, *supra* note 14 at 724.

[20] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (setting forth the current two-part test used to determine whether a search has occurred); *see also* California v. Greenwood, 486 U.S. 35, 40–41 (1988) (holding that the defendants did not have a reasonable expectation of privacy in the contents of garbage bags they placed at the curb); California v. Ciraolo, 476 U.S. 207, 214 (1986) (holding that the warrantless aerial observation of a homeowner's yard did not violate the Fourth Amendment because his expectation of privacy was not reasonable).

[21] *See Katz*, 389 U.S. at 351 (laying the foundation of the third-party doctrine); *see also* Smith v. Maryland, 442 U.S. 735, 743 (1979) (applying the third-party doctrine in holding that Fourth Amendment protection does not extend to numbers dialed on a telephone); United States v. Miller, 425 U.S. 435, 442 (1976) (applying the third-party doctrine in holding that government acquisition of an individual's bank records does not constitute a search).

[22] *See* Boyd v. United States, 116 U.S. 616, 622 (1886).

[23] *Id.* (holding that requiring an individual to produce private papers amounts to a Fourth Amendment search); *see* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 312 (1998) (noting that *Boyd* marked the beginning of the Court defining Fourth Amendment protections as property rights).

[24] *See Boyd*, 116 U.S. at 635 (explaining that the Fourth Amendment must be broadly interpreted to avoid constitutional violations); Radin, *supra* note 19, at 998 (describing the historical framing of the Fourth Amendment as protecting property).

[25] *See Olmstead*, 277 U.S. at 466 (holding that the Fourth Amendment does not protect telephone communications in the absence of physical trespass).

[26] *Id.* at 456–57 (describing how federal prohibition officers discovered the conspiracy by affixing wiretaps to the telephone wires of the homes of four of the suspects and the central office).

[27] *See id.* at 457 (holding that the Fourth Amendment did not protect against wiretapping that did not involve physical trespass on the property of the defendants). In a dissenting opinion, Justice

In 1967, in *Katz v. United States*, the U.S. Supreme Court revisited the historical, trespass-based interpretation of search and held that the Fourth Amendment protects an individual's privacy interest, not merely their property.[28] The Court determined that the FBI had carried out an unconstitutional search when they attached an electronic eavesdropping device to the outside of a public telephone booth from which the defendant, a suspected illegal gambler, had been placing calls.[29] Justice Harlan, concurring, set forth a two-part test for determining whether a search has taken place.[30] Under this test, a court may find that a search has occurred only where (1) the defendant exhibited an expectation of privacy, and (2) society is prepared to recognize that expectation as reasonable.[31] This privacy-based analysis has survived the test of time and remains determinative of whether Fourth Amendment protections apply in a given situation.[32]

Although *Katz* expanded Fourth Amendment safeguards in many ways with the privacy-based model, the majority, in one sentence, simultaneously gauged out innumerable privacy rights.[33] The majority articulated what

---

Brandeis criticized the majority's narrow interpretation of the term search and forecast a reconceptualization of the Fourth Amendment that would come four decades later. *See id.* at 474–75 (Brandeis, J., dissenting) (arguing that the essence of the Fourth Amendment is a guarantee of personal privacy, rather than a protection against physical intrusion); *see also Katz*, 389 U.S. at 351 (holding that "the Fourth Amendment protects people, not places").

[28] *Katz*, 389 U.S. at 351, 353 (concluding that Fourth Amendment had developed beyond the trespass doctrine to provide privacy protection). Although many courts, including the U.S. Supreme Court itself, have interpreted *Katz* as overruling the physical trespass model of *Olmstead*, the Court recently clarified that *Katz* merely expanded the traditional trespass-based notion of a search articulated in *Olmstead*. *See Jones*, 132 S. Ct. at 952 (explaining that the reasonable expectation of privacy test from *Katz* was an addition to, rather than a substitute for, the trespass doctrine); *Kyllo*, 533 U.S. at 32 (noting that the Court no longer required physical trespass to find a Fourth Amendment violation); *Karo*, 468 U.S. at 713 (observing that a physical trespass is not a necessary or a sufficient condition for a violation of the Fourth Amendment); *see also Katz*, 389 U.S. at 351, 353 (concluding that physical trespass was not a prerequisite of a Fourth Amendment violation); *Olmstead*, 277 U.S. at 466 (holding that no Fourth Amendment violation occurred where the government had not conducted a physical trespass).

[29] *Katz*, 389 U.S. at 353 (holding that the government violated the defendant's reasonable expectation of privacy, and therefore the Fourth Amendment, when it used an electronic eavesdropping device to listen to and record his telephone conversation).

[30] *See id.* at 361 (Harlan, J., concurring).

[31] *See id.* (setting forth the reasonable expectation of privacy test).

[32] *See Kyllo*, 533 U.S. at 32–33 (noting that Justice Harlan's concurrence articulated what is now the test for whether a Fourth Amendment search has occurred); *see also Ciraolo*, 476 U.S. at 211 (citing *Katz*, 389 U.S. at 360 (Harlan, J., concurring)) (describing the reasonable expectation of privacy as the standard for Fourth Amendment protection); *Knotts*, 460 U.S. at 281 (applying the reasonable expectation of privacy test).

[33] *See Katz*, 389 U.S. at 351 (explaining that information knowingly exposed to the public does not receive Fourth Amendment protection); Erin Smith Dennis, *A Mosaic Shield:* Maynard*, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 749 (2011) (describing how the third-party doctrine curtails Fourth Amendment protection); *see also* Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Ap-*

would later become the most controversial feature of the Fourth Amendment—the third-party doctrine.[34]

The Fourth Amendment does not protect information that one knowingly exposes to the public.[35] Although typically understood as an exception to the Fourth Amendment, the third-party doctrine is not a true exception because it fits squarely within the two-part *Katz* test.[36] Specifically, third-party divulgence undermines the second prong of the *Katz* test, as society is not prepared to recognize as reasonable an expectation of privacy in information that one knowingly shares with a third party.[37]

In 1976, in *United States v. Miller*, the U.S. Supreme Court formulated the expansive modern approach to the third-party doctrine.[38] The Court held that it was constitutional for the government to subpoena the defendant's

---

ply, 54 B.C. L. REV. 1, 14–28 (2013) (discussing the application of the third-party doctrine to the Internet).

[34] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) (suggesting that scholars love to hate the third-party doctrine); *see also* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 747 (4th ed. 2004) (arguing that one of the leading third-party doctrine cases is "dead wrong" and that the Court's faulty reasoning on the third-party doctrine "does great violence to the theory of Fourth Amendment protection which the Court had developed in *Katz*").

[35] *Katz*, 389 U.S. at 351 (explaining that knowingly exposed information does not receive Fourth Amendment protection). The roots of the third-party doctrine trace back to nearly a century before *Katz* to the "plain view doctrine," which accords no Fourth Amendment protection to objects visible to an inspecting officer. *See Ex parte* Jackson, 96 U.S. 727, 736 (1877) (holding that information exposed on the outside of a parcel of mail is not entitled to Fourth Amendment protection).

[36] *See Katz*, 389 U.S. at 351.

[37] *See* Greg Nojeim, *Why the Third-Party Records Doctrine Should Be Revisited*, A.B.A. (Aug. 1, 2012), http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch4/ch4_ess10.html [https://perma.cc/GD9W-6CPA] (explaining that a divulging party cannot reasonably expect privacy in information shared with third parties because they may disclose that information). *But see* Kerr, *supra* note 34, at 588 (arguing that the third-party doctrine operates as a form of consent rather than an application of the reasonable expectation of privacy test).

[38] *See Miller*, 425 U.S. at 442; *see also* LAFAVE, *supra* note 34, at 744 (noting the opportunities for law enforcement to conduct surveillance through examination of third-party business records are greater then ever before and will continue to grow in the future). In a series of cases on undercover informants, the Court held that defendants were not entitled to Fourth Amendment protection for confidential information that they disclosed to undercover agents. *See* Lee v. United States, 343 U.S. 747, 751 (1952) (holding that Fourth Amendment protection did not apply where the defendant knowingly divulged confidential information to an undercover agent); *see also* United States v. White, 401 U.S. 745, 747 (1971) (holding that no search had occurred where the defendant invited an informant to participate in an incriminating conversation with him); Hoffa v. United States, 385 U.S. 293, 302 (1966) (same); Lewis v. United States, 385 U.S. 206, 207 (1966) (same); Lopez v. United States, 373 U.S. 427, 439 (1963) (same). The Court anchored these decisions in the assumption of risk theory, a doctrine typically associated with tort law. *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 108 (1972) (illustrating the assumption of risk doctrine through its most basic application, namely that a person sharing a secret with another assumes the risk of betrayal).

bank to obtain his financial records because the defendant had voluntarily conveyed that information to the bank.[39] The Court stated that the defendant had assumed the risk that the bank would share these records with the government.[40]

Subsequently, in 1979, in *Smith v. Maryland*, the U.S. Supreme Court held that the warrantless installation of a pen register, which recorded the telephone numbers that the defendant dialed, did not violate the Fourth Amendment.[41] The Court found that the defendant did not have a legitimate expectation of privacy in the numbers that he dialed.[42] Citing *Miller*, the Court reaffirmed its position that one cannot reasonably expect privacy in information voluntarily conveyed to a third party.[43]

B. Beepers, GPS, and Locational Privacy

The Fourth Amendment protects an individual's physical location from certain forms of government surveillance.[44] Applying *Katz*'s reasonable

---

[39] *Miller*, 425 U.S. at 442 (observing that all of the documents obtained by the government contained information that is voluntarily shared with banks and their employees in the normal course of business). *But see id.* at 451 (Brennan, J., dissenting) (insisting that disclosures to a bank are not completely voluntary because one cannot lead a modern life without a bank account).

[40] *Id.* at 443 (majority opinion) (citing *White*, 401 U.S. at 751–52) (invoking the assumption of risk doctrine in the context of bank disclosures). The defendant argued that he maintained a reasonable expectation of privacy in his bank records because he disclosed them to the bank for a limited purpose. *See id.* at 442. The majority, however, insisted that disclosures to third parties, whether for a limited purpose or not, fall within the assumption of risk doctrine and are not protected by the Fourth Amendment. *Id.* at 443; *see Jacobsen*, 466 U.S. at 117. *But see Smith*, 442 U.S. at 749 (Marshall, J., dissenting) (contending that disclosures made solely for business purposes should not be subject to the assumption of risk doctrine).

[41] *See Smith*, 442 U.S. at 742 (majority opinion).

[42] *See id.* at 743–44 (noting the Fourth Amendment's inapplicability to third-party disclosures).

[43] *See id.* at 744 (explaining that the defendant had voluntarily conveyed numerical information to the phone company, thereby assuming the risk that the company would share the information with the police). Since the Court solidified the third-party doctrine in *Miller* and *Smith*, circuit courts have split over its application to modern technology. *See id.* at 743 (applying the third-party doctrine to dialed telephone numbers); *Miller*, 425 U.S. at 443 (applying the third-party doctrine to bank records). *Compare* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (declining to extend the third-party doctrine to the content of email intended for a recipient), *with* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (citing *Smith*, 442 U.S. at 742) (applying the third-party doctrine to routing data that the internet service provider required in order to transmit information). The third-party doctrine extends beyond bank records and dialed digits. *See Greenwood*, 486 U.S. at 40 (holding that police had not conducted a search when they inspected the contents of the defendants' garbage bags, which were conveyed to them by the third-party trash collector). *But see* State v. Galloway, 198 P.3d 383, 387 (Or. Ct. App. 2005) (holding that police conducted a Fourth Amendment search when they looked through garbage before it could be gathered by the trash collector).

[44] *See Jones*, 132 S. Ct. at 949 (holding that the government conducted a Fourth Amendment search when it attached a Global Positioning System ("GPS") tracker to a target's vehicle and collected information about the vehicle's movements); *Kyllo*, 533 U.S. at 34 (holding that the use

expectation of privacy analysis, the U.S. Supreme Court has set forth a class of monitoring activities that amount to a search and must be conducted pursuant to a warrant.[45]

In a pair of decisions on government tracking through beepers, the U.S. Supreme Court established that an individual has a reasonable expectation of privacy in location while inside a private residence, but not while traveling on public roads.[46] Although these two cases involved now-obsolete technology, the underlying principles continue to inform judicial treatment of location monitoring by the government.[47]

In 1983, in *United States v. Knotts*, the Court held that a person does not have a reasonable expectation of locational privacy while traveling on public roads.[48] The Court considered whether the government violated the Fourth Amendment by using a beeper to track the location of a suspected drug manufacturer's vehicle as he drove on public roads to a secluded cabin.[49] According to the Court, the beeper had merely augmented the senses of the police, as they could have obtained the same evidence through visual

---

of sense-enhancing technology to obtain information about the interior of a home that could only have been obtained through physical intrusion constitutes a Fourth Amendment search).

