William & Mary Bill of Rights Journal

Volume *26 (2017-2018)*
Issue 2 *Symposium: Big Data, National Security, and the Fourth Amendment*

Article 10

December 2017

The Fourth Amendment Disclosure Doctrines

Monu Bedi

THE FOURTH AMENDMENT DISCLOSURE DOCTRINES

Monu Bedi*

INTRODUCTION

The third party and public disclosure doctrines (together the "disclosure doctrines") are long-standing hurdles to Fourth Amendment protection.[1] These doctrines have become increasingly relevant to assessing the government's use of recent technologies such as data mining, drone surveillance, and cell site location data.[2] It is surprising then that both the Supreme Court and scholars, at times, have associated them together as expressing one principle.[3] It turns out that each relies on unique foundational triggers and does not stand or fall with the other. This Article tackles this issue and provides a comprehensive topology for analyzing the respective contours of each doctrine.[4]

The third party doctrine involves an individual voluntarily disclosing information to a third party and the government thereafter acquiring it from the third party.[5] The nature of the information—whether it is public or private—is not relevant.[6] The individual loses all Fourth Amendment protection to this information because she assumes the risk the third party will hand it over to the government.[7] The Supreme Court has applied this doctrine to discrete conversations revealed to informants,[8] bank records relayed to bank employees,[9] and phone numbers disclosed to phone companies.[10]

---

* Associate Professor, DePaul University College of Law. AB Dartmouth College, M.Phil. University of Cambridge, JD Harvard University.

[1] *See* discussion *infra* Sections I.A–B.

[2] *See, e.g.*, DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017) [hereinafter GRAY, AGE OF SURVEILLANCE] (discussing Fourth Amendment protection and the disclosure doctrines in light of recent technologies and big data collection). The focus here is on the constitutionality of these practices, not any applicable statutory regulations or laws. *See infra* Section II.B, Part III.

[3] *See* discussion *infra* Section I.C.

[4] I build on a prior essay on this topic. *See generally* Monu Bedi, *The Curious Case of Cell Phone Location Data: Fourth Amendment Doctrine Mash-Up*, 110 NW. U. L. REV. 507 (2016) [hereinafter Bedi, *Cell Phone Location Data*].

[5] *See* Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 2 (2013) [hereinafter Bedi, *Facebook*].

[6] *See id.* at 12.

[7] *See id.* at 2.

[8] *See* Hoffa v. United States, 385 U.S. 293 (1966) (holding that communications to an informer were not privileged).

[9] *See* United States v. Miller, 425 U.S. 435 (1976) (holding that there is no Fourth Amendment interest in bank communications).

[10] *See* Smith v. Maryland, 442 U.S. 735 (1979) (holding that phone numbers dialed are not protected); *see also* discussion *infra* Section I.A.

The public disclosure doctrine, on the other hand, focuses on an individual disclosing movements or items that are susceptible to visual observation.[11] There is no third party involved nor is one necessary for an application of the doctrine.[12] The key to vitiating Fourth Amendment protection is simply that the government is surveilling these movements or observing these items while they are public. The Supreme Court has applied this doctrine to government use of beeper tracking,[13] GPS surveillance,[14] and aerial reconnaissance.[15]

The Court as well as scholars have been guilty of grouping together these two doctrines when assessing Fourth Amendment protection, particularly as it relates to new technologies. For instance, in *United States v. Jones*[16]—the most recent Supreme Court case on surveillance and technology—Justice Sotomayor in her now famous concurrence argues that the third party doctrine may not be viable in today's technology-dominated world.[17] This interesting non sequitur is puzzling as the case only dealt with visual surveillance and the public disclosure doctrine.[18] Scholars too—in their assessment of mass surveillance and data collection—have lumped the two doctrines together, suggesting they stand or fall as one.[19] On one level, this association is understandable as both doctrines involve waiving Fourth Amendment protection to certain actions and assuming the risk the government will acquire the information. But a more precise understanding of the respective elements of the doctrines is imperative if scholars and courts are to properly assess Fourth Amendment protection when it comes to new methods of government surveillance and data collection.

For example, there may be instances where the third party doctrine applies—such as mass collection of phone numbers or other private data—but there is no potential application of the public disclosure doctrine because the information is not public. Similarly, there may be instances where the public disclosure doctrine applies—such as surreptitious government long-term monitoring using GPS or drones—but there would be no application of the third party doctrine because there is no knowing disclosure to a third party.

There also may be situations where both doctrines could potentially apply. I use cell phone site location data as a case study.[20] Courts seem to pick and choose a

---

[11] Bedi, *Cell Phone Location Data*, *supra* note 4, at 513.

[12] *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); *see also* discussion *infra* Section II.B.

[13] *See Knotts*, 460 U.S. at 285 (applying the doctrine to beepers).

[14] United States v. Jones, 565 U.S. 400, 402 (2012) (applying the doctrine to GPS).

[15] California v. Ciraolo, 476 U.S. 207, 209 (1986) (applying the doctrine to aerial surveillance); *see also* discussion *infra* Section I.B.

[16] 565 U.S. 400 (2012).

[17] *Id.* at 417 (Sotomayor, J., concurring).

[18] *Id.* at 412–13 (majority opinion).

[19] *See* discussion *infra* Section I.C.

[20] *See* discussion *infra* Section III.B.

doctrine without a complete understanding of why one or the other applies (or does not apply).[21] These inconsistent results are primarily due to the unique nature of this technology and the different ways one can conceptualize how the government collects it. The data can be viewed as non-public information disclosed to a cell phone provider (suggesting a potential application of the third party doctrine) or seen as public movements susceptible to visual surveillance (suggesting a potential application of the public disclosure doctrine).[22] The key to applying the right doctrine is recognizing in which of these two contexts the government activity is taking place.

The Article proceeds in three parts. Part I provides an historical development of each disclosure doctrine and how new technologies have impacted their respective application. It also highlights how the Court and scholars have grouped together the doctrines in assessing Fourth Amendment protection. Part II works with the Court's jurisprudence to tease out the respective elements of each doctrine. Part III explores how these doctrines—with an understanding of their unique requirements—can potentially apply to current issues of big data and new technologies, with a focus on cell site location data. Working with a better understanding of the reach of each disclosure doctrine, I provide a clearer picture of the relevant privacy considerations in this unique context.

I. DEVELOPMENT AND CONFLATION OF THE DISCLOSURE DOCTRINES

A. History of the Third Party Doctrine

1. *Katz* and Human Interaction

The early cases applying the third party doctrine centered on face-to-face conversations with government informants.[23] Under these decisions, as long as agents did not trespass on a person's property, individuals did not have Fourth Amendment protection in what they disclosed to an undercover informant, irrespective of the individual's belief that the informant would not disclose the information to the government.[24] Any such information can be gathered without a warrant or probable cause and subsequently used against the person at trial.[25] As the Court articulated, "a wrongdoer's misplaced belief that a person to whom he voluntary confides his wrongdoing will not reveal it" receives no protection under the Fourth Amendment.[26]

---

[21] *See* discussion *infra* Section III.B.3.

[22] *See* discussion *infra* Section III.B.3.

[23] *See* Hoffa v. United States, 385 U.S. 293 (1966); Lewis v. United States, 385 U.S. 206 (1966); Lopez v. United States, 373 U.S. 427, 439 (1963); On Lee v. United States, 343 U.S. 747 (1952).

[24] *See, e.g.*, *Hoffa*, 385 U.S. at 302–03; *Lewis*, 385 U.S. at 210–11.

[25] *See, e.g.*, *Lopez*, 373 U.S. at 438–40.

[26] *Hoffa*, 385 U.S. at 302.

This has become known as the "third party doctrine," which states that the Fourth Amendment does not protect information a person voluntarily discloses to a third party and thereafter acquired by the government.[27]

Katz v. United States[28] dramatically reconceptualized Fourth Amendment analysis but left unchanged the application of the third party doctrine.[29] The Court no longer restricted Fourth Amendment protection to a person's property or physical space; rather, the Court applied Fourth Amendment protection more broadly to any situation in which an individual has a reasonable expectation of privacy.[30] In holding that the defendant had a reasonable expectation of privacy in a telephone booth, Justice Harlan in his famous concurrence articulated the now well-known two-part test for when Fourth Amendment protection applies: a person must have a subjective expectation of privacy and the expectation must be objectively reasonable.[31]

Shortly after *Katz*, in 1971, in *United States v. White*,[32] the Supreme Court explicitly made clear that the third party doctrine survived the new expectation of privacy test.[33] In *White*, a government informant, without first seeking a warrant, used a radio transmitter to surreptitiously transmit conversations with the defendant at various locations, including the defendant's home.[34] The Court found no Fourth Amendment violation in using these transmitted conversations at trial because the defendant voluntarily disclosed the information to a third party, which vitiated any reasonable expectation of privacy.[35] It did not matter that the defendant may have subjectively believed the conversation was being kept secret or the informant was not working with police to record the information.[36] This actual expectation was not constitutionally justified because "the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent."[37]

United States v. Miller[38] extended the third party doctrine beyond conversations to include personal documents and records conveyed to third parties.[39] In *Miller*, by voluntarily disclosing records to a bank and its employees, the defendant lost any claim of Fourth Amendment protection to those documents.[40] Citing *Katz*, the Court

---

[27] *See* United States v. White, 401 U.S. 745, 749 (1971); *see also* Bedi, *Facebook*, *supra* note 5, at 8 (discussing history and development of the third party doctrine and how it vitiates Fourth Amendment privacy protection).

[28] 389 U.S. 347 (1967).

[29] *Id.*

[30] *Id.* at 350–53.

[31] *Id.* at 360–61 (Harlan, J., concurring).

[32] 401 U.S. 745 (1971).

[33] *See id.*

[34] *Id.* at 746–47.

[35] *Id.* at 751–52.

[36] *Id.* at 752.

[37] *Id*.

[38] 425 U.S. 435 (1976).

[39] *Id.* at 445.

