A Fourth Amendment Framework for the Future: Applying the Mosaic Theory to Digital Communications

AARON STEVENSON*

TABLE OF CONTENTS

* J.D. Candidate 2017, The Ohio State University Moritz College of Law; B.A., The Ohio State University. The author would like to dedicate this article to his father, the Honorable James F. Stevenson, Shelby County Common Pleas Court Judge, for instilling in him a passion and admiration for the law. The author would also like to thank Professor Ric Simmons and the *Ohio State Law Journal* staff for their invaluable advice and feedback on this piece.

I. INTRODUCTION

> *"[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."*[1]

Recent and rapid technological change requires the Supreme Court to update Fourth Amendment[2] jurisprudence for the twenty-first century.[3] Unfortunately, the Fourth Amendment is outdated for a world that relies on communications facilitated by third-party intermediaries. The protection (or lack thereof) of these communications sits on unsettled ground. Consider the following:

a. A text message sent to a friend letting her know you are on your way.
b. A two-month chain of emails sent to contractors building your new house.
c. A Facebook post updating your "friends" as you travel on vacation.
d. The search terms entered into your Google search in the past week.

Each of these illustrates a communication sent through an intermediary party. Do the senders have a reasonable expectation of privacy in these communications?[4] Federal courts are grappling with this question,[5] and the Supreme Court has provided no clear guidance on the issue.

---

[1] United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010).

[2] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue, but upon probable cause . . . .").

[3] *See infra* Part II.

[4] "Reasonable expectation of privacy" is the standard used when determining if a Fourth Amendment violation has occurred. *See infra* Part II.A.

[5] In a recent Fourth Amendment case, one judge stated: "[C]ellular (not to mention internet) communication has left courts struggling to determine if (and how) existing tests

Because of this uncertainty, privacy in digital communications currently lies at two extremes—neither of which produces desirable results. At one extreme, courts strictly apply the third-party doctrine and remove all privacy protections from digital communications.[6] Under this theory, the sender knowingly exposes information to a third-party and thus has no reasonable expectation of privacy over the communication. At the other extreme, courts distinguish between "address" and "content" information and determine privacy protection based on this classification.[7]

These competing solutions leave much to be desired. The first solution (the third-party doctrine) does not protect the many digital conversations Americans have in everyday life. The second solution extends the established address/content distinction too far, and may lead to problems that are more difficult to resolve in the future.

If the Supreme Court desires to protect digital communications (as it should), a much better solution is available: the mosaic theory. The mosaic theory finds that when law enforcement aggregates small amounts of information, it creates a clear picture of an individual's intimate details and thus violates an individual's reasonable expectation of privacy.[8] For example, one email may not possess a reasonable expectation of privacy, but many months of emails may collectively possess a reasonable expectation of privacy.

Applying the mosaic theory to digital communications strikes a middle ground between the two current extremes. This solution allows the third-party doctrine to remain intact, and simultaneously protects large amounts of information sent through digital intermediaries. Further, this solution presents a flexible framework that courts can apply to future technology.

Revising the Fourth Amendment framework for digital communications will have a lasting effect on the privacy enjoyed—or not enjoyed—in the coming decades. Future Fourth Amendment decisions will affect information stored in "the cloud;"[9] communications sent through social media platforms such as Facebook,[10] Snapchat,[11] and Tinder;[12] financial information sent through Venmo;[13] and forms of electronic communication not yet imagined.

---

apply or whether new tests should be framed." United States v. Carpenter, 819 F.3d 880, 894 (6th Cir. 2016) (Stranch, J., concurring); *see also infra* Part III.

[6] *See infra* Part III.A.

[7] *See infra* Part III.B.

[8] *See infra* Part II.B.

[9] "The cloud" is a phrase used to describe a network of servers that have the ability to run applications, deliver services, and store large amounts of data in connection with certain personal accounts. *See* Jess Fee, *The Beginner's Guide to the Cloud*, MASHABLE (Aug. 26, 2013), http://mashable.com/2013/08/26/what-is-the-cloud/#DcaJ.uiPJkqq [https://perma.cc/L7Q9-MZLP].