[45] *See Karo*, 468 U.S. at 716 (holding that the government implicates the Fourth Amendment by using an electronic tracking device to determine if a person or object is located within a constitutionally protected space); *see also Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (noting that even short-term monitoring raises substantial privacy concerns); *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (expressing concern about long-term location monitoring); Dennis J. Braithwaite & Allison L. Eiselen, *Nowhere to Hide? An Approach to Protecting Reasonable Expectations of Privacy in Cell Phone Location Data Through the Warrant Requirement*, 38 AM. J. TRIAL ADVOC. 287, 308 (2014) (noting that the U.S. Supreme Court has not decided whether the acquisition of cell-site location information amounts to a Fourth Amendment search).

[46] *See Karo*, 468 U.S. at 716; *Knotts*, 460 U.S. at 281.

[47] *See Jones*, 132 S. Ct. at 953–54 (discussing the applicability of *Knotts* and *Karo* but ultimately distinguishing them based on their facts). Before relying on satellites and cell phones, law enforcement agents tracked the location of suspects using a beeper, a small radio transmitter that emits signals and provides directional information. *See Knotts*, 460 U.S. at 277 (describing a beeper as a battery-operated radio device that transmits signals to a receiver); Jerry L. Dowling, *"Bumper Beepers" and the Fourth Amendment*, 13 CRIM. L. BULL. 266, 266 (1977). Beepers are "directional finders" because they provide information about the relative direction of the subject being tracked, but not its precise location. *See* Brief of Center for Democracy & Technology et al. as Amici Curiae in Support of Respondent at 15–18, *Jones*, 132 S. Ct. 945 (No. 10-1259) [hereinafter Amicus Brief in Support of Respondent] (explaining that beepers provide only rough approximations of the direction and distance of the vehicle relative to the location of the receiver). Because neither the beeper nor its receiver can store location information, the utility of this device is limited to real-time surveillance. Dowling, *supra*, at 269 (explaining that because beepers are limited to real-time monitoring, they are used to supplement visual surveillance by filling in a gap in visual contact).

[48] *Knotts*, 460 U.S. at 281 (holding that an individual traveling in a vehicle on public roads does not have a reasonable expectation of privacy in his or her movements).

[49] *Id.* at 277.

surveillance.[50] Because the police had ceased beeper monitoring upon the defendant's arrival at the cabin, the Court was not confronted with the weighty Fourth Amendment implications of privacy within the home.[51]

The following year, in *United States v. Karo*, the Court was squarely presented with the question left open by *Knotts*: does warrantless beeper surveillance violate the Fourth Amendment when it is carried out in a private residence?[52] The Court answered in the affirmative.[53] Agents of the Drug Enforcement Administration placed a beeper in a can of ether that the defendant had planned to use to manufacture drugs.[54] Using the beeper, the agents tracked the whereabouts of the can as the defendant and his associates moved it between various houses and storage facilities.[55] Distinguishing this case from *Knotts*, the Court held that the use of a tracking device within a home constitutes a search and is therefore subject to the Fourth Amendment's warrant requirement.[56] The Court decided both *Knotts* and *Karo* under *Katz*'s reasonable expectation of privacy test, affirming that the historical sanctity of the home would not be eroded by novel tracking technology.[57]

In 2001, in *Kyllo v. United States*, the U.S. Supreme Court held that the use of sense-enhancing technology to obtain information about the interior of a home that could only have been accessed through physical intrusion constitutes a search, at least where such technology is not in general public use.[58] Suspecting that the defendant was growing marijuana in his Oregon

---

[50] *Id.* at 282 (holding that the Fourth Amendment does not prohibit police from utilizing sensory enhancement devices).

[51] *Id.* at 284–85 (noting that there was no evidence to indicate that the beeper device had been used after the defendant arrived at the residence); *see* Stephen P. Jones, *Reasonable Expectations of Privacy: Searches, Seizures, and the Concept of Fourth Amendment Standing*, 27 U. MEM. L. REV. 907, 957 (1997) (observing that the home receives the strongest Fourth Amendment protection of all places); *see also* Payton v. New York, 445 U.S. 573, 601 (1980) (noting the historical sanctity of the home).

[52] *Karo*, 468 U.S. at 707.

[53] *Id.* at 714.

[54] *Id.* at 708.

[55] *Id.* at 708–09, 714 (describing how law enforcement used the beeper to locate the ether in a specific house).

[56] *Id.* at 716 (rejecting the notion that the government should be able to use an electronic device to determine if somebody or something is inside an individual's home at a certain time without being subjected to Fourth Amendment constraints); *see Knotts*, 460 U.S. at 281 (holding that one cannot have a reasonable expectation of locational privacy while traveling in a vehicle on public roads).

[57] *See Karo*, 468 U.S. at 714 (holding that monitoring an individual's location within a home violates reasonable privacy expectations under the Fourth Amendment); *Knotts*, 460 U.S. at 281 (holding that tracking an individual's travel on public roads does not violate the Fourth Amendment because one cannot reasonably expect such movement to be private); *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (setting forth the reasonable expectation of privacy test).

[58] *See Kyllo*, 533 U.S. at 34.

residence, federal agents used a thermal imager to determine that a portion of the house was substantially warmer than the rest of the house and neighboring homes.[59] Honoring the deep-rooted inviolability of the home, the Court held that the government had infringed the defendant's reasonable expectation of privacy.[60] Central to the Court's decision was its concern that technological innovation would allow law enforcement to strip away individuals' Fourth Amendment right to privacy.[61]

In 2012, in *United States v. Jones*, the Court revisited the issue of beeper surveillance, but left the *Knotts-Karo* public travel framework undisturbed by anchoring its decision in a physical trespass theory.[62] Law enforcement, suspecting that the defendant was engaged in narcotics trafficking, affixed an electronic GPS tracking device to the bottom of an automobile registered to the defendant's wife.[63] Over the next twenty-eight days,

---

[59] *See id.* at 30 (describing how the thermal scan of the defendant's home revealed a higher temperature on the roof and outer wall than the rest of the home). Based on these thermal scans and other evidence, a judge issued a search warrant of the defendant's home, which was found to contain a substantial marijuana growing operation. *See id.* (noting that the judge issued a warrant based on the thermal imaging, utility bills, and tips from informants).

[60] *See id.* at 34–35 (discussing the historical sanctity of the home before concluding that the use of a thermal imager amounted to a Fourth Amendment search); *see also Payton*, 445 U.S. at 590 (insisting that the Fourth Amendment provides rigid protection against home intrusions); Silverman v. United States, 365 U.S. 505, 511 (1961) (describing how privacy within the home stands at the core of the Fourth Amendment); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 58 (2008) (tracing the sanctity of the home back to antiquity).

[61] *See Kyllo*, 533 U.S. at 35–36 (rejecting a mechanical interpretation of the Fourth Amendment that would allow law enforcement to use new technology to discern activity within the home). The Court acknowledged the limitations of the thermal imager used by the agents, but recognized it was necessary to craft an approach that would protect against encroachments carried out by more sophisticated devices. *See id.* at 36 (noting that, despite the relatively unsophisticated device used in this case, the Court needed to adopt a rule in anticipation of more advanced technology in the future).

[62] *See Jones*, 132 S. Ct. at 949 (holding that a Fourth Amendment search had occurred where the government had physically trespassed on an individual's property to obtain information); Steven I. Friedland, Riley v. California *and the Stickiness Principle*, 14 DUKE L. & TECH. REV. 121, 132 (2016) (observing that *Jones* offered the Court an opportunity to modernize the *Katz* doctrine to account for novel tracking technology but the Court instead retreated to the physical trespass model of the Fourth Amendment).

[63] *Jones*, 132 S. Ct. at 948. Originally developed for the military, GPS technology provides law enforcement with location tracking that is far more sophisticated than directional information from beepers. *See* Amicus Brief in Support of Respondent, *supra* note 47, at 16–22. Relying on a constellation of satellites, GPS broadcasts three-dimensional navigation data to anybody on Earth with a GPS receiver. *Id.* at 7 (describing how the receiver uses satellite data to determine the receiver's location). Beyond its improved accuracy over beepers, GPS is entirely automated—it does not require that an officer physically pursue a suspect. *Id.* at 16–17, 21 (noting that GPS conducts automatic data collection and does not need to be monitored by a human in real time); *see GPS Accuracy*, GPS.GOV, http://www.gps.gov/systems/gps/performance/accuracy/ [https://perma.cc/BF88-STN6] (describing how a high-quality GPS receiver can provide location information that is accurate within 3.5 meters). Finally, GPS data is not limited to real-time, but can be recorded over a

the government tracked the movements of the vehicle, ultimately amassing over 2000 pages of location data.[64]

Relying on the trespass model, the Court held that the government had conducted an unconstitutional search.[65] Writing for the majority, Justice Scalia focused on the text of the Fourth Amendment, as well as its history, and declined the opportunity to modernize the framework.[66] Justice Scalia first fit the defendant's car within the enumerated spheres protected under the Fourth Amendment, asserting that "a vehicle is an 'effect.'"[67] He then concluded that the government's physical attachment of the tracking device to the underside of the defendant's vehicle and subsequent monitoring amounted to a Fourth Amendment search.[68]

Justices Sotomayor and Alito authored opinions, concurring with the majority's result but expressing a preference for the privacy-based "mosaic theory" over the resurrection of the trespass model, which has limited applicability to twenty-first-century technology.[69] The mosaic theory considers prolonged surveillance to amount to a search because it reveals a com-

---

prolonged period. Amicus Brief in Support of Respondent, *supra* note 47 at 16–17 (noting that GPS allows for twenty-four-hour, long-term location tracking and uses few resources).

[64] *See Jones*, 132 S. Ct. at 948. Using satellites, the device communicated to the government the vehicle's location within fifty to one hundred feet. *See id.*

[65] *See id.* at 949; *see also* Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 7 (2012) (noting that the physical trespass in *Jones* allowed the case to be decided without reliance on *Katz*'s reasonable expectation of privacy test).

[66] *See Jones*, 132 S. Ct. at 949 (holding that the physical intrusion of the GPS device and its subsequent data collection would have been considered a search under the original interpretation of the Fourth Amendment); *see also Kyllo*, 533 U.S. at 34 (noting that the physical trespass doctrine sets a floor to Fourth Amendment protection).

[67] *Jones*, 132 S. Ct. at 949 (declaring that a vehicle counts as an "effect" under the Fourth Amendment); *see* U.S. CONST. amend. IV (providing "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").

[68] *Jones*, 132 S. Ct. at 949 (holding that the government conducted a search by installing a GPS device on the defendant's vehicle and subsequently using it to monitor the movements of the vehicle). The Court distinguishes the unconstitutional search in *Jones* from the similar, yet constitutional, search in *Knotts* using a theory of consent by the owner. *See id.* at 952 (noting that the search in *Knotts* implicated the reasonable expectation of privacy test but not the trespass theory); *Knotts*, 460 U.S. at 278–79 (describing how officers installed a tracking device inside the chemical container with the consent of its then-owner). Although the vehicle in *Jones* was registered to the defendant's wife, the Court explains that he was the exclusive driver, which bestowed upon him the property rights of a bailee and accorded Fourth Amendment protection to the automobile. *Jones*, 132 S. Ct. at 949 n.2.