[40] *Id.* at 442–43.

explained that the defendant's misplaced subjective belief or trust that these records would only be used for a limited financial purpose did not change the fact that once he conveyed the information to the bank employees he took the risk that the government may obtain this information from them.[41] Thus, the Court held that the defendant could not object to the government acquiring the documents from the bank without a warrant as he possessed no Fourth Amendment interest in the items.[42]

2. Disclosures to Machines and Companies

In *Smith v. Maryland*,[43] the Court took the third party doctrine one step further and applied it to information disclosed to a telephone company's automated switching equipment.[44] In *Smith*, the government requested that the phone company set up a "pen register," a device intended to record all outgoing phone numbers dialed by the defendant from his home.[45] The device was installed at the phone company's offices; at no point did the government enter the defendant's property.[46] The Court upheld the warrantless use of the pen register, stating that the Fourth Amendment did not protect the numbers dialed by the telephone user.[47] Applying the two-part *Katz* test, the Court held that the defendant did not have a subjective expectation of privacy in the dialed numbers, nor would any such expectation be reasonable.[48] Telephone users realize that they must convey the number to the telephone company in order to make a call and that the company has facilities for making permanent records of the numbers dialed.[49]

Further, and more importantly, the Court held that any subjective expectation of privacy (assuming one existed) was not something society would find reasonable.[50] Citing *Miller*, the Court concluded that the defendant did not satisfy the second element of the *Katz* test because he did not have a reasonable expectation of privacy in the dialed numbers.[51] The Court explained that "[w]hen he used his phone,

---

[41] *See id.*

[42] *Id.* at 440–46.

[43] 442 U.S. 735 (1979).

[44] *Id.*

[45] *Id.* at 737. This device "records the numbers dialed . . . by monitoring the electrical impulses caused when the dial on the telephone is released." *Id.* at 736 n.1 (quoting United States v. New York Tel. Co., 434 U.S. 159, 161 n.1 (1977)). The device does not record the conversations that take place after a call has been made. *Id.* (citing *New York Tel. Co.*, 434 U.S. at 161 n.1).

[46] *Id.* at 741.

[47] *Id.* at 745–46.

[48] *See id.*

[49] *Id.* at 742.

[50] *Id.* at 743.

[51] *Id.* at 743–44 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976)).

[the defendant] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[52]

The fact that the number was disclosed to an automated machine instead of a human being was of no consequence.[53] The Court explained:

> The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.[54]

This point is critical to the holding in *Smith*. The Court did not address whether a human being actually observed the number being dialed.[55] This apparently was not relevant.[56] All that mattered was that the defendant voluntarily exposed the number to a third party's machine—in this case, the telephone company's switching equipment.[57] The implication here is that an individual will likely lose Fourth Amendment protection to any information she exposes to a third party's machine in the normal course of business, regardless of whether a human actually observes the information.[58]

The holding in *Smith v. Maryland*—while seemingly an uncontroversial application of the third party doctrine—has led to difficult questions regarding disclosure to companies in today's technology-dominated world.[59] Take the fact that nearly all data, including emails, are stored with third party servers or Internet service providers.[60] Internet service providers (ISPs) like Gmail, Facebook and other companies—not unlike phone companies using phone numbers to contact individuals—store these

---

[52] *Id.* at 744.

[53] *Id.*

[54] *Id.* at 744–45 (internal citation omitted).

[55] *See id.*

[56] *See id.*; *see also* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 600 (2011) ("[T]here is no legally relevant difference between disclosure of one's personal information to a third party's automated systems and disclosure to a human being.").

[57] *Smith*, 442 U.S. at 744–45; Tokson, *supra* note 56, at 600.

[58] *See Smith*, 442 U.S. at 744–45; Tokson, *supra* note 56, at 600.

[59] *See* Bedi, *Facebook*, *supra* note 5, at 15–32 (discussing the role of third party servers in transmission of communications over the Internet and the potential implication of the third party doctrine); Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809 (2014) [hereinafter Bedi, *Mosaic Theory*] (discussing how the mosaic theory may protect internet communications from the third party doctrine).

[60] Tokson, *supra* note 56, at 585; *see* PRESTON GRALLA, HOW THE INTERNET WORKS 88–99 (8th ed. 2007) (describing how emails are transmitted and stored).

communications for brief periods in order to deliver them to their recipient.[61] The third party doctrine would suggest that the government can acquire this information from the ISP without first seeking a warrant.[62] The Court has to yet decide whether the third party doctrine vitiates Fourth Amendment privacy in this context.[63] Some appellate courts have found that these communications are potentially subject to the third party doctrine whereas others attempt to distinguish the type of information contained in the communication to support privacy protection.[64] Scholars too disagree on how the Fourth Amendment should apply to these disclosures.[65]

---

[61] *See* GRALLA, *supra* note 60, at 89 ("The [Transmission Control] protocol breaks your messages into packets, the IP protocol delivers the packets to the proper location, and then the TCP reassembles the message on the receiving mail server so it can be read."); Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 813–14 (2003) (describing how emails are routed by equipment owned by the ISP that processes their data); Tokson, *supra* note 56, at 602–03 (describing how email service providers, such as Gmail and Hotmail, store email data). Even deleted emails are at least temporarily stored on third party systems. *See, e.g.*, James X. Dempsey, *Digital Search and Seizure: Updating Privacy Protections to Keep Pace with Technology*, *in* 1 SEVENTH ANNUAL INSTITUTE ON PRIVACY LAW: EVOLVING LAWS AND PRACTICES IN A SECURITY-DRIVEN WORLD 505, 523 (2006) ("[S]ince ISPs [such as Gmail and Yahoo] retain data for varying lengths of time, and do not always delete email immediately upon request, customers may not be aware of whether their email is still stored and thus susceptible to disclosure.").

[62] *See* Bedi, *Facebook*, *supra* note 5, at 15–18 (discussing application of third party doctrine to internet communications). It is important to note that even if the Fourth Amendment does not apply, separate statutory restrictions are in place before the government can obtain these communications. *Id.* at 31–36 (discussing congressional legislation and specifically Electronic Communications Privacy Act as means to protect internet communications); *see* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522, 2701–2711, 3117, 3121–3127 (2012)).

[63] *See, e.g.*, Rehberg v. Paulk, 611 F.3d 828, 844 (11th Cir. 2010) ("The Supreme Court has not yet addressed the question of privacy rights in email material.").

[64] *See id.* at 846 ("Given the lack of precedent, we now question whether it would be prudent in this case and on this limited factual record to establish broad precedent as to the reasonable privacy expectation in email content."); United States v. Warshak, 631 F.3d 266, 285–87 (6th Cir. 2010) (analogizing emails to letters and finding that content of emails but not the subject/to lines garner Fourth Amendment protection even though voluntarily transmitted to ISP); *In re* United States, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009) (noting that email users "voluntarily conveyed to the ISPs and exposed to the ISP's employees in the ordinary course of business the contents of their e-mails"); *see also* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904–05 (9th Cir. 2008) (holding that users have an expectation of privacy in the contents of their text messages), *rev'd sub nom.* City of Ontario v. Quon, 560 U.S. 746 (2010) (holding that the search, even if it did implicate the Fourth Amendment, was in any case reasonable).

[65] *See, e.g.*, Bedi, *Facebook*, *supra* note 5, at 18–28 (discussing theories by Professors Matthew Tokson (automation rationale), Orin Kerr (content vs. non-content), and Katherine Strandburg (technosocial theory) on ways to protect internet communications despite third party doctrine).

The ability of the government to collect massive amounts of data further complicates a straightforward third party doctrine calculus. *Smith v. Maryland* only dealt with one phone number over a short period of time.[66] Does the analysis change if we are dealing with significant amounts of data mining over longer periods of time? In 2013, it came to light that the National Security Agency was working with Verizon to collect massive amounts of phone numbers of thousands of subscribers over a number of years.[67] While the government did seek statutory approval prior to this collection, the American Civil Liberties Union brought suit on behalf of the subscribers alleging that this activity fell under the Fourth Amendment and thus the government was required to first obtain a warrant supported by probable cause.[68] After two years of debate, Congress changed the relevant law surrounding this type of collection.[69] Meanwhile, the cases made their way through the Second and D.C. Circuits where both appellate courts ultimately punted on the relevant Fourth Amendment question, resting their findings on other grounds.[70] Scholars have tackled the constitutionality of this practice and debated how (if at all) bulk collection of private data more generally can garner Fourth Amendment protection in light of the third party doctrine.[71]

---

[66] *See generally* Smith v. Maryland, 442 U.S. 735 (1979); *supra* notes 43–58 and accompanying text.

[67] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 EDT), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/3C2B-YDEF] (describing the extent of government collection of the phone records of U.S. citizens). There was no evidence that the government was otherwise monitoring the content of the calls. *See generally id.*

[68] Ellen Nakashima & Scott Wilson, *ACLU Sues over NSA Surveillance Program*, WASH. POST (June 11, 2013), https://www.washingtonpost.com/politics/aclu-sues-over-nsa-surveillance-program/2013/06/11/fef71e2e-d2ab-11e2-a73e-826d299ff459_story.html [https://perma.cc/H56L-NYBD].

[69] *See* Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection, and Online Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. No. 114-23, 129 Stat. 268 (codified at 50 U.S.C. § 1861 (2015)); *see also* Nicole B. Cásarez, *The Synergy of Privacy and Speech*, 18 U. PA. J. CONST. L. 813, 823–36 (2016) (discussing the history of the new law and arguing that, while it did limit the government's ability to obtain this kind of bulk information, the new legislation does not terminate the program).

[70] *See* ACLU v. Clapper, 785 F.3d 787, 824 (2d Cir. 2015) ("Because we conclude that the challenged program was not authorized by the statute on which the government bases its claim of legal authority, we need not and do not reach these weighty constitutional issues."); Obama v. Klayman, 800 F.3d 559, 564 (D.C. Cir. 2015) ("Having barely fulfilled the requirements for standing at this threshold stage, Plaintiffs fall short of meeting the higher burden of proof required for a preliminary injunction.").