[10] Facebook is a social media platform that strives to connect friends and family. *See Company Info*, FACEBOOK NEWSROOM, https://newsroom.fb.com/company-info/ [https://perma.cc/TXA9-AJZB].

This Note examines digital communications and the feasibility of resolving current and future privacy issues using the mosaic theory. Part II surveys the background and development of Fourth Amendment jurisprudence. Part III examines the existing methods of analyzing digital communications and critiques those frameworks. Part IV proposes that courts use the mosaic theory to determine when the Fourth Amendment protects digital communications and addresses counterarguments to this approach. Part V concludes.

II. EXAMINING THE PAST TO SOLVE THE PROBLEMS OF THE FUTURE: A QUICK LOOK AT THE DEVELOPMENT OF FOURTH AMENDMENT JURISPRUDENCE

To examine the future of the Fourth Amendment, it is important to first understand the conceptual underpinnings of the Fourth Amendment.

A. Katz *and the Elusive Reasonable Expectation of Privacy*

The Fourth Amendment protects individuals from certain government searches; it ensures that law enforcement cannot enter the home, search mail, or arbitrarily seize property. However, the Fourth Amendment is not all-encompassing. Over the past century, the Supreme Court has defined the limits of Fourth Amendment protection.

Modern Fourth Amendment framework began in 1967 when the Supreme Court decided *Katz v. United States*.[14] In *Katz*, the Court departed from the traditional Fourth Amendment trespass analysis,[15] stating: "[T]he Fourth Amendment protects people, not places."[16] This is known as the "*Katz* Test."[17]

---

[11] Snapchat is an application that allows the user to send self-destructing photos to other users. *See* Elyse Betters, *What's the Point of Snapchat and How Does It Work?*, POCKET-LINT (Dec. 26, 2015), http://www.pocket-lint.com/news/131313-what-s-the-point-of-snapchat-and-how-does-it-work [https://perma.cc/W5LW-RFVM].

[12] Tinder is an online dating application that opens a line of communication between two individuals based on mutual attraction. *See* Antonio Borrello, *The Shocking Truth About Tinder; It's More than Just a Hook-up App!*, HUFFINGTON POST, http://www.huffingtonpost.com/antonio-borrello-phd/the-shocking-truth-about-_7_b_8011462.html [https://perma.cc/F56D-D5HU] (last updated Aug. 20, 2016).

[13] Venmo is a financial application that enables individuals to electronically transfer funds. *How It Works*, VENMO, https://venmo.com/about/product/ [https://perma.cc/TNQ7-SE28].

[14] Katz v. United States, 389 U.S. 347 (1967). In Katz, law enforcement placed a listening device on the outside of a telephone booth where Katz was making a call to discuss illegal wagering. *Id.* at 348. Under the traditional trespass doctrine, this would not be a Fourth Amendment violation because there was no trespass on Katz's property rights. *See id.* at 352–53.

[15] Until 1967, the Fourth Amendment only protected against government agents physically trespassing upon a suspect's property rights. *See* Olmstead v. United States, 277

The *Katz* Test asks if the government action violates an individual's "reasonable expectation of privacy."[18] The test is a two-part framework.[19] First, the defendant must have a subjective expectation of privacy in the area or item searched.[20] Second, society must deem it an objectively reasonable expectation of privacy.[21] The first prong is easily met,[22] while the second prong is difficult to define.[23] The Court has explained that the second prong examines "our societal understanding" of what deserves "protection from government invasion."[24] Although the societal understanding of privacy constantly evolves, the Court has established some general rules.

First, anything exposed to the public possesses no reasonable expectation of privacy.[25] Second, information that is knowingly given to a third-party has no reasonable expectation of privacy.[26] Third, anything in a constitutionally

---

U.S. 438, 463–64 (1928), *overruled by Katz*, 389 U.S. at 353, *and* Berger v. New York, 388 U.S. 41, 50–51 (1967). It should be noted, however, that the Court has not completely discarded the trespass doctrine. It appears that the *Katz* Test supplements the trespass doctrine instead of replacing it. *See* United States v. Jones, 132 S. Ct. 945, 950–51 (2012).

[16] *Katz*, 389 U.S. at 351.

[17] Cases as recent as April of 2016 have used this term. *See* United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016).