[69] *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (expressing a preference for resolving the case under the reasonable expectation of privacy test and considering the implications of prolonged surveillance, including government knowledge of one's political beliefs, religious practices, and sexual habits); *id.* at 962 (Alito, J., concurring) (noting that the Court's reliance on the trespass doctrine would present difficult issues in cases involving electronic surveillance).

plete and intimate picture of a person's life.[70] Notably, *Jones* shows that the mosaic theory has won the support of five Justices.[71] Justice Sotomayor took a firmer stand against government intrusions than the majority, suggesting that the Court consider abandoning the third-party doctrine and arguing that surveillance also implicates the First Amendment.[72] Ultimately, because the mosaic theory is not law and the *Jones* majority rested its decision on the physical trespass model, the Fourth Amendment continues to provide little guidance on the increasingly pervasive non-attachment-based location monitoring.[73]

II. TRACKING TECHNOLOGY RACES AHEAD OF THE LAW

This Part explores government acquisition of cell phone location information through third-party cooperation and direct interception, and describes efforts by the U.S. Department of Justice ("DOJ") and various state legislatures to regulate the Dirtbox and other cell-site simulators.[74] Section A de-

---

[70] *See* CIA v. Sims, 471 U.S. 159, 178 (1985) (describing how individual activities, although trivial when viewed in isolation, are far more telling when observed in context); United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (noting that prolonged surveillance may reveal a complete picture of an individual's life), *aff'd in part sub nom. Jones*, 132 S. Ct. 945. The mosaic theory represents a departure from the traditional application of the Fourth Amendment, which requires a court to scrutinize each government act individually. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315 (2012) (observing that courts determine whether a Fourth Amendment search has occurred by analyzing a particular government action in isolation). In contrast, a court employing the mosaic doctrine examines a collection of government actions over time as one potential "search." *See id.* at 320 (describing how a mosaic theory analysis considers a series of government acts together, rather than examining them in isolation).

[71] *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring); *id.* at 963–64 (Alito, J., concurring); *see also* Kerr, *supra* note 70, at 320–21 (noting that *Maynard* and *Jones* suggest that a majority of the Court is prepared to embrace the mosaic theory); Slobogin, *supra* note 65, at 7 (observing that, as of 2012, five Justices were ready to abandon the connection between physical trespass and the Fourth Amendment). Despite the recent traction that it has gained, the mosaic theory is not without its critics. *See* United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting) (rejecting the mosaic theory), *aff'd*, 132 S. Ct. 945; *see also* Kerr, *supra* note 70, at 346 (expressing concern about the mosaic theory and advocating for its rejection by courts).

[72] *See Jones*, 132 S. Ct. at 956–57 (Sotomayor, J., concurring) (suggesting that the Court reconsider the fundamental premise underlying the third-party doctrine, which is "ill suited to the digital age" and warning that awareness of government monitoring chills First Amendment freedoms); Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 58 B.U. L. REV. 685, 689 (1978) (defining the "chilling effect" as an act of deterrence that causes people to refrain from engaging in activities for fear of punishment); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 747 (2008) (arguing that relational surveillance by the government threatens not only individual privacy, but also First Amendment rights to freedom of association and assembly).

[73] *See Jones*, 132 S. Ct. at 953 (explaining that cases of non-physical electronic surveillance remain subject to analysis under *Katz*'s reasonable expectation of privacy test).

[74] *See infra* notes 78–139 and accompanying text.

scribes cell-site location information.[75] Section B examines the use of cell-site simulators, such as the Dirtbox, by law enforcement.[76] Section C explores attempts to regulate the Dirtbox by the Department of Justice and legislatures.[77]

A. Cell-Site Location Information

As the availability and sophistication of location tracking technology has surged, so has its use by law enforcement.[78] Radio-frequency enabled trackers were once a valuable tool for police officers, but satellite-based technology, such as GPS devices, has rendered radio "beepers" obsolete.[79] GPS devices remain a popular option for location tracking, but this attachment-based technology presents practical and legal obstacles.[80] Law enforcement is increasingly turning to cell phone tracking as an appealing alternative to attachment-based tracking devices.[81]

---

[75] *See infra* notes 78–94 and accompanying text.

[76] *See infra* notes 95–113 and accompanying text.

[77] *See infra* notes 114–139 and accompanying text.

[78] *See* Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. TIMES (Mar. 31, 2012), http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html?_r=0 [https://perma.cc/RR56-WQ89] (revealing that cell phone tracking has gone from a national security measure to an everyday tool for local law enforcement, with little or no judicial oversight); Jennifer Valentino-Devries, *Sealed Court Files Obscure Rise in Electronic Surveillance*, WALL STREET J. (June 2, 2014), http://www.wsj.com/articles/sealed-court-files-obscure-rise-in-electronic-surveillance-1401761770 [https://perma.cc/3AUJ-78MN] (describing how law enforcement requests in federal courts for location data and electronic tracking have increased substantially over the past decade); *see also* United States v. Jones, 132 S. Ct. 945, 963 (2012) (noting the recent development of novel location tracking technology).

[79] *See, e.g.*, People v. Weaver, 12 N.Y.3d 433, 440 (2009) (describing beepers as "very primitive tracking device[s]"); April A. Otterberg, Note, *GPS Tracking Technology: The Case for Revisiting* Knotts *and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661, 694 (2005) (noting that GPS devices are more accurate than beepers); Ramya Shah, Note, *From Beepers to GPS: Can the Fourth Amendment Keep up with Electronic Tracking Technology?*, 2009 U. ILL. J.L. TECH. & POL'Y 281, 285 (noting that beepers are smaller than GPS trackers and less sophisticated).

[80] *See* Travis Martinez, *Using GPS Tracking Devices as Alarms*, 8 COMMUNITY POLICING DISPATCH, no. 1, Jan. 2015, http://cops.usdoj.gov/html/dispatch/01-2015/using_gps_as_alarms.asp [https://perma.cc/TT6F-J3UZ] (describing how law enforcement has difficulty deploying GPS trackers on certain property without the devices being detected); Kim Zetter, *Busted! Two New Fed GPS Trackers Found on SUV*, WIRED (Nov. 8, 2011), http://www.wired.com/2011/11/gps-tracker-times-two/ [https://perma.cc/8D2X-967T] (telling the story of a California man who discovered and removed two GPS tracking devices that police officers had placed on his car); *see also Jones*, 132 S. Ct. at 949 (holding that the warrantless attachment of a GPS receiver to an automobile violates the Fourth Amendment). This Note refers to beepers and GPS receivers as "attachment-based" tracking devices to distinguish them from the more modern tracking devices that do not require physical attachment.

[81] *See* Bryan Bender, *Cellphone Firms Regularly Give Data to Law Enforcement*, BOS. GLOBE, (Dec. 9, 2013), https://www.bostonglobe.com/news/nation/2013/12/09/new-figures-show-growth-law-enforcement-requests-for-cellphone-data/9o1TZ1xz5VUBButjteO1jL/story.html [https://perma.

Law enforcement may avoid the inherent problems of attachment-based tracking by obtaining a suspect's cell-site location information ("CSLI").[82] Every cell phone automatically generates CSLI for its wireless service provider ("WSP") in its normal course of functioning.[83] Given the numerous cellular towers, or "cell sites," in a geographic area through which a call could be routed, and their varying signal strengths, cell phones continually register with the cell site emitting the strongest signal to ensure optimal connectivity.[84] WSPs maintain a record of this registration, indicating which of its many cell-sites was pinged and at what time.[85] Depending

---

cc/2Z2J-FL64] (describing how the largest wireless carriers in the United States now routinely provide state and local law enforcement with thousands of records containing customers' location information in furtherance of criminal investigations); Sarah Roberts, *Court Says No GPS Tracking? How About Cell Phone Tracking?*, AM. C.L. UNION: SPEAK FREELY (Apr. 6, 2012), https://www.aclu.org/blog/technology-and-liberty-national-security/court-says-no-gps-tracking-how-about-cell-phone [https://perma.cc/D5YB-8PFE] (describing how after warrantless GPS surveillance failed to pass constitutional muster, the government has turned to cell phone monitoring to obtain individuals' location information).

[82] M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1413 (2007) (noting that a great advantage of cell phone tracking is law enforcement's ability to circumvent legal and practical hurdles that are often associated with the physical installation of a tracking device). With 90% of American adults using cell phones, law enforcement can track the majority of the population without planting any external devices. *See Mobile Technology Fact Sheet*, PEW RESEARCH CTR. (Oct. 2014), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ [https://perma.cc/57Q6-NSUD]. Also, whereas GPS receivers are typically affixed to automobiles, cell phones remain within arm's length of users throughout the day. *See In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) (observing that many people never stray more than a few feet from their cell phone).

[83] *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 4 (2010) (statement of Matt Blaze, Professor, University of Pennsylvania) [hereinafter Blaze Testimony]; Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 705 (2011) (describing how cell phones constantly generate registration data, regardless of whether a call is in progress); Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, The ATLANTIC (Aug. 8, 2015), http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/ [http://perma.cc/8AJA-QQVW] (explaining that cell phone users create a trail of cell-site location information as they move throughout the day).

[84] *See* Blaze Testimony, *supra* note 83, at 4 (describing the process by which a call is handed off seamlessly between base stations when a cell phone is moving); Freiwald, *supra* note 83, at 705 (explaining how frequent registration enables cellular service providers to locate the optimal tower through which to transfer incoming and outgoing calls); Meyer, *supra* note 83 (noting that cell phones continually register with the closest cellular tower). Regardless of whether a user is placing a call, as long as the cell phone is turned on, cell-site registration occurs every seven seconds or whenever the signal grows weak. *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005).

[85] *See* Blaze Testimony, *supra* note 83, at 7; *see also* COMPUT. CRIME AND INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, RETENTION PERIODS OF MAJOR CELLULAR SERVICE PROVIDERS 1 (2010), https://www.aclu.org/files/pdfs/freespeech/retention_periods_of_major_cellular_service_providers.pdf [http://perma.cc/BW2L-N8PQ] (showing that most major wireless service providers retain CSLI for over a year).

on the area of coverage, or "cell sector," of a cell-site, CSLI can indicate the location of a cell phone from anywhere between a few miles to a few meters.[86]

CSLI exists in two forms: historical and real-time.[87] Historical CSLI consists of records stored by a WSP that indicate where a cell phone was located in the past.[88] Real-time CSLI, on the other hand, refers to the data that reveals the current location of a cell phone.[89] Notably, real-time CSLI may be more accurate than historical CSLI because the former can be enhanced through triangulation.[90]

---

[86] *See* Freiwald, *supra* note 83, at 711 (citing Blaze Testimony, *supra* note 83, at 25) (noting that, in small cell sectors, CSLI can reveal the location of a cell phone with great accuracy). Although early cell sectors were quite large, the increased demand for bandwidth has led to significantly smaller base stations, some designed to serve specific floors of a building or even an individual home). Blaze Testimony, *supra* note 83, at 8–9. Despite shrinking cell-sites, it is generally accepted that CSLI is less accurate than GPS. *See The Two Towers*, THE ECONOMIST (Sept. 6, 2014), http://www.economist.com/news/united-states/21615622-junk-science-putting-innocent-people-jail-two-towers (noting that juries' unquestioning reliance on historical CSLI leads to false convictions because such location information is significantly less accurate than prosecutors may claim). *But see* Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, 59 U.S. ATT'YS BULL. 16, 17 (2011) (describing historical CSLI as "reliable, accurate, and useful in criminal trials"). Accurate cell phone location information is a federal requirement. *See* 47 C.F.R. § 20.18(h)(1) (2012) (setting forth location accuracy requirements for network-based cellular devices to assure that law enforcement can find 911 emergency callers).

[87] *See* United States v. Graham, 846 F. Supp. 2d 384, 391–92 (D. Md. 2012), *aff'd*, 796 F.3d 332 (4th Cir.), *vacated*, 624 Fed. App'x 75 (4th Cir. 2015) (distinguishing between historical CSLI and real-time CSLI); State v. Perry, 776 S.E.2d 528, 534 (N.C. Ct. App. 2015), *review denied*, 781 S.E.2d 622 (N.C. 2016) (mem.) (same).

[88] *Graham*, 846 F. Supp. 2d at 391 (explaining that historical CSLI "exposes to the government only where a suspect *was* and not where he *is*"); *Perry*, 776 S.E.2d at 534 (noting that historical CSLI indicates where a cell phone was located at a certain time in the past).

[89] *See Perry*, 776 S.E.2d at 534 (explaining that real-time CSLI reveals the present location of a cell phone); *see also* Ford v. State, No. PD-1396-14, 2015 WL 8957647, at *10 (Tex. Crim. App. Dec. 16, 2015) (distinguishing real-time CSLI from historical CSLI).