[71] *See, e.g.*, Randy Barnett, *Why the NSA Data Seizures Are Unconstitutional*, 38 HARV. J.L. & PUB. POL'Y 3, 8–9 (2015) (distinguishing *Smith v. Maryland* and mass collection on particularity grounds); Bedi, *Facebook*, *supra* note 5 (using interpersonal privacy rights to protect social networking communications); Cásarez, *supra* note 69, at 850–53 (applying First Amendment to protect bulk collection of domestic communications metadata); David

More recently, courts and scholars have struggled with how the third party doctrine should apply in the context of the government acquiring historical cell site location data.[72] I will address this unique situation in greater detail below.[73] The purpose of this Article, however, in the end is not to fully debate and resolve the merits of Fourth Amendment protection in these various technology-based contexts. Rather, the key takeaway is to recognize that the third party doctrine conceptually is not limited by the nature of the disclosure (it can potentially apply to voice conversations, physical information, electronic data, etc.) nor to whom it is disclosed (it can potentially apply to individuals, companies, ISPs, etc.).[74]

B. History of Public Disclosure Doctrine

1. Visual Observation of Public Information

The first cases of the public disclosure doctrine centered on visual observation by police in public. In *Hester v. United States*,[75] the Court found no issue with police observing the movements of the defendant or the items carried by him outside his home from a distance away.[76] Because the defendant's actions were out in the open for all to see, these movements garnered no Fourth Amendment protection.[77] This

---

Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013) (using a technology-centered approach to quantitative privacy to protect against government collection of mass data).

[72] *See* discussion *infra* Section III.B.

[73] *See* discussion *infra* Section III.B.

[74] The Court seems to have carved out an exception to the third party doctrine for certain disclosures conveying content as opposed to non-content information. *Compare Ex parte* Jackson, 96 U.S. 727, 733 (1878) (holding that letters and sealed packages cannot be opened unless the government obtains a warrant), *with* United States v. Van Leeuwen, 397 U.S. 249, 251–52 (1970) (finding that a 29-hour holding of suspicious First-Class packages was not unreasonable under the Fourth Amendment). *See also* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2162–63 (2009) (arguing that courts could limit the third party doctrine reasoning in *Smith* by applying it only to non-content information over the Internet); Bedi, *Facebook*, *supra* note 5. Lower courts have gone further to carve out exceptions for disclosures made to lawyers or medical providers. *See, e.g.*, Doe v. Broderick, 225 F.3d 440, 450–52 (4th Cir. 2000) (holding that detective's examination of a patient file held by a methadone clinic was a search and, without probable cause, violated the patient's Fourth Amendment rights); DeMassa v. Nunez, 770 F.2d 1505, 1508 (9th Cir. 1985) (holding that "an attorney's clients have a legitimate expectation of privacy in their client files").

[75] 265 U.S. 57 (1924).

[76] *Id.* at 58–59.

[77] *Id.* at 59 ("[T]he special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers, and effects,' is not extended to the open fields." (quoting U.S. CONST. amend. IV)).

became known as the public disclosure doctrine, which says that there is no privacy protection for a person's movements in public.[78]

The *Katz* reconceptualization and the introduction of Harlan's two-part test for reasonable expectation of privacy did not change the operation of this doctrine.[79] In that case, the government installed, without a warrant and unbeknownst to the defendant, a listening device in a phone booth that was used by the defendant to make illegal gambling calls.[80] The Court found that this recording violated the defendant's Fourth Amendment right to privacy and satisfied the now famous two-part test.[81] The defendant purposefully entered the telephone booth, shut the door behind him, and paid the toll that permits him to place a call.[82] The Court found that, collectively, these actions exhibited an expectation of privacy and that this belief was reasonable.[83] Thus, the government was required to obtain a warrant before intercepting the call.[84]

However, the Court also explained that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[85] In the instant case, the booth was partly constructed out of glass such that the defendant was visible in the same way before or after he closed the door and made the call.[86] The Court went on to say that the defendant sought to exclude the "uninvited ear," not the "intruding eye."[87] The implication here is that the police were free to observe the defendant through the glass without first seeking a warrant because that information (unlike the defendant's voice) was open for all the public to see.[88]

The Court has applied the public disclosure doctrine beyond what a police officer can see from the ground to include visual surveillance from above. In *California v. Ciraolo*,[89] the police secured a private plane and flew over the defendant's home at an altitude of 1,000 feet and visually identified marijuana growing in the yard.[90]

---

[78] *See, e.g.*, New York v. Class, 475 U.S. 106, 114 (1986) ("The exterior of a car, of course, is thrust into the public eye, and thus to examine it does not constitute a 'search.'"); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (stating that "objects, activities, or statements that [a person] exposes to the 'plain view' of outsiders" do not receive Fourth Amendment protection).

[79] 389 U.S. at 359.

[80] *Id.* at 348.

[81] *Id.* at 359.

[82] *Id.* at 352 ("One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

[83] *Id.* at 361 (Harlan, J., concurring); *see id.* at 352 (majority opinion).

[84] *Id.* at 357–58 (majority opinion).

[85] *Id.* at 351.

[86] *Id.* at 352.

[87] *Id.*

[88] *See id.*

[89] 476 U.S. 207 (1986).

[90] *Id.* at 209.

The Court found that no warrant was required for this kind of surveillance.[91] Using the *Katz* two-part test, the Court first conceded that the defendant likely had a subjective intent of privacy because he erected a ten-foot fence to conceal the marijuana crop from street-level views.[92] However, the Court found this expectation unreasonable because the defendant voluntarily exposed his backyard to visual observation from publicly navigable airspace.[93]

The public disclosure doctrine also explains the Court's ruling on garbage placed outside an individual's residence. In *California v. Greenwood*,[94] the defendant placed his garbage in plastic bags and left them on the curb in front of the house.[95] The police searched the bags and found items indicative of narcotics.[96] Citing *Katz*, the Court found that even if the defendant subjectively thought that "there was little likelihood that [the bags] would be inspected by anyone," there was no reasonable expectation of privacy in the bag because defendant voluntarily "exposed the[ ] garbage to the public sufficiently to defeat [a] claim to Fourth Amendment protection."[97] The Court noted that the bags were left on the public street and were readily accessible to anyone including children, scavengers, and animals.[98]

While the holding relied on the public disclosure alone, it is interesting that the Court also seemed to reference an application of the third party doctrine.[99] The police officer in this case actually received the bags from the trash collector after asking him to collect the garbage and turn it over to the authorities.[100] The Court noted that the defendant "placed the[ ] refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through [defendant's] trash or permitted others, such as the police, to do so."[101] This is another way of saying that the defendant voluntarily disclosed the garbage to a third party—in this case the trash collector—and thus lost all Fourth Amendment protection to it. I will address situations where both doctrines can apply in greater detail below.[102] For now, it is enough to say that a proper application of either doctrine is sufficient to vitiate privacy protection.

---

[91] *Id.* at 215.

[92] *Id.* at 211.

[93] *Id.* at 213; *see also* Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that use of an aerial mapping camera to photograph an industrial complex does not implicate the Fourth Amendment because the property was susceptible to visual surveillance from above).

[94] 486 U.S. 35 (1988).

[95] *Id.* at 37.

[96] *Id.* at 37–38.

[97] *Id.* at 39–40.

[98] *Id.* at 40.

[99] *See id.*

[100] *Id.* at 37–38.

[101] *Id.* at 40.

[102] *See* discussion *infra* Section III.A.

2. GPS and Beyond

Technological advancements and the rise of big data—much like in the third party doctrine context—have complicated the application of the public disclosure doctrine. The first Supreme Court case to tackle enhanced surveillance technology beyond visual observation seems uncontroversial.

In *United States v. Knotts*,[103] the police lawfully placed a beeper inside a container of chemicals purchased by the defendant.[104] The beeper emitted a signal, which allowed the authorities to track the package for an entire afternoon.[105] Without first seeking a warrant, the police tracked the container as it was transported in two separate vehicles until it reached its destination, the defendant's cabin.[106] In applying the public disclosure doctrine and finding no Fourth Amendment protection here, the Court reasoned:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction . . . .[107]

It did not matter that, without the beeper system, the police would not have been able to maintain visual observation of the defendant to his ultimate destination.[108] The Court noted that this technological advancement simply augmented traditional visual surveillance by providing a more efficient means to monitor a defendant's movements through public streets.[109] The Court, however, specifically left open the possibility of a different constitutional conclusion if the surveillance had lasted for a full day or longer.[110]

---

[103] 460 U.S. 276 (1983).

[104] *Id.* at 278.

[105] *Id.*

[106] *Id.*

[107] *Id.* at 281–82.

[108] *Id.* at 282 ("The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of [the defendant's] automobile to the police receiver, does not alter the situation.").

[109] *Id.* ("Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.").

[110] *Id.* at 283–84 ("[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." (citing Zurcher v. Stanford Daily, 436 U.S. 547, 566 (1978)).

The issue of long-term surveillance using a technological device finally reached the Court in its most recent decision on the public disclosure doctrine and new technology. In *United States v. Jones*,[111] the government—without the consent or knowledge of the defendant or under the terms of a warrant—installed a Global Positioning System (GPS) device under his car and tracked his public movements with the device for nearly thirty days.[112] The Court (both the majority and concurrences) wrestled with how this government activity could fall under the scrutiny of the Fourth Amendment when the public disclosure doctrine mandated that none of this surveillance would garner constitutional protection.[113]

The majority focused on the initial act of placing the GPS device under the car as constituting an unlawful physical trespass without reaching the issue of the surveillance itself.[114] Though it bypassed a direct analysis of the potential application of the public disclosure doctrine in this context, the majority did note that any such discussion would lead to a host of "particularly vexing problems" on the nature of visual observation versus technologically enhanced surveillance, and the problem of drawing lines between what constitutes short-term from longer-term surveillance.[115]

However, the concurring opinions took this issue head on. Both Justices Sotomayor and Alito found that a straightforward application of the public disclosure doctrine was not appropriate given the length of surveillance and the technology employed.[116] "I would ask," explained Justice Sotomayor, "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[117] She felt that the net result of this long-term GPS monitoring may chill "associational and expressive freedoms" and fundamentally

---

[111] 565 U.S. 400 (2012).

[112] *Id.* at 402–03 (the GPS ultimately "relayed more than 2,000 pages of data over the 4-week period").

[113] *Id.* at 404–13; *id.* at 413–18 (Sotomayor, J., concurring); *id.* at 418–31 (Alito, J., concurring).

[114] *Id.* at 404–05 (majority opinion) ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'"). The majority went on to say:

> [E]ven assuming that the concurrence is correct to say that "[t]raditional surveillance" of Jones for a 4-week period "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.