[18] This phrase was coined in Justice Harlan's concurrence in *Katz*, 389 U.S. at 360 (Harlan, J., concurring), and is the benchmark test for determining if a government action constitutes a search under the Fourth Amendment. RIC SIMMONS & RENÉE MCDONALD HUTCHINS, LEARNING CRIMINAL PROCEDURE 56 (2015).

[19] SIMMONS & HUTCHINS, *supra* note 18, at 57.

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

[21] *Id.*

[22] Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809, 1823 (2014) (citing Debra Katz, Case Comment, *Constitutional Law—Fourth Amendment Protection for Homeless Person's Closed Containers in an Outdoor "Home,"* 26 SUFFOLK U. L. REV. 279, 281 & n.15 (1992)).

[23] *Id.* (citing several articles devoted to examining the question of what constitutes an objective reasonable expectation of privacy). Ironically, the *Katz* Test—while groundbreaking—actually produced more confusion regarding what constituted a "search" under the Fourth Amendment. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 580 (5th ed. 2012).

[24] LAFAVE, *supra* note 23, at 588 (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)).

[25] *Katz*, 389 U.S. at 351; *see also* Hester v. United States, 265 U.S. 57, 59 (1924). Although *Hester* was decided before *Katz*, the principle in that case remains good law: when an individual engages in activity in open view, there is no Fourth Amendment protection. For example, the Fourth Amendment does not protect anything seen from a government-operated plane because it is in public view. California v. Ciraolo, 476 U.S. 207, 213–14 (1986).

[26] United States v. White, 401 U.S. 745, 749 (1971) (holding that an individual does not have a reasonable expectation of privacy in information voluntarily revealed to a third-party because it is reasonable to assume that the third-party will convey that information to law enforcement); s*ee also infra* Part II.C.

protected area discovered by law enforcement, solely because of special technology, maintains a reasonable expectation of privacy.[27]

B. *Adapting to Change: How the Reasonable Expectation of Privacy Adjusts to Technology*

One question has troubled courts since the implementation of the *Katz* Test: How does the reasonable expectation of privacy change with new developments in technology? The second prong of the *Katz* analysis requires societal recognition of the expectation of privacy. However, society's expectations of privacy change when society itself changes. Thus, new technology affects the implementation of the Fourth Amendment in two major ways: first, new technology used by law enforcement; and second, new technology used by individuals[28] (such as computers, email, and cell-site data).

It has been easier for the Court to apply the Fourth Amendment to new technologies used by law enforcement.[29] The Court developed a flexible, enduring, and broad framework to analyze new technology used by law enforcement.[30] However, the Court has struggled to create such a test for new technology used by the public.[31]

An adequate test for technology is elusive because of the difficulty determining when a technology becomes so widely used, and used in such a way, that society recognizes a reasonable expectation of privacy in that technology. Due to this difficulty, the Supreme Court—despite several opportunities to do so—has not issued a broad, generally applicable test to determine when the Fourth Amendment protects new technology.[32] Without

---

[27] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[28] Ric Simmons, *The Missed Opportunities of* Riley v. California, 12 OHIO ST. J. CRIM. L. 253, 257 (2014).

[29] *Id. Kyllo v. United States* is the seminal case regarding law enforcement's use of new technology. *See Kyllo*, 533 U.S. at 33. In *Kyllo*, police officers used thermal imaging technology to sense heat from lamps used to grow marijuana in the defendant's house. *Id.* at 29. This was a search because the technology was not in general public use, and it revealed information (heat emanating from lamps) that could not be collected without entering into a constitutionally protected area. *Id.* at 40. The Court followed a similar rationale in *Ciraolo* in finding that the mere fact that the defendant erected a fence around his yard to shield his activities did not preclude an officer from observing his yard from a public vantage point; thus, the defendant's expectation that his yard was protected from observation was unreasonable. *Ciraolo*, 476 U.S. at 213–14.

[30] *See* SIMMONS & HUTCHINS, *supra* note 18, at 91.

[31] Simmons, *supra* note 28, at 257.