[90] *See In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Phone, 460 F. Supp. 2d 448, 451 (S.D.N.Y. 2006) (explaining how the process of triangulation can render real-time cell phone location information "with a fair degree of precision"); *see also In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 137 (E.D.N.Y. 2013) (observing that the accuracy of CSLI can be significantly enhanced by triangulating a cell phone's signal to multiple towers). Because historical CSLI is comprised of location data obtained from one tower at a time, it cannot be improved through triangulation, which requires data from multiple towers. *See In re* Application of the U.S. for an Order Authorizing the Disclosure of Cell Site Location Info., No. 6:08-6038M-REW, 2009 WL 8231744, at *2 (E.D. Ky. Apr. 17, 2009) (noting that triangulation is not possible with historical CSLI, which is derived from a single cell site); Interview with Nathan Freed Wessler, Staff Attorney, Am. Civil Liberties Union (July 1, 2014), http://www.theblaze.com/stories/2014/07/01/is-your-local-police-force-using-high-tech-tracking-the-top-four-terms-you-need-to-know/ (explaining that real-time CSLI provides more precise tracking than historical CSLI because the former can be triangulated). *But see* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J.

The government typically obtains cell phone location data by requesting CSLI from a WSP, which poses legal and practical obstacles.[91] The patchwork of statutory authority upon which the government relies to obtain CSLI is ill fitted to such technology and leads to inconsistent outcomes across jurisdictions.[92] Furthermore, the government's reliance on a third party may result in delay or uncooperativeness.[93] For these reasons, law enforcement has increasingly begun to take matters into their own hands by intercepting CSLI, thus avoiding the hindrances of courts and third-party WSPs.[94]

117, 128 (2012) (noting that although it is not common practice, some cellular providers routinely record triangulated CSLI).

[91] *See Cell Phone Location Tracking Public Records Request*, AM. C.L. UNION (Mar. 25, 2013), https://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request [http://perma.cc/TQH9-RCJJ] (revealing that out of a survey of approximately 250 law enforcement agencies, only thirteen did not engage in cell phone tracking); Shira Schoenberg, *Law Enforcement Agencies Made 1.1 Million Requests for Americans' Cell Phone Records in 2012, U.S. Sen. Ed Markey Finds*, MASSLIVE (Dec. 9, 2013, 5:43 PM), http://www.masslive.com/politics/index.ssf/2013/12/law_enforcement_agencies_made.html [https://perma.cc/9C59-42NL].

[92] *See Transparency Report*, AT&T, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html [https://perma.cc/ELL9-S5ET] (offering data from 2015 on subpoenas, court orders, and search warrants sought by law enforcement to obtain customers' cell phone location information); *e.g.*, *In re* Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. (Sealed), 402 F. Supp. 2d 597, 600 (D. Md. 2005) ("[T]he government contends that the [Stored Communications Act] authorizes disclosure of historical cell site information and, when combined with the Pen/Trap Statute, also authorizes disclosure of real time cell site information."). *Compare* United States v. Davis, 785 F.3d 498, 511 (11th Cir.), *cert. denied*, 136 S. Ct. 479 (2015) (mem.) (holding that the government may obtain historical CSLI pursuant to the Stored Communications Act), *with In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 574–75 (D. Md. 2011) (holding that the government may not obtain historical CSLI pursuant to the Stored Communications Act).

[93] *See Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Statement Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary* (2011) (statement of Valerie Caproni, Gen. Counsel, Federal Bureau of Investigation), https://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies [https://perma.cc/9MCY-9QXX] [hereinafter *Going Dark*] (describing the increasingly common situation of cell phone providers failing to comply with court orders); *see also* David Kravets, *Cell-Tracking Bills Require Info Dump for Missing Persons*, WIRED (Oct. 22, 2009), http://www.wired.com/2009/10/cell-tracking-bills/ [https://perma.cc/C3EU-43YU] (detailing the story of Kelsey Smith, a teenage girl who was kidnapped and killed during the days it took law enforcement to obtain her CSLI from Verizon). Apple's recent refusal to provide the DOJ with backdoor access to its iPhone has ignited national debate regarding uncooperative intermediaries, highlighting the challenges of third-party reliance. *See* Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0 [https://perma.cc/34GQ-FS2R] (describing the legal dispute and national policy debate that erupted after Apple refused to circumvent iPhone safeguards and provide the DOJ with access to the cell phone belonging to the San Bernardino shooter).

[94] *See generally* John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (June 13, 2014), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-

B. Stingrays and Dirtboxes: Cutting out the Middle Man with Cell-Site Simulators

Federal, state, and local law enforcement use devices called Stingrays to intercept cell phone location information.[95] The Stingray, part of a broader class of international mobile subscriber identity ("IMSI") catchers, mimics a cellular tower and compels all cell phones within range to transmit their location data to the device.[96] With this data, law enforcement can use triangulation to calculate an individual's precise location.[97] Although typically used to target the location of a single cell phone, Stingrays intercept data from every cell phone within range.[98] Originally developed for counter-terrorism, these devices are now routinely used by local law enforcement.[99] Despite the widespread use of Stingrays, the federal government has resorted to extreme measures to keep them classified.[100]

---

nsa-police/3902809/ [https://perma.cc/2JH2-B22M] (noting that law enforcement is increasingly relying on new technology to intercept cell phone location information).

[95] *See* Joseph Goldstein, *New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says*, N.Y. TIMES (Feb. 11, 2016), http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html?_r=0 [http://perma.cc/LRH5-BUMB] (revealing that the New York Police Department has been using Stingrays "as frequently as 200 times a year" since 2008); 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 [http://perma.cc/9RRW-RLSC] ("Law enforcement officials across the United States have become enamored of the StingRay . . . ."); *Stingray Tracking Devices: Who's Got Them?*, AM. C.L. UNION, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them [https://perma.cc/TCN4-KKRE] (tracking Stingray use by federal, state, and local law enforcement across the country). Harris Corporation, the designer and manufacturer of the Stingray, produces variations on this device, which include the Stingray II, AmberJack, KingFish, TriggerFish, and LoggerHead. Jennifer Valentino-Devries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL STREET J. (Sept. 22, 2011), http://www.wsj.com/articles/SB10001424053111904194604576583112723197574 [https://perma.cc/JP5P-AGE3].

[96] *See* Goldstein, *supra* note 95 (describing Stingrays as portable devices that intercept the location information of cell phones by imitating cellular towers); Williams, *supra* note 95 (explaining how Stingrays mimic cellular towers).

[97] *See* Joel Hruska, *Stingray, the Fake Cell Phone Tower Cops and Carriers Use to Track Your Every Move*, EXTREMETECH (June 17, 2014), http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move [https://perma.cc/7G9Y-7QSV] (explaining how law enforcement typically operate this device from within a vehicle, allowing them to discretely obtain cell phone signals from several locations and then triangulate those signals to hone in on a suspect's precise location); Jennifer Valentino-Devries, *How 'Stingray' Devices Work*, WALL STREET J.: DIGITS (Sept. 21, 2011, 10:33 PM), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/ [https://perma.cc/GC3D-JDSM] (describing how Stingrays can measure cell phone signals and then triangulate them to obtain more precise location information).

[98] Goldstein, *supra* note 95 (explaining that although Stingrays are used to locate specific individuals, the devices also gather data from other cell phones within range); *see Stingray Tracking Devices: Who's Got Them?*, *supra* note 95 (noting that Stingrays gather cell phone location information from bystanders).

[99] *See* Kelly, *supra* note 94 (noting that "[a]t least 25 police departments own a Stingray" and that "[t]he federal government funds most of the purchases, via anti-terror grants"). Since obtain-

In November 2014, a news report revealed that the DOJ uses airplane-mounted IMSI catchers that are far more sophisticated than the Stingray.[101] Named after its manufacturer, Digital Receiver Technology Inc., the DRTbox (or "Dirtbox") also dupes cell phones into transmitting their location information to the device by posing as a cellular tower.[102] In a surveillance program operated by the U.S. Marshals Service since 2007, Dirtboxes are affixed to the underside of small-sized Cessna aircraft, which regularly fly over an area covering most of the population of the United States in search of criminal suspects.[103] The two-foot-square box is humble in size relative to the cellular towers it mimics, but it is extremely powerful—in a single flight, the Dirtbox intercepts data from tens of thousands of cell

---

ing regulatory approval, the Stingray has deviated from its intended and approved usage. *See* Nathan Freed Wessler & Nicole Ozer, *Documents Suggest Maker of Controversial Surveillance Tool Misled the FCC*, AM. C.L. UNION: FREE FUTURE (Sept. 17, 2014 10:15AM), https://www.aclu.org/blog/documents-suggest-maker-controversial-surveillance-tool-misled-fcc [https://perma.cc/NHF4-6KAP]; *see also* Email from Tania Hanna, Harris Corp. Emp/, to Bruce Romano (June 24, 2010), https://s3.amazonaws.com/s3.documentcloud.org/documents/1303034/fcc-foia-harris-emails.pdf [https://perma.cc/828Y-Z94T] (describing the Stingray as a piece of equipment intended for emergency use).

[100] *See* Nathan Freed Wessler, *U.S. Marshals Seize Local Cops' Cell Phone Tracking Files in Extraordinary Attempt to Keep Information from Public*, AM. C.L. UNION: FREE FUTURE (June 3, 2014), https://www.aclu.org/blog/us-marshals-seize-local-cops-cell-phone-tracking-files-extraordinary-attempt-keep-information [http://perma.cc/LHW9-9EXK] (recounting that as the American Civil Liberties Union ("ACLU") prepared to review Stingray-related Freedom of Information Act documents at a local Florida police station, U.S. Marshals arrived and seized all of the documents); *see also* Thomas v. State, 127 So. 3d 658, 660 (Fla. Dist. Ct. App. 2013) (describing how police officers declined to seek a warrant to avoid revealing information about the device they deployed to track the cell phone's location); Shawn Musgrave, *Before They Could Track Cell Phone Data, Police Had to Sign a NDA with the FBI*, MUCKROCK (Sept. 22, 2014), https://www.muckrock.com/news/archives/2014/sep/22/they-could-track-cell-phone-data-police-had-sign-n/ [https://perma.cc/8RYY-RA8Y] (revealing that the FBI requires state and local law enforcement to sign a nondisclosure agreement before acquiring a Stingray).

[101] Barrett, *supra* note 2 (describing the Dirtbox surveillance program as "more sophisticated than anything previously understood about government use of such technology"); Gail Sullivan, *Report: Secret Government Program Uses Aircraft for Mass Cellphone Surveillance*, WASH. POST (Nov. 14, 2014), https://www.washingtonpost.com/news/morning-mix/wp/2014/11/14/report-secret-government-program-uses-aircraft-for-mass-cellphone-surveillance/ [https://perma.cc/2PJH-3MEB] (describing the Dirtbox program). The devices are now being used by other federal agencies, as well as state and local law enforcement. *See* Ferner, *supra* note 1 (noting that the police in Anaheim are using surveillance equipment thought to have only been used by the federal government and in larger cities).

[102] Barrett, *supra* note 2 (describing how the Dirtbox mimics cellular towers, causing cell phones to connect to it and transfer their registration information). The Dirtbox acquires this IMSI directly, obviating the need for tower-based CSLI. *See id.*

[103] *Id.* (explaining that, for cost reasons, a single flight typically targets multiple suspects); *see* Memorandum, Dep't of Justice, Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology 3 (Sept. 3, 2015), http://www.justice.gov/opa/file/767321/download [http://perma.cc/C52N-EHNJ] [hereinafter DOJ Cell-Site Policy Memo] (providing guidelines for "use of a cell-site simulator on an aircraft").

phones.[104] After compelling a cell phone to register with the Dirtbox at multiple points in the sky, the Marshals can use trilateration to determine the location of an individual within ten feet.[105]

Because it directly intercepts location data, in real-time, and combines dragnet capabilities with high-accuracy triangulation, this high-flying imposter delivers unique benefits to law enforcement.[106] By mounting the Dirtbox on an aircraft, the government can quickly and discretely comb through thousands of phone numbers in search of persons of interest in an urban or suburban area.[107] Dirtbox surveillance has many potential uses, from foiling criminal acts to assisting search-and-rescue missions in remote locations.[108] Despite these benefits, the Dirtbox poses significant privacy concerns.[109]

---

[104] Barrett, *supra* note 2. According to people with knowledge of the surveillance program, the Dirtbox determines which cell phone registration information belongs to criminal suspects, then discards the rest. *Id.*

[105] *See id.* Because it uses trilateration, the Dirtbox obtains more accurate location information than single tower historical CSLI. *See In re* Application of the U.S. for an Order Authorizing the Disclosure of Cell Site Location Info., No. 6:08-6038M-REW, 2009 WL 8231744, at *2 (E.D. Ky. Apr. 17, 2009) (explaining that historical CSLI cannot provide precise location information through triangulation because it relies on single-site activation).