Id. at 412 (alteration in original) (internal citation omitted).

[115] *Id.* at 411–12 (quoting *id.* at 426 (Alito, J., concurring)).

[116] *Id.* at 416 (Sotomayor, J., concurring); *id.* at 428–30 (Alito, J., concurring).

[117] *Id.* at 416 (Sotomayor, J., concurring).

"alter the relationship between citizen and government in a way that is inimical to democratic society."[118]

Along the same lines, Justice Alito expressed concern over the government's unfettered ability to conduct long-term monitoring using GPS technology.[119] He explained that the facts here arose from the use of new surveillance technology and that prior to the computer age, this type of extended police surveillance would not have been possible.[120] While he recognized reasonableness is a moving target shaped by technological advancements, he concluded that, for now, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[121]

These arguments by Justices Sotomayor and Alito more generally have come to be known as the mosaic theory.[122] The basic premise of the theory is that even though the individual or discrete movements lose protection because of their exposure to public view, the aggregation of these movements via enhanced technology may constitute something worthy of Fourth Amendment protection.[123]

This type of dragnet surveillance is not limited to GPS technology. The rise of comprehensive surveillance—through public cameras and unmanned drones—may suggest other applications of the mosaic theory to combat the public disclosure doctrine.[124] Government cameras are already in public areas and have the ability to capture a large amount of a person's movements.[125] Drone use—which continue to grow in size—may pose even a greater threat to privacy.[126] These devices have advanced capability to covertly and constantly capture all public movements with greater precision and magnification.[127] Scholars have debated if the mosaic theory or some

---

[118] *Id.* (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

[119] *Id.* at 428 (Alito, J., concurring).

[120] *Id.* at 429.

[121] *Id.* at 430.

[122] *See* Bedi, *Mosaic Theory*, *supra* note 59, at 1810–11.

[123] *See, e.g.*, *id.* at 1810–11, 1834–48.

[124] *See, e.g.*, Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527 (2017).

[125] *See, e.g.*, *id.* at 539–42 (noting the dramatic advances in camera technology, including facial recognition); Afsheen John Radsan, *The Case for Stewart over Harlan on 24/7 Physical Surveillance*, 88 TEX. L. REV. 1475 (2010) (discussing potential of constant monitoring by law enforcement using public cameras).

[126] *See, e.g.*, Gregory S. McNeal, *Drones and the Future of Aerial Surveillance*, 84 GEO. WASH. L. REV. 354, 357 (2016) ("Some estimate that 30,000 drones will be flying in the national airspace ('NAS') by the end of the decade, while others suggest that as many as one million drones will be sold in 2015 alone." (citations omitted)).

[127] *See, e.g.*, Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 31, 33 (2013);

other limiting principle may provide Fourth Amendment protection for this kind of law enforcement surveillance that seemingly falls outside of constitutional scrutiny.[128] My purpose is not to fully assess the merits of the public disclosure doctrine in these new contexts but simply recognize that emerging surveillance technology and its ability to observe large amounts of information with advanced precision may impact how we apply this doctrine.[129]

C. The Doctrines as a Single Principle

On a number of occasions, the Court has discussed the disclosure doctrines as embodying a single or unified expression of privacy or lack thereof. *United States v. Knotts*—a case dealing with surveillance of public movements—provides such an example.[130] Here, the Court discussed and cited to *Smith v. Maryland*—a case involving the third party doctrine—in support of its finding that public movements garner no Fourth Amendment protection.[131] The Court detailed the circumstances and findings in *Smith v. Maryland* as constituting the "factual counterpart" to the public movements at issue in the *Knotts* case.[132]

Kyllo v. United States[133] provides another illustration. The issue in that case centered on the constitutionality of a thermal imaging device the police had set up across from the defendant's house to detect heat emanating from his home.[134] The

---

Gray & Citron, *supra* note 71, at 105–06; Jake Laperruque, *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance*, 51 U. RICH. L. REV. 705, 706–11 (2017); Levinson-Waldman, *supra* note 124, at 542–44.

[128] *See, e.g.*, Marc Jonathan Blitz et al., *Regulating Drones Under the First and Fourth Amendments*, 57 WM. & MARY L. REV. 49 (2015) (using the Fourth Amendment to constitutionally limit government use of drone surveillance); Gray & Citron, *supra* note 71, at 101–03 (using a technology-centered approach to limit the impact of public disclosure doctrine on Fourth Amendment protection); Laperruque, *supra* note 127, at 722–26 (distinguishing naked-eye observations from observations via technology to limit the impact of public disclosure doctrine); Levinson-Waldman, *supra* note 124, at 555–79 (incorporating mosaic theory with multifactor approach to limiting public surveillance). Others focus on statutory or legislative remedies to limit this kind of surveillance. McNeal, *supra* note 126, at 394–95.

[129] This type of inquiry—the impact of technology on the application of the disclosure doctrines—has historical roots in early Fourth Amendment cases. *See, e.g.*, United States v. White, 401 U.S. 745, 790 (1971) (Harlan, J., dissenting) ("The Fourth Amendment does, of course, leave room for the employment of modern technology in criminal law enforcement, but in the stream of current developments in Fourth Amendment law I think it must be held that third-party electronic monitoring, subject only to the self-restraint of law enforcement officials, has no place in our society.").

[130] 460 U.S. 276 (1983).

[131] *Id.* at 283 (citing Smith v. Maryland, 442 U.S. 735, 744–45 (1979)).

[132] *Id.* (citing *Smith*, 442 U.S. at 744–45).

[133] 533 U.S. 27 (2001).

[134] *Id.* at 29.

Court ultimately found that this government activity did trigger Fourth Amendment protection and that the public disclosure doctrine did not apply.[135] Because there was no evidence or contention that the defendant was aware of this device, there would be no possible application of the third party doctrine.[136] Nevertheless, as part of its analysis, the Court listed *Smith v. Maryland* together with two aerial surveillance cases as expressing the same reasonable expectation of privacy test.[137] The dissent, in finding that the heat was simply something that the defendant exposed to the public, also cited to *Smith v. Maryland* in the same sentence as an aerial surveillance case when discussing the inferences within a home.[138]

To the extent these exemplars seem indirect or somewhat exaggerated, *United States v. Jones* stands as a more direct and explicit instance of the conflation of the two doctrines. As explained above, this case only dealt with the public disclosure doctrine and the surveillance of an individual through public streets.[139] Justice Sotomayor, in her concurrence, discussed the problems with this kind of long-term monitoring.[140] At the conclusion of her opinion, she added a puzzling a part about the third party doctrine—a seeming non sequitur. She argued:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[141]

It is not clear why she referenced *Smith v. Maryland* and these specific disclosures. All of them—phone numbers, texts, emails, medications, books—squarely implicate the third party doctrine but have nothing to do with observing public movements,

---

[135] *Id.* at 31–34. The Court distinguished this case from the aerial surveillance cases on the grounds that the thermal imaging device (which was not in general public use) went beyond naked-eye surveillance and revealed information within a person's home that would otherwise have required physical intrusion. *Id.* at 33–38.

[136] *See id.* at 32–33 (citing Florida v. Riley, 488 U.S. 445 (1989); California v. Ciraolo, 476 U.S. 207, 211 (1986); *Smith*, 442 U.S. at 743–44).

[137] *Id.* at 33.

[138] *Id.* at 44 (Stevens, J., dissenting) (citing *Smith*, 442 U.S. 735).

[139] *See supra* notes 111–14 and accompanying text.

[140] United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring).

[141] *Id.* at 417 (citing *Smith*, 442 U.S. at 742; United States v. Miller, 425 U.S. 435, 443 (1976)).

which was the issue in the case.[142] It is interesting that she introduces this argument by the phrase "[m]ore fundamentally," which seems to suggest that the third party doctrine somehow underlies both disclosure doctrines.

Scholars too (admittedly, including me) have associated the doctrines as expressing one principle when assessing the merits of their application. Professor Stephen Henderson, for example, makes a compelling case for establishing a multifactor test to limit the application of the third party doctrine.[143] While the merits of the argument are not relevant here, it is interesting that he classifies cases like *Knotts*—which only involve visual surveillance—as falling under the third party doctrine calculus.[144] Professor Katherine Strandburg, in arguing for expanded Fourth Amendment privacy protection for use of the internet from the home, devotes a section on the pitfalls of the third party doctrine in which she includes cases dealing with informants, garbage, aerial and GPS surveillance.[145] Professor Matthew Tokson provides a conceptual framework for assessing the knowledge or voluntary requirement in the disclosure doctrine contexts but, in doing so, associates the third party and the public disclosure doctrines as representing a single principle of exposure and loss of privacy protection.[146] In crafting a constitutional theory using the mosaic theory to protect social networking communications on the Internet, I similarly discuss the two doctrines as analogs of each other as part of my argument to assess the merits of privacy protection in these situations.[147]

On one level this close association by the Court and scholars is understandable. Both doctrines can be seen as waiver or consent principles. Under this interpretation, an individual "consents or waives her right to Fourth Amendment protection by disclosing the information to another person or disclosing her movements to the public at large."[148] And, "[i]t is not relevant that the individual makes this disclosure thinking that the information or her movements will remain private."[149] While both doctrines thus contemplate an assumption of risk by the individual, the specific risk

---

[142] *Compare* discussion *supra* Section I.A, *with* Section I.B.

[143] *See generally* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011).

[144] He also cites to *United States v. Maynard*, 615 F.3d 544, 555–58 (D.C. Cir. 2010), the D.C. Circuit opinion upon which *United States v. Jones* is based. *See* Henderson, *supra* note 143, at 43.

[145] Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 633–36 (2011).

[146] *See* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139 (2016) [hereinafter Tokson, *Knowledge*]; *see also* Fabio Arcila, Jr., *GPS Tracking out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 37–42 (2012) (discussing implications of *United States v. Jones* by explicitly linking *Smith v. Maryland* and *United States v. Miller* to the surveillance cases as foundational cases).

[147] *See* Bedi, *Mosaic Theory*, *supra* note 59, at 1820–31, 1843–45.

[148] *See id.* at 1826.

[149] *Id.*

involved is quite different. In the third party scenario, the individual assumes the risk that the person to whom she discloses the information will reveal it to the government. In the public disclosure scenario, the individual assumes the risk that her public movements are being contemporaneously surveilled by the government.[150]

Other scholars perhaps have done a better job of identifying these as two distinct principles. Professor David Gray, in a recent book on police surveillance, devotes a separate section to each of the disclosure doctrines and seems to recognize their unique contours.[151] What is missing from his work, however, is a doctrinal framework for when these respective doctrines apply. This Article fills this important gap by articulating the key elements that trigger the application of each doctrine.

II. THE UNIQUE REQUIREMENTS OF THE RESPECTIVE DISCLOSURE DOCTRINES

A. Trigger for Third Party Doctrine

A proper application of the third party doctrine contemplates three things: (1) there is a voluntary disclosure (2) of non-public information to a third party (3) from which the government acquires the information.[152] The first requirement is relatively straightforward. In all the aforementioned third party cases—disclosing verbal conversations, phone numbers, financial records, etc.—the individual is voluntarily or knowingly providing the information to the third party.[153] These disclosures occur in the normal course of the interaction or business transaction.[154] In other words, coercing an incriminating statement by putting a gun to a suspect's head or otherwise threatening a person to hand over the information would in all likelihood not satisfy the voluntariness requirement.[155]

---

[150] *See* Arcila, *supra* note 146, at 38 ("The assumption-of-risk doctrine is particularly prevalent in the context of informants and co-occupants. The third party and assumption-of-risk doctrines played a central role in *Jones* because they led to the *United States v. Knotts* . . . ." (citations omitted)); Strandburg, *supra* note 145, at 635 ("The first, 'assumption of risk,' step of the third party doctrine argument is pervasive in Fourth Amendment law. It underlies cases such as those involving searches of garbage left for pickup, undercover policing and use of informants, and law enforcement 'flyovers' of residential areas." (internal citations omitted)).

[151] *See* GRAY, AGE OF SURVEILLANCE, *supra* note 2, at 78–89.

[152] *See* Bedi, *Mosaic Theory*, *supra* note 59, at 1813–15.

[153] *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979) (disclosing phone number during normal course of business); United States v. Miller, 425 U.S. 435 (1976) (disclosing financial records to bank); United States v. White, 401 U.S. 745 (1971) (disclosing information during personal conversations). I use the terms voluntarily and knowingly interchangeably. For a more detailed discussion on the voluntary or knowing requirements in the Fourth Amendment context, see generally Tokson, *Knowledge*, *supra* note 146.

[154] *See, e.g.*, *Miller*, 425 U.S. at 437–38 (discussing business transaction); *White*, 401 U.S. at 746–47 (discussing interactions).

[155] *See cf.* Schneckloth v. Bustamonte, 412 U.S. 218 (1973) (reasoning that proper consent to search requires voluntariness where defendant was not coerced by police).

The second element focuses on the fact that the information disclosed will most often be non-public. When it comes to incriminating statements, dialed phone numbers, and bank records, all of these items are private information that are not available to the public at large.[156] It is no accident that the Court talks about misplaced trust and assuming the risk of the third party disclosing the information to the government when discussing the effect of the doctrine.[157] If the information were otherwise publicly available, the individual generally would not be taking on any additional risk by disclosing to a third party.

I qualify this analysis because there can be instances (albeit infrequent) where public information—i.e., susceptible to visual surveillance—is disclosed to a third party. I already talked about the circumstances under which disposing of garbage can trigger the third party doctrine.[158]

A more recent example embodying new technology would be the use of Google Street View. Started in 2007, this application allows users to obtain pictures of streets and the exterior of residences.[159] While it doesn't allow for real-time observation, it does permit users to observe past images as if they were positioned from the vantage point of a pedestrian on-site.[160] The images are readily available to anyone.[161] It should come as no surprise then that law enforcement have used these historical images to investigate cases.[162] No one would suggest the police need a warrant or probable cause before making this inquiry.[163] An individual does not seem to have any reasonable expectation of privacy to these images.

The third party doctrine provides a doctrinal hook for why the government can use this service without any Fourth Amendment scrutiny. Here, an individual voluntarily discloses her movements or other information to Google when she is outside.

---

[156] *See* discussion *supra* Section I.A.

[157] *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 302–03 (1966).

[158] *See supra* notes 94–102 and accompanying text.

[159] *See* Mary G. Leary, *The Missed Opportunity of* United States v. Jones: *Commercial Erosion of Fourth Amendment Protection in a Post-Google Earth World*, 15 U. PA. J. CONST. L. 331, 350 (2012) (discussing the history of Google Street View and its capabilities); *see also Street View*, GOOGLE, https://www.google.com/maps/views/streetview [https://perma.cc/KD86-K2T8] (last visited Dec. 4, 2017).

[160] *See* Blitz et al., *supra* note 128, at 75; Leary, *supra* note 159, at 345–51; *Street View*, *supra* note 159.

[161] *See* Blitz et al., *supra* note 128, at 75; Leary, *supra* note 159, at 345–46.

[162] *See* Blitz et al., *supra* note 128, at 75 (citing instances where law enforcement used the application); Benjamin Fearnow, *Google Street View Images Catch Robbery Suspects in the Act 3 Years Later*, CBS HOUSTON (July 15, 2014, 2:06 PM), http://houston.cbslocal.com/2014/07/15/google-street-view-images-catch-robbery-suspects-in-the-act-3-years-later/ [https://perma.cc/MJ7H-8DCP].

[163] *See* Blitz et al., *supra* note 128, at 75–76. *But see* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 98–108 (2007) (arguing public camera surveillance should be limited based on First and Fourth Amendment grounds).

The government acquires the information no differently than telephone data or bank records. Given the prevalence of this Google technology and how long it has been in existence, an individual is on constructive notice that her public movement/activities are being stored by the company, much like an individual is on notice that the phone company will store the numbers one dials.[164] An individual therefore assumes the risk that the images may find themselves in the hands of the government.[165]

The third requirement—that the government acquires the information from the third party—is critical to a proper application of the doctrine. This feature underscores the assumption of risk analysis discussed above.[166] The point here is that the third party (e.g., telephone provider, informant, Google) at the behest of the government will hand over the information, not that the government will acquire the information directly bypassing the third party altogether. Indeed, the Court's most recent case on technology and Fourth Amendment protection confirms this requirement. In *Riley v. California*,[167] the Court ruled that a police officer could not search phone numbers on a cell phone as part of a search incident to the arrest of a recent car occupant.[168] It specifically cited *Smith v. Maryland* as inapposite precedent to support searching a cell phone in this instance.[169] This is because the police officer would be looking through the dialed numbers directly (thus, not satisfying element (3)) instead of obtaining the numbers from the cell phone provider.[170]

B. Trigger for Public Disclosure Doctrine

A proper application of the public disclosure doctrine requires three things: (1) there is a voluntary disclosure (2) of movements/items that are susceptible to

---

[164] *See cf.* United States v. White, 401 U.S. 745, 749 (1971) (finding defendant had no Fourth Amendment protection—because of third party doctrine—to conversations simultaneously transmitted to police agent even though defendant not aware of second agent). The third party doctrine, *a fortiori*, provides a doctrinal justification for why a person loses all privacy protection to a public item or movement photographed or otherwise witnessed by a neighbor that the government thereafter requests to be introduced at trial. Individuals are on constructive notice that their public actions may be observed/photographed by fellow citizens. The public disclosure doctrine may possibly provide a separate basis for why this kind of public activity does not garner privacy protection. *See supra* notes 159–63 and accompanying text.

[165] Even if an individual subjectively believes that their public activities will not be captured by Google or be captured for a limited purpose not related to law enforcement, this belief would not be reasonable. *See supra* notes 38–73 and accompanying text (discussing the operative facts in *Smith v. Maryland* and *United States v. Miller* and unreasonableness of any subjective expectation to privacy of information disclosed to third parties).

[166] *See supra* notes 148–50 and accompanying text.

[167] 134 S. Ct. 2473 (2014).

[168] *Id.* at 2485 (finding that the unique nature of electronic data on cell phones forecloses the rationale for allowing search incident to arrest of phone numbers and other data without a warrant).

[169] *Id.* at 2492 (citing Smith v. Maryland, 442 U.S. 735 (1979)).

[170] *See id.* at 2492–93.

public observation and (3) the government is contemporaneously monitoring the movements/information.[171] The first requirement tracks the first requirement of the third party doctrine. An individual must voluntarily or freely make the disclosure. However, unlike the third party doctrine, there is no requirement of a knowing disclosure to a third party.

The second requirement simply focuses on the public nature of the act. The individual must make a certain movement (e.g., walking outside or driving her car) or expose certain property (e.g., garbage on the outside) under circumstances that make this activity/property susceptible to visual surveillance by the public.[172] Locations that are private would not fall under the public disclosure doctrine. For example, in *United States v. Karo*,[173] the Court found that beeper monitoring within the home did not trigger the public disclosure doctrine because these movements could not be "visually verified."[174]

This requirement does not mean, however, that the government must *actually* visually observe the action. All that matters is that the activity is capable of being visually observed. For example, in *Knotts* and *Jones*, the defendant's car was not always under visual surveillance by the police but these movements were always potentially observable.[175] It is worth noting that analyzing *Knotts* or *Jones* using the third party doctrine comes out differently. Since neither suspect was aware of the beeper or GPS device and its emanating signal,[176] neither could have voluntarily disclosed his movements to the government. The public disclosure doctrine thus does not implicate the same issues of *how* the government obtains the information. The reason for this is because the public nature of the movements (e.g., the car's location) serves as the critical factor.

The third requirement, however, is the key trigger. In all the above-mentioned cases applying the public disclosure doctrine, the government was monitoring the movements or items while they were susceptible to visual observation.[177] This kind of contemporaneous government surveillance can happen by street observation,[178] from above by plane,[179] or via some type of monitoring device.[180]

Greenwood, or the garbage disposal case, may be a little trickier but it ultimately follows the same pattern.[181] The government (or its agent) still observes the property

---

[171] *See* discussion *supra* Section I.B.1.

[172] *See* Bedi, *Cell Phone Location Data*, *supra* note 4, at 514.

[173] 468 U.S. 705 (1984).

[174] *Id.* at 715.