[106] *See* Barrett, *supra* note 2 (describing the effectiveness of Dirtbox technology in apprehending criminal suspects); DOJ Cell-Site Policy Memo, *supra* note 103, at 1 (noting that cell-site simulators further public safety objectives, "[w]hether deployed as part of a fugitive apprehension effort, a complex narcotics investigation, or to locate or rescue a kidnapped child"); *see also* Devlin Barrett, *CIA Aided Justice Department Secret Program to Spy on U.S. Cellphones*, WALL STREET J. (Mar. 10, 2015), http://www.wsj.com/articles/cia-gave-justice-department-secret-phone-scanning-technology-1426009924 [http://perma.cc/A8F4-JAUZ] (explaining how Dirtbox technology is used to locate criminal suspects in the United States and terror suspects abroad).

[107] *See* Jessica Trufant & Patrick Ronan, *Quincy Finally Gets Some Answers About Mysterious Plane*, PATRIOT LEDGER (June 1, 2014), http://www.patriotledger.com/article/20140601/News/140609702 [http://perma.cc/ENX8-4ZBL] (reporting that the government circled Dirtbox-equipped Cessnas over Quincy, Massachusetts, in the wake of the 2013 Boston Marathon bombing to investigate a man with suspected ties to the bombing); *see also* Barrett, *supra* note 2.

[108] *See* Barrett, *supra* note 2 (noting that this airborne surveillance device "has been effective in catching suspected drug dealers and killers"); Michael Isikoff, *FBI Tracks Suspects' Cell Phones Without a Warrant*, NEWSWEEK (Feb. 18, 2010), http://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099 (describing how federal agents used real-time CSLI to track a Mexican drug cartel transporting 2200 kilograms of cocaine); *see also* Lichtblau, *supra* note 78 (describing how police in Michigan used real-time CSLI to find a stabbing victim who was in a basement hiding from his attacker); Kravets, *supra* note 93 (detailing the story of Kelsey Smith, a teenage girl who was kidnapped and killed during the days it took law enforcement to obtain her CSLI from Verizon); Valentino-Devries, *supra* note 97 (describing how IMSI catchers are used to locate criminal suspects and help search-and-rescue teams find missing people).

[109] *See* Matt Cagle, *Dirtbox Over Disneyland? New Docs Reveal Anaheim's Cellular Surveillance Arsenal*, AM. C.L. UNION OF NORTHERN CAL. (Jan. 27, 2016), https://www.aclunc.org/blog/dirtbox-over-disneyland-new-docs-reveal-anaheim-s-cellular-surveillance-arsenal [https://perma.cc/W3KS-DQMH] (discussing how Dirtbox surveillance in Anaheim, California may affect the privacy of millions of residents and visitors); *see also* Barrett, *supra* note 2 (quoting Christopher Soghoian, Chief Technologist at the ACLU, as stating: "Maybe it's worth violating privacy

The November 2014 revelation of the U.S. Marshals' Dirtbox program triggered public outcry and calls for transparency.[110] Civil liberties groups decried the wide-sweeping surveillance as overzealous, questioning its constitutionality and demanding government disclosures.[111] Troubled by the privacy concerns posed by the Dirtbox and the DOJ's silence, various members of Congress insisted that the Department disclose specific details regarding this location tracking technology.[112] Months after the congressional demands, and despite DOJ briefings on location tracking technology, the House Committee on Oversight and Government Reform pressed the DOJ to produce department-wide policies concerning cell-site simulation technology.[113]

C. Attempts to Rein in the Dirtbox

On September 3, 2015, the DOJ issued a policy memorandum establishing guidance for the Department's use of the Dirtbox and other cell-site

---

of hundreds of people to catch a suspect, but is it worth thousands or tens of thousands or hundreds of thousands of peoples' privacy?").

[110] Trevor Timm, *First Snowden. Then Tracking You on Wheels. Now Spies on a Plane. Yes, Surveillance Is Everywhere*, The GUARDIAN (Nov. 15, 2014), http://www.theguardian.com/commentisfree/2014/nov/15/spies-plane-surveillance-us-marshals [https://perma.cc/5UUT-UJ7A] (expressing shock at congressional silence on "blatant domestic spying abuse," which entails "spies on a plane, snooping exclusively on Americans, on a massive scale"); *see* Owsley, *supra* note 7, at 81–82 (arguing that Dirtbox surveillance amounts to a Fourth Amendment search and therefore requires a warrant supported by probable cause).

[111] *See* Bennett Stein, *ACLU Seeks Information About Airborne Cell Phone Snooping*, AM. C.L. UNION: FREE FUTURE (Nov. 19, 2014, 7:59 AM), https://www.aclu.org/blog/free-future/aclu-seeks-information-about-airborne-cell-phone-snooping [http://perma.cc/SJ7M-V7VU] (noting increasing public resistance towards the government's use of cell-site simulators); *see also* Complaint for Injunctive Relief at 1–2, Elec. Frontier Found. v. Dep't of Justice, No. 1:15-cv-00200 (D.D.C. Feb. 10, 2015) (seeking expedited records from executive agencies concerning Dirtbox data collection); Letter from Nathan Freed Wessler, Staff Attorney, Am. Civil Liberties Union, to Dep't of Justice (Nov. 19, 2014), https://www.aclu.org/sites/default/files/field_document/baltimore_surveillance_flight_foia_request.pdf [https://perma.cc/67XS-STLD] (requesting information regarding the government's use of cell-site simulators).

[112] *See* Letter from Jon Tester, U.S. Senator of Mont. et al. to Eric H. Holder, Jr., Attorney Gen., U.S. Dep't of Justice, & Jeh Johnson, Sec'y of Homeland Sec., Dep't of Homeland Sec. (Dec. 9, 2014), https://www.documentcloud.org/documents/1378358-249798493-tester-s-letter-to-attorney-general.html [https://perma.cc/7FTC-QQT7] (asking that the DOJ provide responses to questions regarding the Dirtbox surveillance program); Letter from Edward J. Markey, U.S. Senator of Mass., to Eric H. Holder, Jr., Attorney Gen., U.S. Dep't of Justice (Nov. 14, 2014), http://www.markey.senate.gov/imo/media/doc/2014-11-14_DOJ_Surveillance.pdf [https://perma.cc/QE3P-94YS] (same); *see also* Barrett, *supra* note 2 (stating that an official from the Department of Justice would not confirm or deny the existence of the Dirtbox program).

[113] *See* Letter from Jason Chaffetz, Chairman, House Comm. on Oversight & Gov't Reform et al. to Eric H. Holder, Attorney Gen., U.S. Dep't of Justice (Apr. 24, 2015), https://oversight.house.gov/wp-content/uploads/2015/10/2015-04-24-JEC-EEC-WH-RK-to-Holder-DOJ-stingrays-due-5-8.pdf [http://perma.cc/J5DH-9M3Q].

simulators (the "DOJ memo").[114] The DOJ memo sets forth background information regarding cell-site simulators and outlines procedures for internal controls and accountability.[115] More importantly, the DOJ memo establishes legal protocols for the use of this technology and the subsequent management of data collected.[116] Foremost among these protocols is a rule that agents obtain a search warrant prior to deploying a cell-site simulator.[117]

Under this new policy, a warrant is not required in circumstances that are "exigent" or "exceptional."[118] Exigent circumstances exist where the needs of law enforcement are so compelling that the search would be objectively reasonable, even without a warrant.[119] Under such circumstances, an agent is still required to obtain judicial authorization under the pen register statute, as well as internal approval.[120] Exceptional circumstances permit law enforcement to conduct cell-site interception where it is impracticable

---

[114] DOJ Cell-Site Policy Memo, *supra* note 103; *see* Tal Kopan & Josh Gaynor, *DOJ Cracks Down on Use of Cell-Duping Stingrays*, CNN POLITICS (Sept. 3, 2015, 6:13 PM), http://www.cnn.com/2015/09/03/politics/stingrays-cell-site-simulator-justice-department-rules/ [http://perma.cc/5WC7-RJMN] (describing the DOJ's new guidelines on cell-site simulators); Ellen Nakashima, *Justice Department: Agencies Need Warrants to Use Cellphone Trackers*, WASH. POST (Sept. 3, 2015), https://www.washingtonpost.com/world/national-security/justice-department-agencies-will-have-to-obtain-warrant-before-using-cellphone-surveillance-technology/2015/09/03/08e44b70-5255-11e5-933e-7d06c647a395_story.html [http://perma.cc/AW4Y-YP5K] (predicting that the guidelines announced by Deputy Attorney General Sally Quillian Yates will increase transparency); *ACLU Comment on New Justice Department Guidelines for Secretive Stingray Surveillance Devices*, AM. C.L. UNION (Sept. 3, 2015), https://www.aclu.org/news/aclu-comment-new-justice-department-guidelines-secretive-stingray-surveillance-devices [https://perma.cc/NS45-KBG5] [hereinafter *ACLU Comment*] (characterizing the guidelines as "a positive first step" but advocating that the DOJ close certain loopholes in the policy and extend its applicability to other federal agencies, as well as state and local law enforcement).

[115] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 2 (describing the basic uses and limitations of cell-site simulators, and requiring that the technology be used only by "knowledgeable and accountable personnel").

[116] *See id.* at 3–6 (requiring that all data obtained during Dirtbox location tracking be deleted as soon as the target cellphone is located, and at least once per day).

[117] *See id.* at 3 ("[A]s a matter of policy, law enforcement agencies must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure . . . ."). The DOJ memo also requires that the use of a cell-site simulator have judicial approval under the pen register statute. *See id.*; *see also* 18 U.S.C. § 3123 (2012) (requiring that the government certify that the information it seeks is relevant to an ongoing criminal investigation). For all court applications, the DOJ memo requires agents to describe the purpose of the interception and the nature of the technology. *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 5.

[118] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 3–4 (setting forth two exceptions to the DOJ's warrant requirement for the use of cell-site simulators).

[119] *Id.* at 3 (setting forth examples of exigent circumstances, including the need to protect against serious harm to human life, prevent the imminent destruction of evidence, pursue a fleeing criminal, and prevent the escape of a fugitive suspect or convict).

[120] *Id.* at 4; *see* 18 U.S.C. § 3123 (providing for judicial authorization of a pen register or trap and trace device upon certification by the government that the information likely to be obtained is relevant to an ongoing criminal investigation).

to obtain a search warrant.[121] Agents in these situations must nevertheless obtain three levels of internal Department authorization.[122]

These guidelines, although robust, are limited in applicability and enforceability.[123] First, the warrant exceptions cut deeply into the rule.[124] Second, the policy applies only to agents of the DOJ.[125] Finally, the memo sets forth nothing more than policy guidance—it creates no rights or binding obligations.[126]

Reactions to the DOJ policy memo were generally positive, but questions remained about the carve-outs and limited applicability of the guidelines.[127] On November 2, 2015, House Representative Jason Chaffetz introduced a bill to expand and codify the DOJ memo.[128] Under the proposed

---

[121] DOJ Cell-Site Policy Memo, *supra* note 103, at 4 (restricting the use of the exceptional circumstances exception to situations in which "the law does not require a search warrant" and noting that these circumstances are expected to be "very limited").

[122] *See id.* (requiring agents excused from the warrant rule under exceptional circumstances to obtain approval for deployment of a cell-site simulator from executive-level personnel at the DOJ headquarters, a U.S. Attorney, and a Criminal Division Deputy Assistant Attorney General).

[123] *See id.* at 2 n.2, 6.

[124] *See* Carrie Johnson, *New Cellphone Surveillance Safeguards Imposed on Federal Law Enforcement*, NPR (Sept. 4, 2015, 11:50 AM), http://www.npr.org/sections/itsallpolitics/2015/09/03/437311545/new-cell-phone-surveillance-safeguards-imposed-on-federal-law-enforcement [https://perma.cc/X83F-SC7H] (expressing concern that the guidelines leave open a loophole for the warrantless use of cell-site simulators in an undefined category of "exceptional circumstances"); DOJ Cell-Site Policy Memo, *supra* note 103, at 3–4.