[175] United States v. Jones, 565 U.S. 400, 402–03 (2012); United States v. Knotts, 460 U.S. 276, 278–82 (1983).

[176] *Jones*, 565 U.S. at 402–03; *Knotts*, 460 U.S. at 278–82.

[177] *See* discussion *supra* Section I.B.

[178] Hester v. United States, 265 U.S. 57, 58–59 (1924).

[179] California v. Ciraolo, 476 U.S. 207, 209 (1986).

[180] *Jones*, 565 U.S. at 402–03; *Knotts*, 460 U.S. at 278–82.

[181] 486 U.S. 35 (1988).

(i.e., takes it from the curbside) while it is susceptible to visual surveillance.[182] It just so happens that the disposal of garbage on the streets keeps the property in visual observation for a lengthy period of time until the government takes it.

In this way, until element (3) happens, the individual's actions or property are not subject to the public disclosure doctrine and the defendant has the ability to thwart its application.[183] For example, an individual could take her disposed garbage back inside the house or remove the marijuana from the front yard before a law enforcement officer observes or otherwise monitors the property. At that point, the items are no longer publicly available—i.e., susceptible to visual observation—and the government will need to obtain a warrant before searching for them.[184] Similarly, if a person returns home after a public outing without the government monitoring her movements, these movements would no longer be public and cannot be acquired without first seeking a warrant.[185] In the end, this limitation makes sense. Once the very thing that places these items or movements outside the purview of the Fourth Amendment—i.e., their public status—is no longer present, the public disclosure doctrine does not apply.[186] To hold otherwise, would mean that anytime something is publicly disclosed, even if for a brief moment, it is permanently without privacy protection. Not only is this conclusion not supported by the relevant case law, but also it would have unwanted implications for Fourth Amendment protection.[187]

III. BIG DATA AND APPLYING THE DISCLOSURE DOCTRINES

A. Two Different Concepts—Two Different Analyses

Scholars arguing for the elimination or limitation of the disclosure doctrines in light of today's technological advancements have generally analyzed them as a package

---

[182] In this case, the garbage collector was working with the government. *Id.*; *see* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (noting that the Fourth Amendment applies to private individuals working on behalf of the government); *supra* notes 94–102 and accompanying text.

[183] *See supra* discussion at Section I.B.

[184] *See* U.S. CONST. amend. IV.

[185] How these movements would be memorialized in a way that can subject someone to a warrant is a different issue.

[186] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* discussion *supra* Section I.B.

[187] Certain personal characteristics, however, such as the tone and manner of person's voice, their facial characteristics, or handwriting, are always considered publicly available and the government thus can freely ask a person to create or present them without Fourth Amendment scrutiny. United States v. Dionisio, 410 U.S. 1, 14 (1973). Because these things are constantly exposed to the public, as the Court explained, "[n]o person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world." *Id.* This carve out seems reasonable given the unique nature of these personal characteristics which are indelible to the way a person presents herself to the world in a way that items or movements temporarily exposed to the public are not.

deal.[188] But as two unique doctrines with unique triggers, they can be analyzed (and thus constrained) separately.

One of the current controversies surrounding the third party doctrine is whether the individual "voluntarily" transmitted the information to the third party. The disclosures in *Smith v. Maryland* and the informant cases seem noncontroversial.[189] Things get trickier, however, when you include the myriad of disclosures (e.g., emails, phone numbers, cell site location data, public street images) we make every day to companies and ISPs.[190] While individuals are certainly not coerced to make these disclosures, can they really be considered voluntary given how ubiquitous and necessary these actions have become? This was Justice Sotomayor's point in *Jones* regarding the need to reconsider the viability of the third party doctrine.[191] Scholars, too, have questioned whether today's disclosure to these various entities and companies are really voluntary.[192]

Resolution of this issue—while certainly an important question—does not bear on the voluntariness element in the public disclosure case. It is not a disclosure to a person or entity that vitiates privacy (in fact, the defendants in the cases cited generally have no idea that the government is tracking them) but rather voluntarily making oneself or an item susceptible to visual observation.[193] This kind of assessment is more straightforward and less controversial because individuals more easily know when their activities are visually observable. However, this doctrine invokes its own distinct privacy concerns and issues. Should public locations always be susceptible to government monitoring? Can surveillance be too long such that it impedes on individual privacy? Enter the mosaic theory as a means to limit the application of the public disclosure doctrine when it comes to long-term surveillance.[194]

---

[188] *See supra* notes 143–51 and accompanying text.

[189] *See, e.g.*, *supra* note 66 and accompanying text.

[190] I will discuss the specific issue of cell phone site location data in greater detail in Section III.B.

[191] *See* United States v. Jones, 565 U.S. 400, 413–18 (2012) (Sotomayor, J., concurring); *supra* notes 116–23 and accompanying text.

[192] *See* Tokson, *Knowledge*, *supra* note 146, at 171–76 (discussing problems with the Court's analysis of the knowing or voluntary disclosure requirement in light of new technologies and the myriad of disclosures individuals make, including emails, phone number, and cell site location data). Integral to this analysis would naturally include a discussion of nature of the data (e.g., content vs. non-content disclosed). *See also* GRAY, AGE OF SURVEILLANCE, *supra* note 2; Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/Non-Content Distinction*, 54 SANTA CLARA L. REV. 821 (2014) (arguing that the content/non-content distinction should be abandoned in the third party doctrine context).

[193] *See* discussion *supra* Section I.B.1. Unlike in the third party context, the nature of the information exposed to the public (either content vs. non-content) is not relevant. The public disclosure doctrine applies to any information that is voluntarily disclosed to the public at large. *See* discussion *supra* Section I.B.

[194] *See* Bedi, *Mosaic Theory*, *supra* note 59, at 1810–11; *supra* notes 122–26 and accompanying text.

Scholars, however, have pointed out the difficulty in applying this theory in the context of public surveillance.[195] How long is too long?[196] Does it matter if there is delay in surveillance?[197] And what surveillance methods count toward the mosaic?[198] Answering these questions (while important) do not bear on the elements of third party doctrine and its proper scope.

I am not suggesting that the mosaic theory cannot also be applied to curtail the impact of third party doctrine (even though it originated to combat the public disclosure doctrine). It can. Some scholars have argued that the government should similarly be limited in its collection of big data such as phone records or other digitally stored information.[199] My point is simply that the Court can restrict one doctrine (via the mosaic theory or some other limiting principle) without interfering with the full application of the other or vice versa.

Perhaps most important, these two doctrines do not stand or fall together. The Court could get rid of one doctrine without disturbing the effect of the other. For example, as some have argued (including Justice Sotomayor), the third party doctrine should not have a place in today's technological world where disclosures to various entities and individuals have become ubiquitous.[200] This conclusion may have its own repercussions for law enforcement investigative techniques but it does not impact the application of the public disclosure doctrine.[201] While police would have to get a warrant before acquiring any information from a third party, they would continue to be free to publicly surveil individuals without any restrictions. One could also advocate for the converse. The Court could get rid of the public disclosure doctrine (thus requiring police to get a warrant before surveilling anyone) but keep intact the full effect of the third party doctrine.

There may also be instances (albeit infrequent) where both doctrines could potentially apply. This would encompass situations where public information is disclosed to a third party. I have already referenced the case of an individual disposing

---

[195] *See, e.g.*, Bedi, *Mosaic Theory*, *supra* note 59, at 1845–48; Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 333–36 (2012).

[196] *See* Kerr, *supra* note 195, at 333.

[197] *Id.* at 334.

[198] *Id.* at 334–35.

[199] *See, e.g.*, David Gray et al., *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 765–68, 785–88 (2013) [hereinafter Gray et al., *Fighting Cybercrime*] (discussing how the mosaic theory could protect the collection of aggregated digital data).

[200] *See* United States v. Jones, 565 U.S. 400, 417 (Sotomayor, J., concurring); Henderson, *supra* note 143, at 39–40 (celebrating that the Third Party Doctrine "has at least taken ill, and it can be hoped it is an illness from which it will never recover"); *see also supra* notes 166–68 and accompanying text.

[201] *See* Bedi, *Mosaic Theory*, *supra* note 59, at 1843 (discussing how getting rid of third party doctrine may frustrate long standing investigative techniques including, for example, use of undercover informants or gathering documents from a third party without a warrant or probable cause).

of garbage on the street as potentially triggering both doctrines.[202] The use of Google Street View by police presents a more recent example, albeit a controversial application.[203] In addition to the third party doctrine, one could argue for a possible application of the public disclosure doctrine as a separate means of vitiating privacy. At the time Google took the picture, the first two elements of the public disclosure doctrine seemed to apply, namely an individual voluntarily made her movements susceptible to visual observation.[204]

The sticking point, however, would be element (3) since a private company—not the government—is conducting the surveillance at the moment the location is publicly available. Unlike the disposed garbage scenario, the government only enters the equation—by formally requesting that Google hand over the images—after the location is no longer public.[205] Is contemporaneous government (rather than private) surveillance necessary for triggering this doctrine? In the Google hypothetical, an answer is not consequential since the third party doctrine already vitiates privacy protection.[206] But what if it were a different company that was taking the street pictures and it was not readily known to the public? Perhaps, Amazon has a secret drone program that unbeknownst to the public, surveils the streets of most major cities.[207] If the government requests this data from Amazon a person's movements are no longer public; does the Fourth Amendment apply? Here, unlike in the Google Street hypothetical, there most likely would be no application of the third party doctrine because the individual is not reasonably aware (either actually or constructively) that her movements are being monitored by Amazon.[208]

---

[202] California v. Greenwood, 486 U.S. 35, 37 (1988); *see supra* notes 94–98 and accompanying text.

[203] *See supra* notes 159–65 and accompanying text.

[204] *See supra* notes 159–65 and accompanying text.

[205] It is worth pointing out that if Google on its own delivered the images to the police—without any influence or the behest of government—the Fourth Amendment would not be implicated because there would be no state action. *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921) ("The Fourth Amendment gives protection against unlawful searches and seizures, and . . . protection applies to government action.").

[206] Either doctrine thus is sufficient to vitiate privacy protection. Take the *Knotts* case. There, third party doctrine does not even apply because the suspect—lacking knowledge of the beeper—could not possibly have voluntarily conveyed his location to the government. United States v. Knotts, 460 U.S. 276, 284–85 (1983). This fact was not relevant to the lack of privacy protection because the suspect's public movements and the direct government surveillance of them fell directly under the public disclosure doctrine. *Id.* at 281–82. In the Google hypothetical, it is the reverse. While it is not clear whether the elements of the public disclosure are fully satisfied, the triggers for the third party doctrine are present. *See supra* notes 159–65 and accompanying text.

[207] *See generally Amazon Prime Air*, AMAZON, https://www.amazon.com/Amazon-Prime-Air/b?node=8037720011 [https://perma.cc/FWJ7-3MM7] (last visited Dec. 4, 2017) (describing Amazon's new air delivery system utilizing drone delivery technology).

[208] I qualify this statement because one could argue that today all individuals are

It is not readily apparent that the public disclosure doctrine applies in this unique context.[209] All the relevant public disclosure cases described above—human observation,[210] beeper tracking,[211] GPS long term monitoring,[212] aerial reconnaissance[213]—involve direct government surveillance of locations that are publicly available at that time. A definitive answer here ultimately depends on how one conceptualizes privacy in this context. Because the image was susceptible to visual surveillance, one could argue that as long as it was in fact observed or monitored at that time (regardless of whether by the government or a private entity), an individual loses all expectation of privacy. The government then is free to acquire it without a warrant.[214] On the other hand, one may argue that one only assumes the risk that the government—not a private entity without any law enforcement interest—is surveilling the activity at that time it is public. One does not assume the risk that the government will at a later date request a private party to hand over the data after it is no longer in public view. It would certainly be a significant change from the Court's jurisprudence to include surveillance by private actors as triggering the public disclosure doctrine.

Privacy advocates would no doubt push against this expansion and probably for good reason. This would allow the government to more easily acquire erstwhile public information from a third party on account of the fact that the government could bypass the third party doctrine's specific (and seemingly more rigorous) voluntariness requirement and rely instead on the more straightforward voluntariness requirement of the public disclosure doctrine. These scenarios of private surveillance of public movements are, thus, perhaps better left as potential applications of the third party doctrine, a doctrine that explicitly incorporates the role of third parties in the government's collection efforts.

B. The Curious Case of Cell Site Location Data

1. A Primer on Cell Site Location Data

The disclosure doctrines have become increasingly relevant in the government collection and monitoring of cell site location data. Cell phones use radio waves to connect to their service provider in order to facilitate a host of functions, including,

---

constructively on notice that someone or some company is always watching their public movements. *See supra* note 164 and accompanying text.

[209] The analysis would be easier if the government were working with Amazon to surveil individuals in real time through this technology because this activity would trigger the third element of contemporaneous government (sponsored) surveillance.

[210] Hester v. United States, 265 U.S. 57, 58–59 (1924).

[211] *Knotts*, 460 U.S. at 276–82.

[212] United States v. Jones, 565 U.S. 400, 402–03 (2012).

[213] California v. Ciraolo, 476 U.S. 207, 209 (1986).

[214] *See* U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347 (1967).

making/receiving phone calls, sending/receiving text messages, and using the internet.[215] Cell phone providers, in turn, maintain thousands of cell phone towers that receive these radio signals.[216] Cell phones emit these signals anytime they are turned on after which the nearest cell phone tower acquires the signal.[217] The signal moves from tower to tower as cell phone users change their location.[218] The location of the nearest cell tower is automatically transmitted to the cell phone provider anytime a user makes or receives a call or text message.[219] Cell phone providers collect and store this cell site location data as the normal part of their business of providing service.[220]

Law enforcement use this data in two primary ways. The first involves acquiring historical cell site data from the cell phone provider.[221] Police request that the cell phone provider provide authorities a set of location data for a suspect relating to a specific period of time in the past.[222] Police can then use this data to show that the suspect was in the general area where the crime was committed.[223] The second way involves surveilling a suspect with real-time cell site data.[224] Here, police request that cell phone providers transmit the current location of the cell tower for direct tracking purposes.[225]

---

[215] *See, e.g.*, State v. Earls, 70 A.3d 630, 636–37 (N.J. 2013) (discussing the basics of how cell site location data works).

[216] *Id.* at 637.

[217] *Id.*

[218] Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 702 (2011).

[219] United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016); United States v. Carpenter, 819 F.3d 880, 885 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402); *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 611–13 (5th Cir. 2013); *Earls*, 70 A.3d at 637–38.

[220] *Earls*, 70 A.3d at 637.

[221] *See* Patrick E. Corbett, *The Fourth Amendment and Cell Site Location Information: What Should We Do While We Wait for the Supremes?*, 8 FED. CTS. L. REV. 215, 217 (2015).

[222] *See, e.g.*, *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d at 614.

[223] *Id.*

[224] *See* Corbett, *supra* note 221, at 217.

[225] *See generally In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129 (E.D.N.Y. 2013). I recognize that as soon as the provider gives police the tower location, the data is, technically speaking, a historical location as it happened in the past (albeit a few seconds ago). The key distinction between historical versus real-time data is not the nature of the actual cell tower location but the fact that in the real-time context, the government is using this (historical) data to directly surveil the individual while her movements are public, much like in the *Jones* and *Knotts* cases described above (where the location via the GPS/beeper signal would also technically be historical in nature). *See supra* Section I.B.2. Police may also "ping" a cell phone as a variation of this real-time surveillance. Only this time, the government does not wait for the phone itself to send its routine signal to the cell tower. Rather, the police request that cell phone providers send an affirmative signal to the suspect's phone in order to directly monitor her cell site location. *See, e.g.*, *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d at 132–33.

2. How Courts Have Applied the Doctrines

While the Supreme Court has not ruled on the status of police use of cell site location data, the consensus amongst circuit courts appears to be that this government activity falls outside of the scope of the Fourth Amendment.[226] Most appellate courts that have addressed this issue have focused on historical cell site location data.[227] These decisions generally have relied on the third party doctrine and the precedent in *Smith v. Maryland* to find that the individual voluntarily discloses her location to the cell provider. The Fifth Circuit, for example, reasoned that a "cell service [user], like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call."[228] The court cited to evidence that a "cell service providers' and subscribers' contractual terms of service . . . expressly state that a provider uses a subscriber's location information to route his cell phone calls."[229] The Fourth Circuit similarly focused on the common knowledge of cell phone users in this context: "As most cell phone users know all too well, proximity to a cell tower is necessary to complete these tasks. Anyone who has stepped outside to 'get a signal,' or has warned a caller of a potential loss of service . . . understands, on some level, that location matters."[230] The Sixth Circuit similarly concluded "any cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower."[231]

Not all courts agree with this analysis. For example, the Third Circuit in finding that the third party doctrine does not apply, emphasized the lack of voluntariness.[232] It reasoned that a cell phone user does not "share[ ] his location information with a

---

[226] It appears that the Court has recently granted cert in *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402); *see also* Amy Howe, *Justices to Tackle Cell Phone Data Case Next Term*, SCOTUSBLOG (June 5, 2017, 12:52 PM), http://www.scotusblog.com/2017/06/justices-tackle-cellphone-data-case-next-term/ [https://perma.cc/SF3R-7D7N].

[227] *See, e.g.*, United States v. Graham, 824 F.3d 421 (4th Cir. 2016); *Carpenter*, 819 F.3d 880; United States v. Davis, 785 F.3d 498 (11th Cir. 2015); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600; *In re* Application of the U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010). Scholars too have analyzed how (if at all) the Fourth Amendment should apply to cell site location data. *See, e.g.*, Levinson-Waldman, *supra* note 124, at 536–39, 553–55; Tokson, *Knowledge*, *supra* note 146, at 159–63.

[228] *In re Historical Cell Site Data*, 724 F.3d at 613.

[229] *Id.*

[230] *Graham*, 824 F.3d at 430.

[231] *Carpenter*, 819 F.3d at 888. The court also focused on the fact that location data was non-content in nature much like the data in *Smith v. Maryland. Id.*

[232] *In re Application of the U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to Gov't*, 620 F.3d at 317.

cellular phone provider in any meaningful way . . . [as] it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information."[233] The court concluded that the customer only knowingly and voluntarily conveys the number to the cell phone provider.[234]

As discussed earlier, the issue of voluntariness pervades a discussion of the third party doctrine and new technologies.[235] Reasonable people can disagree on whether courts should find this disclosure to be a voluntary one.[236] My purpose here is not to settle this question in this context. I am more interested in the way courts have muddied the waters by interjecting a discussion of the public doctrine when talking about historical cell site location data.

The Fourth Circuit, for example, includes discussions of the public nature of the data in arguing against Fourth Amendment protection under the third party doctrine.[237] After applying *Smith v. Maryland*, the court seems to support its conclusion by noting that this location information is public in nature, quite different from the private information in *Karo* or *Kyllo*.[238] But the public nature of this data (or lack of it) is not relevant to an application of the third party doctrine.[239] To further confuse matters, in the next paragraph, the court seems to recognize that historical cell site data does not implicate "direct government surveillance" and the key issue is whether the government "invades an individual's reasonable expectation of privacy when it obtains, from a third party, the third party's records, which permit the government to deduce location information."[240]

The Sixth Circuit, too, seems to indirectly discuss the public disclosure doctrine.[241] It raises the potential application of *Jones* and long-term monitoring but ultimately distinguishes the case because cell site location data is less precise than GPS data.[242] But, the more pertinent distinction rests on the fact that the monitoring in *Jones* involved contemporaneous government surveillance in a way that the collection of historical location data does not.[243]

---

[233] *Id.*

[234] *Id.* at 317–18.

[235] *See* discussion *supra* Section I.A.2.

[236] *See, e.g.*, Monu Bedi, *Texting the Government Your Location*: *The Case of Historical Cell Phone Location Data and Fourth Amendment Protection*, CASETEXT (Aug. 26, 2015), https://www.casetext.com/posts/texting-the-government-your-location [https://perma.cc/CG33-2JND].

[237] United States v. Graham, 824 F.3d 421, 426 (4th Cir. 2016).

[238] *Id.* (citing Kyllo v. United States, 533 U.S. 27, 34–35 (2001); United States v. Karo, 468 U.S. 705, 714–15 (1984)).