[125] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 6 ("This policy applies to all instances in which Department components use cell-site simulators in support of other Federal agencies and/or State and Local law enforcement agencies."); *see also* Johnson, *supra* note 124 (noting the limited applicability of the guidelines). Shortly after the DOJ issued this policy memo, the Department of Homeland Security issued one of its own. *See* Memorandum from Alejandro N. Mayorkas, Deputy Sec., Dep't of Homeland Sec. to Various DHS Components (Oct. 19, 2015), http://www.justice.gov/opa/file/767321/download [http://perma.cc/W2YB-9YKU] (setting forth policy directives nearly identical to those in the DOJ memo).

[126] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 2 n.2 (stipulating that the policy serves internal management purposes only and "is not intended to and *does not create any right*, benefit, trust, or responsibility, whether substantive or procedural, *enforceable at law or equity*" and does not "create any right of review in an administrative, judicial, or any other proceeding" (emphasis added)).

[127] *See* Johnson, *supra* note 124 (quoting Senator Patrick Leahy, D-VT, as stating: "Today's announcement is a welcome step forward . . . . However, I have serious questions about the exceptions to the warrant requirement that are set forth in this new policy, and I will press the Department to justify them."); *ACLU Comment*, *supra* note 114 (noting that the policy provides desirable protections but that it should go further); DOJ Cell-Site Policy Memo, *supra* note 103.

[128] Cell-Site Simulator Act of 2015, H.R. 3871, 114th Cong. (2015) (proposing regulations on the use of cell-site simulators by federal agencies, as well as state and local law enforcement); *see Chaffetz Introduces Legislation to Address Government Use of Cell Site Simulators*, U.S. CONGRESSMAN JASON CHAFFETZ (Nov. 2, 2015), https://chaffetz.house.gov/press-release/chaffetz-introduces-legislation-address-government-use-cell-site-simulators [https://perma.cc/39WN-9P9N] (announcing Rep. Chaffetz' introduction of the legislation in response to the abuse of cell-site simulators by law enforcement agencies, and asserting that the bill "codifies recent guidance from the Department of Justice"); *see also* Kim Zetter, *New Bill Would Make Local and State Law*

legislation, no government official may use a cell-site simulator without a warrant.[129] The bill would provide warrant exceptions that largely trace those in the DOJ memo, but with additional safeguards.[130] Despite the increased protections offered by the bill, it is unlikely to be enacted.[131]

States have begun to pass their own legislation to address the use of cell-site simulators.[132] In 2013, Montana passed a law requiring the government to obtain a warrant prior to using a cell-site simulator.[133] Tennessee, Utah, Indiana, and Minnesota passed similar laws and set forth a range of warrant exceptions.[134] More recently, California enacted what was hailed

---

Enforcers Get a Warrant to Use Stingrays, SLATE: FUTURE TENSE (Nov. 6, 2015, 4:55 PM), http://www.slate.com/blogs/future_tense/2015/11/06/stingray_surveillance_technology_new_bill_would_force_local_state_law_enforcement.html [http://perma.cc/XT7H-HB8B] (noting that the Act was introduced to close the loophole in the DOJ policy memo that limits the warrant requirement to agents of the DOJ).

[129] H.R. 3871 (setting forth a general prohibition on the use of cell-site simulators, but noting that such prohibition does not apply to "[u]se of a cell-site simulator by a governmental entity under a warrant issued under the procedures described in the Federal Rules of Criminal Procedure"). Any evidence obtained in violation of the Cell-Site Simulator Act would be inadmissible. *Id.*

[130] *See id.* (waiving the warrant requirement for surveillance (1) under the Foreign Intelligence Surveillance Act, (2) under emergency circumstances, or (3) when a warrant cannot be obtained). The emergency circumstances are limited to physical danger, a threat to national security, or organized criminal conspiracy. *Id.* Furthermore, under the emergency circumstances exception, the use of a cell-site simulator would only be permitted if there were grounds upon which a warrant could be issued and if the government official applied for a warrant within forty-eight hours of commencing surveillance. *Id.*

[131] *See H.R. 3871: Stingray Privacy Act of 2015*, GOVTRACK.US, https://www.govtrack.us/congress/bills/114/hr3871 [http://perma.cc/K44W-D4GS] (predicting a 5% chance that the bill becomes enacted).

[132] Williams, *supra* note 95 (describing how states are pushing back against the use of cell-site simulators by law enforcement); *Nationwide Effort Aims to Empower Americans to "Take Control" of Their Privacy*, AM. C.L. UNION (Jan. 20, 2016), https://www.aclu.org/news/16-states-dc-introduce-legislation-limit-surveillance-and-protect-student-and-employee-privacy [http://perma.cc/85YU-LKYF] (describing the announcement of state legislation on location tracking by a coalition of legislators and advocacy groups).

[133] MONT. CODE ANN. § 46-5-110(1)(a) (2015) (providing that "a government entity may not obtain the location information of an electronic device without a search warrant issued by a duly authorized court"). The Montana statute provides an exception to the warrant requirement in situations involving stolen devices, an emergency, or informed consent. *Id.*

[134] *See* IND. CODE ANN. § 35-33-5-12(a) (2015) (prohibiting law enforcement from using real-time cellular tracking devices without first obtaining "an order issued by a court based upon a finding of probable cause," unless exigent circumstances exist); MINN. STAT. § 626A.42, subd. 2(a) (2014) (providing that "a government entity may not obtain the location information of an electronic device without a tracking warrant," except in situations of lost or stolen devices, emergency, or informed consent); TENN. CODE ANN. § 39-13-610(b) (2014) (providing that "no governmental entity shall obtain the location information of an electronic device without a search warrant issued by a duly authorized court," except in circumstances of a stolen device, an emergency, affirmative consent, a user posting his location on social media, or exigency); UTAH CODE ANN. § 77-23c-102(1)(a), (2)(a) (West 2014) (providing that "a government entity may not obtain the location information . . . of an electronic device without a search warrant issued by a court

as comprehensive privacy legislation, but which allows law enforcement to use cell-site simulators pursuant to a wiretap order.[135]

With no clear limits yet from Congress on Dirtbox or Stingray technology and without guidance from the U.S. Supreme Court as to whether CSLI acquisition amounts to a Fourth Amendment search, lower courts are split.[136] Courts have generally held that the government may acquire historical CSLI from a wireless service provider without a warrant because such information constitutes a business record and falls within the third-party doctrine.[137] In contrast, courts have been more troubled by the government obtaining real-time CSLI and have held such acquisition to amount to a

---

upon probable cause," except in situations involving an emergency, locating a stolen device, informed consent, judicially recognized warrant exceptions, or voluntary public disclosure).

[135] *See* CAL. PENAL CODE § 1546.1(c)(1)–(2) (West 2016) (providing that "[a] government entity may access electronic device information by means of . . . electronic communication with the device" pursuant to a warrant or wiretap order); *see also SB 178 Fact Sheet*, AM. C.L. UNION OF NORTHERN CAL., https://www.aclunc.org/sites/default/files/SB%20178%20CalECPA%20Fact%20Sheet_1.pdf [https://perma.cc/63HR-H5T9] (noting that "[l]aw enforcement is increasingly taking advantage of outdated privacy laws to turn mobile phones into tracking devices" and that, in response, "SB 178 heeds the call in *Jones* for the legislature to balance privacy and public safety"); Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), http://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/ [https://perma.cc/85YU-LKYF] ("The law places California not only at the forefront of protecting digital privacy among states, it outpaces even the federal government, where such efforts have stalled."). The warrant-or-court-order requirement does not apply in circumstances involving consent, an emergency, or loss of the device. *See* CAL. PENAL CODE § 1546.1(c)(3)–(6).

[136] *See* Tim Cushing, *Supreme Court Turns Down Opportunity to Straighten out Cell Site Location Information Mess*, TECHDIRT (Nov. 13, 2015, 12:48 PM), https://www.techdirt.com/articles/20151113/06185532808/supreme-court-turns-down-opportunity-to-straighten-out-cell-site-location-information-mess.shtml [https://perma.cc/LL24-XWFL] (providing a map to show the jurisdictional jigsaw that persists following the U.S. Supreme Court's 2015 decision to deny certiorari in *United States v. Davis*, an Eleventh Circuit Court of Appeals case concerning government acquisition of historical CSLI); *see also* Meyer, *supra* note 83 (noting the circuit split on the warrantless acquisition of CSLI); Abigail Tracy, *While the Supreme Court Hesitates on Warrantless Cell Location Data Collection, Your Privacy Remains at Risk*, FORBES (Oct. 16, 2015, 9:00 AM), http://www.forbes.com/sites/abigailtracy/2015/10/16/while-the-supreme-court-hesitates-on-warrantless-cell-location-data-collection-your-privacy-remains-at-risk/#109274993056 [http://perma.cc/586M-L9JB] (quoting David Markus, attorney for the defendant in *Davis*, as snoting that "[j]udges, police officers and lawyers are all in limbo"). *Compare Davis*, 785 F.3d at 531 (holding that the defendant had no reasonable expectation of privacy in his cell phone location records held by his cellular provider, which were subject to the third-party doctrine), *with* Commonwealth v. Augustine, 4 N.E.3d 846, 864 (Mass. 2014) (holding that the Massachusetts Constitution requires the government to obtain a warrant prior to obtaining historical CSLI).

[137] *See, e.g.*, *Davis*, 785 F.3d at 531 (holding that government acquisition of historical CSLI does not amount to a Fourth Amendment search and does not require a warrant); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013) (same); *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 313 (3d Cir. 2010) (same); United States v. Suarez-Blanca, No. CR 1:07 CR0023MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) (same); *Perry*, 776 S.E.2d at 536. *But see Augustine*, 4 N.E.3d at 867 (holding that the Massachusetts Constitution requires that law enforcement obtain a warrant prior to obtaining an individual's historical CSLI).

Fourth Amendment search.[138] In the limited number of cases involving Stingray or similar technology, the courts have not been tasked with Fourth Amendment analysis because the government has conceded that such interception amounts to a search.[139]

III. DIRTBOX LOCATION TRACKING IS A FOURTH AMENDMENT SEARCH

This Part argues that Dirtbox location monitoring implicates the Fourth Amendment and therefore the government must be required to get a warrant before using this technology.[140] Section A contends that Dirtbox surveillance violates its targets' reasonable expectation of privacy and, therefore, amounts to a Fourth Amendment search.[141] Section B asserts that although the policy guidance promulgated by the DOJ is a step in the right direction, Congress needs to pass legislation to ensure that individuals maintain an enforceable right to locational privacy.[142]

A. The Dirtbox Conducts Fourth Amendment Searches

Though often invoked to shield government surveillance from the Fourth Amendment's warrant requirement, the third-party doctrine does not apply to Dirtbox surveillance.[143] First, Dirtbox surveillance is accomplished through government interception, rather than cooperation of a third party.[144] The U.S. Supreme Court has never extended the third-party doctrine to government interception of information that was merely intended for a third

---

[138] *See, e.g.*, *In re* Application of U.S. for an Order Authorizing Disclosure of Location, 849 F. Supp. 2d at 541–42 (holding that the acquisition of real-time CSLI amounts to a Fourth Amendment search and requires a warrant); Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) (same); State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (same, but under the New Jersey Constitution).

[139] *See, e.g.*, State v. Tate, 849 N.W. 2d 798, 805 (Wis. 2014), *cert. denied*, 135 S. Ct. 1166 (2015) (mem.) (noting that the State had conceded that the acquisition of cell-site location information was a search under the Fourth Amendment); United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013) (noting the government's stipulation that operation of the Stingray amounted to a Fourth Amendment search and seizure).

[140] *See infra* notes 143–186 and accompanying text.

[141] *See infra* notes 143–165 and accompanying text.

[142] *See infra* notes 166–186 and accompanying text.

[143] *See* Katz v. United States, 389 U.S. 347, 351 (1967) (noting that the Fourth Amendment does not protect information that one knowingly shares with the public); *see also* Smith v. Maryland, 442 U.S. 735, 743 (1979) (holding that Fourth Amendment protection does not extend to numbers dialed on a telephone); United States v. Miller, 425 U.S. 435, 442 (1976) (holding that government acquisition of an individual's bank records does not constitute a search).