[239] *See generally* discussion *supra* Section I.A.

[240] *Graham*, 824 F.3d at 426 (emphasis removed).

[241] United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402).

[242] The Sixth Circuit correctly noted that there was no trespass with the collection of cell site location as in the *Jones* case. *Id.*

[243] *See id.* at 895.

The Third Circuit's discussion of the public disclosure doctrine was more direct and consequential.[244] While it concluded that disclosing cell location data to the cell phone company was not voluntary—and thus the third party doctrine did not apply—it nonetheless found that the public disclosure doctrine did apply.[245] Citing *Knotts*, the Court explained:

> We cannot reject the hypothesis that [historical cell site location data] may, under certain circumstances, be used to approximate the past location of a person. If it can be used to allow the inference of present, or even future, location, in this respect [cell site location data] may resemble a tracking device which provides information as to the actual whereabouts of the subject. The *Knotts*/*Karo* opinions make clear that the privacy interests at issue are confined to the interior of the home. There is no evidence in this record that historical [cell site location data] . . . extends to th[is] realm. We therefore cannot accept the . . . conclusion that [this data] . . . requires probable cause for its production.[246]

The point here seems to be that historical cell site location data is similar in nature to tracking technologies that catalog a suspect's public location, which the court uses to explain why the public disclosure doctrine applies equally to both. But the critical distinction, again, between these two situations—and, in turn, a proper application of the public disclosure—rests on the fact that *Knotts* and *Karo* involved contemporaneous government surveillance, a feature not present in the historical location data context.[247] I address this issue in more detail below.

Real-time location data would appear to fall or stand with historical location data, at least when it comes to an application of the third party doctrine. This information, too, is "in fact, a stored, historical record because it [was] received by the cell phone service provider and stored, if only momentarily, before being forwarded to law enforcement officials."[248] For this reason, some courts have treated historical and real-time data the same way, finding no protection based on an application of the third party doctrine.[249]

---

[244] *See In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

[245] *Id.* at 313.

[246] *Id.* at 312–13 (citing United States v. Knotts, 460 U.S. 276 (1983)).

[247] *Id.*

[248] *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006).

[249] *See id.*; *see also* United States v. Wallace, 866 F.3d 605 (5th Cir. 2017); *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129 (E.D.N.Y. 2013).

3. Picking and Choosing Between the Doctrines

Courts seem to pick and choose whether they focus on the third party doctrine, public disclosure doctrine, or both when analyzing cell site location data. Part of the problem centers on the unique nature of this data. On the one hand, the government can treat it like the collection of non-public information, no different than dialed telephone numbers (think historical location data).[250] On the other hand, this data can also be seen as publicly available data that facilitates surveillance, no different than GPS monitoring (think real-time location data).[251]

Historically, the collection of non-public information and surveillance of public movements were neatly separated. Collection of bank records, telephone numbers, incriminating statements, are all information gathering activities of non-public data that have nothing to do with surveillance of the suspect's physical location.[252] On the other hand, use of beeper monitoring, aerial reconnaissance, GPS are all surveillance methods of a suspect's public movements that do nothing more than relay her physical location.[253]

Police use of cell site location data has blurred these lines, thus contributing to the inconsistent application of the disclosure doctrines.[254] Full resolution of Fourth Amendment protection in this context is beyond the scope of this Article. That said, it is important to understand the doctrinal reach of each disclosure doctrine in this unique area so that courts and scholars are in a better position to analyze privacy protection here.

Take the scenario of the government collecting historical cell site location data. The government acquiring this data stands on the same footing as the government acquiring a history of telephone numbers from the telephone company over a period of time. Both scenarios suggest a potential application of the third party doctrine. The critical question would be whether an individual *voluntarily* discloses her location information in the same way she discloses dialed phone numbers. For the reasons mentioned earlier, courts understandably can disagree on this issue. Assuming a voluntary disclosure, however, the other elements are satisfied.[255] Like the

---

[250] *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); *see also* discussion *supra* Section III.B.

[251] *See* discussion *supra* Section I.B.2.

[252] *See* discussion *supra* Section I.A.

[253] *See* discussion *supra* Section I.B. I recognize that location data (whether by GPS, beeper, or cell phone use) is also a type of information and so even in the second scenario, the government is technically "collecting information." But the key difference here is that this information (unlike telephone data) is susceptible to visual observation and facilitates surveillance of the suspect.

[254] *See* discussion *supra* Section I.B.2.

[255] Courts could still try to limit the full effect of the doctrine using the mosaic theory. *See supra* notes 191–95 and accompanying text.

phone numbers in *Smith v. Maryland*,[256] the government acquires the location data directly from the cell phone provider.[257] It isn't clear though why the Fourth Circuit focused on the public nature of the location data in its third party doctrine calculus.[258] It is the voluntariness of the disclosure that does the work, not whether the information is public or private.[259] In fact, most of the aforementioned third party doctrine cases have involved private information (e.g., cell phone numbers, conversations, and bank records).[260]

An application of the public disclosure doctrine in the historical cell site data context would be controversial.[261] The difficulty would be similar to the issue in my Amazon hypothetical. There is no government surveillance, only surveillance by a private entity. The government—much like in the Amazon case—only enters the picture after the fact when the location is no longer public. As previously explained, this application goes against prior precedent and potentially raises privacy concerns on the expansion of the government's ability to acquire information by bypassing the third party doctrine's voluntariness requirement. Before courts simply conclude that the public disclosure doctrine (and its related cases) should reach historical location data (as the Third Circuit, for instance, has done), they must first address these important doctrinal and related policy concerns.[262]

Real-time location data stands or falls together with historical data as far as an application of the third party doctrine.[263] With real time data, the government is similarly acquiring the information from the cell phone provider, only this time the focus is on recent locations as opposed to past ones.[264] Whether this doctrine applies here again depends on if the disclosure to the provider is considered to be a voluntary one.[265]

Real time location data, however, seems more likely to lose Fourth Amendment protection because of the public disclosure doctrine. Here, unlike the historical data scenario, all the three elements are satisfied. The police are monitoring the suspect's public location (via a cell tower location) at the same time the suspect's location is susceptible to visual observation.[266] The cell site location data in this context thus

---

[256] 442 U.S. 735 (1979).

[257] *See* discussion *supra* Section II.A.

[258] *See* United States v. Graham, 824 F.3d 421, 426 (4th Cir. 2016).

[259] The fact that the data, however, can be seen as non-content or metadata like phone numbers would be relevant to a third party doctrine calculus.

[260] *See* discussion *supra* Section I.A.

[261] The first two elements would be satisfied because the suspect voluntarily makes her location susceptible to public observation at the time the cell phone provider records it.

[262] *See, e.g.*, discussion *supra* Section III.B.2.

[263] Corbett, *supra* note 221, at 217.

[264] *Id.*

[265] *See* discussion *supra* Section II.A.

[266] I understand that the transmitted location is of the cell tower not the individual's specific public location. But this distinction is inconsequential since they both would be public

plays the same role as a GPS or beeper. All of these technologies are being used by the government to contemporaneously monitor the suspect's public movements. The only difference is that the government is acquiring the location from the provider rather than directly from the GPS or beeper.[267]

The difference in Fourth Amendment protection between real time data (*most likely not* protected under public disclosure doctrine) and historical data (*may not* be protected under the third party or public disclosure doctrines) makes sense when assessing the relative privacy concerns in each scenario. With stored data, the police can have easy access to significant amounts of location history without expending resources to gather it.[268] There is no practical limitation to the time frame they may acquire. This concern may militate in favor of having a more robust requirement of voluntariness under the third party doctrine so it is harder to acquire this information without Fourth Amendment protection. On the other hand, use of real-time data has some built in practical limitations making the need for Fourth Amendment protection perhaps less important. There is some cost to conducting this kind of surveillance. Police will have to expend resources to monitor a suspect's movements via cell towers, particularly long term surveillance. While cell phone technology—not unlike the GPS tracking in *Jones*—will certainly alleviate some of this work compared to traditional visual surveillance, officers will still need to do more work above and beyond simply requesting a set of historical locations from a provider.[269] Because of this built in cost, an application of the public disclosure doctrine (with its more easily satisfied voluntariness requirement) to real time cell site location data may not be as detrimental to privacy concerns.

CONCLUSION

This Article probably ends with more questions than it answers when it comes to the disclosure doctrines. How should we define voluntariness when applying the

---

locations and the former is simply a proximate location of the latter. It is also possible for the government to acquire historical location data for a period of time and, with that information, work with the cell phone provider to thereafter surveil the individual's public movements via cell towers. Constitutionally speaking, each activity—the initial collection of historical data and the subsequent contemporaneous monitoring—would be analyzed separately.

[267] For similar reasons, a situation where the government is monitoring cell tower location data by "pinging" an individual's cell phone would also likely not garner privacy protection. *See* United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004), *cert. granted*, *judgment vacated on other grounds*, *sub nom*. Garner v. United States, 543 U.S. 1100 (2005) (finding that even though third party doctrine did not apply because government, in collaboration with cell phone company, triggered the location transmission, the public disclosure doctrine vitiates Fourth Amendment because this real-time data was a proxy for the suspect's public locations).

[268] *See* Corbett, *supra* note 221, at 215–17.

[269] *Cf.* 565 U.S. 400, 430 (2012) (Alito, J., concurring) (discussing the relative expenditure of police resources for surveillance via GPS compared with traditional observation).

third party doctrine to new technologies? Does the kind of technology being used make a difference? Should the public disclosure doctrine be expanded to include private surveillance of an individual's public movements? Should the mosaic theory apply to one, both, or none of the disclosure doctrines? These are not easy questions, and I do not pretend to have all the answers. But before we can even begin to tackle these difficult issues, it is imperative we understand the historical context and unique contours of each doctrine. They are not the same thing, nor has the Court applied them in the same way. For prudential reasons, we must strive for a logical and cautious application of these principles that is firmly grounded in prior precedent. Otherwise courts as well as scholars risk muddying the waters and, in turn, making unnecessarily overly broad or erroneous conclusions on important privacy matters. This Article finally provides a workable topology towards this end from which we can intelligently discuss whether and how these disclosure doctrines should, or should not, apply to future technologies.