[144] *See* Barrett, *supra* note 2 (describing how Dirtbox surveillance circumvents cellular providers as intermediaries, allowing the government to take information directly instead of requesting it from a third party).

party—every case has involved a cooperative intermediary.[145] With no third party involved, the third-party doctrine is simply inapplicable.[146]

Second, even if the third-party doctrine were applicable, a cell phone user's disclosure of location data is not voluntary in the sense contemplated by the third-party doctrine cases.[147] To forgo cell phone use is to remove oneself completely from modern society.[148] Furthermore, location information is more private than the typical transactional records covered by the third-party doctrine.[149] Lower courts have signaled that real-time location data is not a typical business record and that its acquisition amounts to a

---

[145] *See Miller*, 425 U.S. at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed *by that person* to the Government." (emphasis added)). *Compare* California v. Greenwood, 486 U.S. 35, 37 (1988) (applying the third-party doctrine where police officers obtained defendants' garbage bags from the trash collector), *with* State v. Galloway, 109 P.3d 383, 388 (Or. Ct. App. 2005) (declining to apply the third-party doctrine where police searched through garbage before it could be gathered by the trash collector).

[146] *See Miller*, 425 U.S. at 443 (explaining that the Fourth Amendment allows the government to obtain information conveyed to it by third parties); Brief of Am. Civil Liberties Union et al. as Amici Curiae Supporting Appellees at 5, Maryland v. Andrews, No. 1496, 2015 WL 9907162, at *5 (Md. Ct. Spec. App. Dec. 23, 2015) [hereinafter Brief for the Appellees] (contrasting *Smith*, where dialed phone numbers where transmitted through the phone company's network, with the Baltimore Police Department's direct interaction with the defendant's cell phone); *see also* Riley v. California, 134 S. Ct. 2473, 2492 (2014) (citing *Smith*, 442 U.S. at 745–46) (differentiating between the government's data collection in *Smith*, which was conducted on the premises of the telephone company, and police officers' direct interaction with the defendant's cell phone in *Riley*). Ensuring that the third-party doctrine apply only to situations involving a third party will afford greater protection to individual privacy, as third-party cooperation provides a check on largely unfettered government interception. *See Going Dark*, *supra* note 93 (describing how cellular providers often delay their response to or entirely refuse to comply with court orders).

[147] *See* State v. Earls, 70 A.3d 630, 641 (N.J. 2013) (noting that cell phone users do not actually provide their location information to cell phone companies voluntarily because it can only be avoided by eschewing cell phone use entirely); *see also Smith*, 442 U.S. at 750 (Marshall, J., dissenting) ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."); *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) ("For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account.").

[148] *See* Andrea Caumont, *Americans Increasingly View the Internet, Cellphones as Essential*, PEW RESEARCH CTR. (Feb. 27, 2014), http://www.pewresearch.org/fact-tank/2014/02/27/americans-increasingly-view-the-internet-cellphones-as-essential/ [https://perma.cc/2KV8-Z3F2] (showing that 49% of American cell phone owners would have a hard time giving them up); *see also Riley*, 134 S. Ct. at 2484 (describing cell phones as "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy").

[149] *See* U.S. DEP'T OF JUSTICE, LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE: CELLULAR, SATELLITE & VOIP PHONE PROVIDERS 6 (2010), https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_irvine4_irvineca.pdf [http://perma.cc/7HQH-TEY6] (outlining a hierarchy of protected information under the Fourth Amendment, where transactional records are the least protected, telephone conversations the most, and location information directly in the middle).

search.[150] IMSI catchers, like the Stingray and Dirtbox, acquire triangulated location information, which is even more accurate than real-time CSLI.[151] Indeed, in the few cases in which the government has been forthright about using the Stingray, the government has conceded that the interception of location information amounts to a search.[152] The Dirtbox, which functions as a high-powered Stingray, intercepts location data that is accurate within ten feet.[153] Such accuracy allows the government to view the dreaded "mosaic" of one's life, from the most mundane to the most personal of activities.[154]

---

[150] *See, e.g.*, *In re* Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. (Sealed), 402 F. Supp. 2d 597, 605 (D. Md. 2005) (requiring that the government obtain a warrant based on probable cause in all future cases in which it seeks to obtain an individual's real-time cell-site location information); Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) (holding that the government conducted a Fourth Amendment search when it tracked the defendant's cell phone location in real time); U.S. DEP'T OF JUSTICE, *supra* note 149 (adopting a warrant requirement for the Department's use of cell-site simulators, which intercept real-time cellular location information).

[151] *See* Barrett, *supra* note 2 (noting that the Dirtbox can "pinpoint [a target's] location within about 10 feet, down to a specific room in a building"); *see also In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 574 (D. Md. 2011) (describing how real-time location information has the potential to be triangulated for greater accuracy); Interview with Nathan Freed Wessler, *supra* note 90 (explaining that real-time CSLI provides more precise tracking than historical CSLI because the former can be triangulated). *But see* Pell & Soghoian, *supra* note 90 (noting that certain cellular providers regularly record triangulated CSLI, although it is not common practice to do so).

[152] *See, e.g.*, State v. Tate, 849 N.W. 2d 798, 805 (Wis. 2014), *cert. denied*, 135 S. Ct. 1166 (2015) (mem.) (noting that the State of Wisconsin had conceded that the use of a Stingray amounted to a Fourth Amendment search); United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013) (acknowledging the government's stipulation that the Stingray operation constituted a search and seizure under the Fourth Amendment).

[153] *See* Barrett, *supra* note 2 (describing how the Dirtbox can "pinpoint [a target's] location within about 10 feet, down to a specific room in a building"); Memorandum from Stephen W. Miko, Res. Manager, Anchorage Police Dep't, to Bart Mauldin, Purchasing Officer, Anchorage Police Dep't (June 24, 2009), http://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf (noting that a portable KingFish cell-site simulator can identify the location of a cellular device within twenty-five feet); *see also* Ali Winston, *Chicago and Los Angeles Have Used 'Dirt Box' Surveillance for a Decade*, REVEAL NEWS (Aug. 7, 2015), https://www.revealnews.org/article/chicago-and-los-angeles-have-used-dirt-box-surveillance-for-a-decade/ [https://perma.cc/QX2U-B53B] (characterizing Dirtboxes as "a more powerful class of cell-site simulator than the more widely used Stingray").

[154] *See* United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (expressing concern about long-term monitoring, which "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations"); Kerr, *supra* note 70, at 315 (describing how a mosaic theory analysis considers a series of government acts together, rather than examining them in isolation); *see also* Barrett, *supra* note 2 (describing how Dirtbox surveillance flights occur regularly).

Dirtbox surveillance amounts to a search because it gathers location information from within private residences.[155] Considering the frequency and remarkable accuracy of Dirtbox data collection, it is very likely that this surveillance acquires location information from individuals inside their homes, a constitutionally protected space.[156] Although it is possible that a single instance of Dirtbox tracking could pinpoint an individual in a constitutionally unprotected space, the U.S. Supreme Court has explicitly forbidden this Russian roulette approach.[157] Dirtbox surveillance, therefore, violates the most inviolable—privacy in the home.[158]

The mosaic theory, though developed in response to continuous GPS tracking, could reasonably be extended to cover continual cell phone loca-

---

[155] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that the acquisition by sense-enhancing technology of information about the inside of a home constitutes a Fourth Amendment search); *United States v. Karo*, 468 U.S. 705, 716 (1984) (holding that the government is not exempt from the warrant requirement when it uses an electronic device to determine whether an item or person is inside of an individual's home). A "mere visual enhancement" argument by the government under *Knotts* would be trumped by the in-home privacy holdings of *Kyllo* and *Karo*, as discussed in this section. *See Kyllo*, 533 U.S. at 34; *Karo*, 468 U.S. at 716.

[156] *See* Barrett, *supra* note 2 (explaining how the Dirtbox enables law enforcement to gather data from "tens of thousands of cellphones in a single flight, collecting their identifying information and general location"); *see also* BUREAU OF LABOR STATISTICS, U.S. DEP'T OF LABOR, AMERICAN TIME USE SURVEY—TIME USE ON AN AVERAGE WORK DAY FOR EMPLOYED PERSONS AGES 25 TO 54 WITH CHILDREN (2013), http://www.bls.gov/tus/charts/ [http://perma.cc/H5DY-4YDQ] (revealing that the average employed person between ages twenty-five and fifty-four with children spends at least 8.8 hours at home on a given work day); Paul Tadich, *I Spy with My Little "Dirtbox": How The U.S Government Surveils Cellphones*, SPUTNIK (Nov. 15, 2014, 12:33PM), http://us.sputniknews.com/us/20141115/1013225346.html [https://perma.cc/3LC5-CSBK] (describing how the DOJ uses the Dirtbox to first isolate the target cell phone, then pinpoint the target within ten feet). The Dirtbox surveillance program signals that it is time for the Court to address the constitutionality of large-scale cell phone location tracking. *See* United States v. Knotts, 460 U.S. 276, 284 (1983) ("[I]f such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

[157] *See Kyllo*, 533 U.S. at 38–39 (holding it impractical in application to prohibit only thermal imaging of "intimate details" because police could not know in advance what through-the-wall surveillance might detect); *Karo*, 468 U.S. at 716 (determining that the government could not use an electronic device to determine whether a person or item was inside a residence at a certain time without being subjected to the requirements of the Fourth Amendment); *see also Tracey*, 152 So. 3d at 518 (explaining that law enforcement has no way of knowing if a suspect will be inside of a constitutionally protected space when they acquire real-time CSLI); *Earls*, 214 N.J. at 586 (noting that "law enforcement had no way of knowing in advance whether defendant's cell phone was being monitored in a public or private space").

[158] *See Kyllo*, 533 U.S. at 34 (holding that the acquisition by sense-enhancing technology of information about the inside of a home constitutes a Fourth Amendment search); *Karo*, 468 U.S. at 716 (holding that the government is not exempt from the warrant requirement when it uses an electronic device to determine whether an item or person is inside of an individual's home); *see also* Brief for the Appellees, *supra* note 146, at 5 ("By pinpointing suspects and third parties while they are inside constitutionally protected spaces, cell site simulators invade reasonable expectations of privacy.").

tion monitoring.[159] The idea behind the mosaic theory is that prolonged surveillance reveals intimate details about a person's life that would not be disclosed under short-term surveillance.[160] A similarly intimate picture would be revealed through continual Dirtbox monitoring, regardless of the brevity of each instance of surveillance.[161] Although the mosaic theory is not yet law, a majority of the Court has expressed concern about the same kind of pattern-tracking surveillance that may be carried out under the Dirtbox program.[162]

When the U.S. Supreme Court decided *Jones*, it avoided the now-pressing issue of cell phone location tracking that is free from physical attachment.[163] When next presented with the opportunity, the Court must acknowledge that individuals have a reasonable expectation of privacy from cell phone location interception.[164] To do so would be to acknowledge that privacy protections must evolve along with the technology that threatens them, and to embrace the reasonable expectation of privacy standard outlined in the Court's 1967 decision in *Katz v. United States*, which allows for this evolution.[165]

B. Congress Must Enact a Warrant Requirement

Although the DOJ policy memo is an encouraging step in transparency and regulation of cell-site simulators, it does not adequately protect the pri-

---

[159] *See Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring) (endorsing some form of the mosaic approach); Kerr, *supra* note 70, at 320–21 (noting that a majority of the Court is prepared to embrace the mosaic theory); Slobogin, *supra* note 65, at 7 (observing that five Justices appear ready to decouple physical trespass from the Fourth Amendment).

[160] *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (explaining how prolonged surveillance reveals habits and is therefore more intrusive than short-term surveillance), *aff'd in part sub nom. Jones*, 132 S. Ct. 945; *see also Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring) (applying the mosaic theory to continuous GPS tracking over a twenty-eight-day period).

[161] *See Jones*, 132 S. Ct. at 963–64; *see also* Barrett, *supra* note 2 (revealing that Dirtbox flights occur regularly). Continual Dirtbox surveillance may represent an even greater intrusion than the vehicle-mounted GPS tracking in *Jones* because it targets cell phones, which are carried by individuals into constitutionally protected spaces. *See* Commonwealth v. Augustine, 4 N.E.3d 846, 861 (Mass. 2014) (citing United States v. Powell, 943 F. Supp. 2d 759, 777 (E.D. Mich. 2013) ("There are practical limits on where a GPS tracking device attached a person's vehicle may go. A cell phone, on the other hand, is usually carried with a person *wherever* they go.").

[162] *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (endorsing some form of mosaic theory); *id.* at 963–64 (Alito, J., concurring) (same); *see also* Barrett, *supra* note 2 (describing how Dirtbox surveillance flights occur regularly).

[163] *Jones*, 132 S. Ct. at 954–64 (Alito, J., concurring) (predicting that the majority's reliance on the trespass doctrine will present courts with frustrating issues in cases involving non-physical, electronic surveillance).

[164] *Id.*

[165] *See id.* at 955 (Sotomayor, J., concurring).

vacy rights of individuals targeted for Dirtbox surveillance.[166] First, the memo provides a broad carve-out from its warrant mandate.[167] Second, the policy only applies to DOJ agents.[168] Finally, the memo consists entirely of unenforceable policy guidelines.[169]

The exceptional circumstances carve-out significantly undercuts the warrant rule.[170] Specifically, agents may deploy cell-cite simulators subject only to internal approval where it is impracticable to obtain a warrant.[171] The memo, however, provides neither an explanation nor examples of the situations in which it would be impracticable to get a warrant.[172] This exception is so vague that it creates a nearly explicit loophole for the DOJ to conduct warrantless cell-site location monitoring at any time.[173] It is little

---

[166] *See* DOJ Cell-Site Policy Memo, *supra* note 103; *ACLU Comment*, *supra* note 114 (recognizing the DOJ guidelines as commendable but insufficient); Johnson, *supra* note 124 (quoting Senator Patrick Leahy, D-VT, who lauded the DOJ's announcement of its new cell-site simulator policy but expressed "serious questions about the exceptions to the warrant requirement"); Faiza Patel, *DOJ's New Stingray Policy Is a Good Start, but It's Got Problems*, BRENNAN CTR. FOR JUST. (Sept. 10, 2015), https://www.brennancenter.org/blog/dojs-new-stingray-policy-good-start-its-got-problems [http://perma.cc/X2LG-V8PK] (lauding the DOJ's policy guidance as a "good first step," but indicating its shortcomings).

[167] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 3–5 (laying out two exceptions to the Department's new warrant rule); *ACLU Comment*, *supra* note 114 (advocating that the DOJ close loopholes left in its newly adopted warrant requirement); Johnson, *supra* note 124 (noting Senator Leahy's concern about the DOJ's warrant exceptions).

[168] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 6 (limiting the applicability of the guidelines to agents of the DOJ); *ACLU Comment*, *supra* note 114 (advocating that the DOJ extend its policy to cover the use of cell-site simulators by state and local law enforcement, which use federal funding to purchase the devices).

[169] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 2 n.2 (clarifying that the policy memo sets forth nothing more than internal policy guidance and does not create any enforceable rights).

[170] *See id.* at 3–5; *ACLU Comment*, *supra* note 114 (advocating that the DOJ close loopholes left in its newly adopted warrant requirement); Johnson, *supra* note 124 (noting Senator Leahy's concern about the DOJ's warrant exceptions).

[171] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 4–5 (setting forth the exceptional circumstances warrant exception); Patel, *supra* note 166 (indicating that the exceptional circumstances carve-out permits the agency to utilize cell-site simulators whenever it believes that obtaining a warrant would be impracticable). In contrast to the exceptional circumstances carve-out, the exigent circumstances exception is reasonable because it permits warrantless operation of a cell-site simulator where there exists a threat to human life or the administration of justice. *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 3–4 (noting that exigent circumstances include the need to protect against serious harm to human life, prevent the imminent destruction of evidence, pursue a fleeing criminal, and prevent the escape of a fugitive suspect or convict).

[172] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 4 (providing that no search warrant will be required under circumstances where obtaining one would be "impracticable"); Patel, *supra* note 166 (noting that the policy does not provide examples of circumstances where it might be impracticable to obtain a warrant).

[173] *See* Johnson, *supra* note 124 (noting the concern of ACLU attorney Nathan Freed Wessler that undefined "exceptional circumstances" leave the door open to warrantless use of cell-site simulators); Patel, *supra* note 166 (highlighting the vagueness of the exceptional circumstances carve-out).

consolation that the DOJ expects this exception to be invoked in a limited number of cases.[174]

Furthermore, the guidelines only apply to DOJ agents.[175] But the DOJ is not the only federal agency that uses cell-site simulators.[176] Of greater concern, this military-grade surveillance technology is now routinely being used by state and local law enforcement.[177] With the help of federal anti-terror grants, local police forces obtain this powerful technology and deploy it for routine investigations.[178]

Finally, the policy memo is toothless—it consists of unenforceable guidelines.[179] In a single footnote, the DOJ clarified that the guidelines are meant to improve internal management and provide no legal rights or reme-

---

[174] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 4 (expecting exceptional circumstances to be "very limited"); *see also* Patel, *supra* note 166 (noting that the policy provides no examples of "exceptional circumstances" other than forecasting that they will be "very limited").

[175] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 6 ("This policy applies to all instances in which Department components use cell-site simulators in support of other Federal agencies and/or State and Local law enforcement agencies."); Patel, *supra* note 166 (interpreting the policy as being completely inapplicable to state and local police). Although the DOJ memo does not govern the use of cell-site simulators by state and local law enforcement, the language of the policy is ambiguous enough to lead some to believe otherwise. *See, e.g.*, Johnson, *supra* note 124 ("The new policy applies to federal agents under Justice Department control *and to state or local investigators who work on federal task forces*." (emphasis added)).

[176] *Stingray Tracking Devices: Who's Got Them?*, *supra* note 95 (listing thirteen federal agencies, some outside of the DOJ, that are known to be using cell-site simulators); Nicky Woolf & William Green, *IRS Possessed Stingray Cellphone Surveillance Gear, Documents Reveal*, The GUARDIAN (Oct. 26, 2015), http://www.theguardian.com/world/2015/oct/26/stingray-surveillance-technology-irs-cellphone-tower [http://perma.cc/5TQ7-UC2K] (detailing how the Internal Revenue Service is among the federal agencies using cell-site simulators).

[177] *See* Cagle, *supra* note 1 (describing how local law enforcement in Anaheim have spent nearly a decade developing an inventory of powerful cell phone location monitoring devices); Ferner, *supra* note 1 (noting that police in Anaheim, California use the Dirtbox); Winston, *supra* note 153 (detailing the use of Dirtboxes by the Los Angeles and Chicago police departments); *see also* Patel, *supra* note 166 (arguing that the policy leaves open a "huge gap" by failing to confront the use of cell-site simulators by state and local law enforcement); *Stingray Tracking Devices: Who's Got Them?*, *supra* note 95 (displaying a map and table revealing the pervasive use of cell-site simulators by both state and local law enforcement across the United States).

[178] Cagle, *supra* note 109 (detailing how the Anaheim police used a federal grant to purchase a Dirtbox); Patel, *supra* note 166 (contending that although the DOJ may be reluctant to extend the new warrant requirement to police departments, it could attach some conditions to the devices that it provides and finances); Nathan Freed Wessler, *Police Citing "Terrorism" to Buy Stingrays Used Only for Ordinary Crimes*, AM. C.L. UNION: FREE FUTURE (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/4ZVE-SGV2] (describing how the state police department in Michigan "justified its initial purchase of the surveillance gear as 'vital to the war on terrorism'" but used the technology "in 128 run-of-the-mill investigations last year—not a single one of which was for terrorism").

[179] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 2 n.2 (clarifying that the policy memo sets forth internal guidelines, not law); Patel, *supra* note 166 (noting that the warrant requirement "is being implemented 'as a matter of policy'—i.e., not as a matter of law").

dies.[180] Therefore, even if a defendant could prove that the DOJ had violated its own rules and obtained incriminating evidence through warrantless Dirtbox surveillance, these guidelines would not necessarily compel a court to suppress that evidence.[181] Because suppression is the primary means to deter law enforcement from evading a warrant requirement, absent judicial or legislative mandate, the DOJ's warrant rule will have little deterrent effect.[182]

Until the U.S. Supreme Court recognizes that individuals have a reasonable expectation of privacy in their cellular location information, Congress should pass legislation requiring the government to obtain a warrant before using the Dirtbox and any other cell-site simulator.[183] As proposed by Representative Jason Chaffetz, Congress should go beyond the scope of the DOJ memo by requiring all law enforcement—whether federal, state, or local—to obtain a warrant before operating a cell-site simulator.[184] Unlike Representative Chaffetz' proposal and the DOJ memo, however, Congress should reject the unspecified "exigent circumstances" loophole and should exempt law enforcement from the warrant requirement in emergency situations only.[185] In the meantime, states should continue to push ahead of the federal government on locational privacy protection.[186]

---

[180] *See* DOJ Cell-Site Policy Memo, *supra* note 103, at 2 n.2 (stipulating that the policy serves internal management purposes only and "is not intended to and *does not create any right*, benefit, trust, or responsibility, whether substantive or procedural, *enforceable at law or equity*" and does not "create any right of review in an administrative, judicial, or any other proceeding" (emphasis added)).

[181] *See id.*

[182] *See id.*; *see also* Mapp v. Ohio, 367 U.S. 643, 655 (1961) (describing the essential deterrent function served by the Fourth Amendment's exclusionary rule).

[183] *See ACLU Comment*, *supra* note 166 (analyzing the inadequacies of the DOJ policy memo and concluding that Congress should pass comprehensive legislation to protect individuals' privacy from encroachments by cell-site simulators and other tracking technology).

[184] *See* Cell-Site Simulator Act of 2015, H.R. 3871, 114th Cong. (2015) (proposing an expansion and codification of the DOJ memo).

[185] *See id.*; DOJ Cell-Site Policy Memo, *supra* note 103, at 4–5.

[186] *See* Andy Greenberg, *Congress Has a Thing or Two to Learn from These State Privacy Laws*, SLATE: FUTURE TENSE (Jan. 26, 2016, 2:49 PM), http://www.slate.com/blogs/future_tense/2016/01/26/electronic_communications_privacy_act_is_due_for_an_upgrade.html [https://perma.cc/VHU7-Z4LL] (noting that various states have introduced legislation to impose a warrant requirement on Stingrays, and that Nebraska has drafted a law that would ban the devices entirely); *see also* IND. CODE ANN. § 35-33-5-12(a) (2015) (prohibiting law enforcement from using real-time cellular tracking devices without first obtaining "an order issued by a court based upon a finding of probable cause," unless exigent circumstances exist); MINN. STAT. § 626A.42, subd. 2(a) (2014) (providing that "a government entity may not obtain the location information of an electronic device without a tracking warrant," except in situations of lost or stolen devices, emergency, or informed consent); TENN. CODE ANN. § 39-13-610(b) (2014) (providing that "no governmental entity shall obtain the location information of an electronic device without a search warrant issued by a duly authorized court," except in circumstances of a stolen device, an emergency, affirmative consent, a user posting his location on social media, or exigency); UTAH CODE

CONCLUSION

The use of Dirtbox technology by law enforcement to intercept individuals' cell phone location data, without judicial or legislative oversight, poses a significant problem. Because surveillance by cell-site simulators violates society's reasonable expectation of privacy, these devices implicate the privacy protections of the Fourth Amendment. The cell-site simulator guidelines issued by the Department of Justice represent an encouraging step in transparency and privacy protection, but the warrant mandate is limited. Across the country, state legislatures have begun imposing restrictions on the use of cell-site simulators. But the current patchwork of inconsistent laws and unenforceable guidelines indicates that more comprehensive protection is needed. Until the U.S. Supreme Court accepts the opportunity to bring the Fourth Amendment into the twenty-first century, Congress must enact a warrant law to ensure that privacy protection keeps pace with surveillance technology.

JONATHAN BARD

ANN. § 77-23c-102(1)(a), (2)(a) (West 2014) (providing that "a government entity may not obtain the location information . . . of an electronic device without a search warrant issued by a court upon probable cause," except in situations involving an emergency, locating a stolen device, informed consent, judicially recognized warrant exceptions, or voluntary public disclosure).