[32] *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014) (limiting the holding to cell phones and declining to extend a general rule to electronic storage); United States v. Jones, 132 S. Ct. 945, 949–50 (2012) (relying on the traditional trespass doctrine to decide the case, thereby passing on the opportunity to create a broad rule for new technologies); City of Ontario v. Quon, 560 U.S. 746, 758–60 (2010) (declining to decide if a reasonable expectation of privacy exists in electronic pagers). *See generally* Simmons, *supra* note 28

guidance from the Supreme Court, lower courts have struggled to apply the Fourth Amendment in the digital age.

This leaves scholars to contemplate how courts should apply the Fourth Amendment to future digital issues that will surely arise. One approach is to adopt the mosaic theory.

The mosaic theory's primary purpose is to protect large amounts of electronic and digital information. Under the mosaic theory, if law enforcement aggregates enough information that is otherwise unprotected, they can violate an individual's reasonable expectation of privacy.[33] The D.C. Circuit introduced this approach in *United States v. Maynard*.[34]

In *Maynard*, the court held that the aggregation of Global Position System (GPS) surveillance over a twenty-eight-day period constituted a violation of the defendant's reasonable expectation of privacy.[35] On appeal, the Supreme Court decided the case using the traditional trespass doctrine[36]—ducking the opportunity to issue a broad rule for new technology.[37] Although the Court declined to issue binding precedent on the mosaic theory, five Justices showed support for the theory in concurring opinions.[38]

Because the Supreme Court avoided ruling on the mosaic theory, it left the lower courts without guidance. As a result, a circuit split developed on the issue.[39] The split was eventually resolved after an en banc hearing in the Fourth Circuit.[40]

The Fourth Circuit originally endorsed the mosaic theory; the court ruled that individuals have a reasonable expectation of privacy over their cell-site

---

(arguing that the Supreme Court has been too cautious in Fourth Amendment cases implicating new technology).

[33] Benjamin M. Ostrander, Note, *The "Mosaic Theory" and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733, 1734–35 (2011) ("The 'mosaic theory' . . . holds that individual law enforcement actions that are not searches become a search when aggregated, as the whole reveals more than the individual acts it comprises.").

[34] United States v. Maynard, 615 F.3d 544, 561–63 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[35] *Id.* at 558, 563 ("Society recognizes Jones's expectation of privacy in his movements over the course of a month as reasonable, and the use of the GPS device to monitor those movements defeated that reasonable expectation."). Notice that the movement was over public roads, and thus the activity was visible to the public. *See id.* at 559. Under traditional Fourth Amendment analysis, this would not be a violation of the defendant's reasonable expectation of privacy, but the court used the mosaic theory and found that "prolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have." *Id.* at 563.

[36] *Jones*, 132 S. Ct. at 953–54, *aff'g in part Maynard*, 615 F.3d 544.

[37] *See* Simmons, *supra* note 28, at 259.

[38] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 312 (2012).

[39] *See infra* notes 40–41 and accompanying text.

[40] *See* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (en banc).

location information (CSLI)[41]: "[T]he government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual over an extended period of time."[42] While the Court never used the word "mosaic," the panel opinion clearly endorsed the mosaic theory.[43] However, because of the lack of guidance and confusion on this issue, the Fourth Circuit reversed in an en banc hearing and decided against adopting the mosaic theory, thereby joining other circuits in their treatment of CSLI.[44] This illustrates the uncertain status of the mosaic theory.

Other circuits have also refused to adopt the mosaic theory. The Sixth, Eleventh, and Fifth Circuits determined that an individual has no reasonable expectation of privacy over his or her CSLI.[45] These courts (including the en banc Fourth Circuit) found that individuals voluntarily convey CSLI to a third-party when they use cell phones and thus have no reasonable expectation of privacy over that information.[46] This reasoning stems from a cornerstone of Fourth Amendment law: the third-party doctrine.

---

[41] As a cell phone receives a cell signal, it communicates with cell towers nearby; this geographic information is stored by the phone company and reveals the location of the phone. *See* Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, ATLANTIC (Aug. 8, 2015), http://www.theatlantic.com/technology/archive/2015/08/warrant less-cell-phone-location-tracking/400775/ [https://perma.cc/DK24-UB3T]. This is not trivial; in 2014, AT&T received nearly 65,000 requests for CSLI. *Id.*

[42] United States v. Graham, 796 F.3d 332, 349 (4th Cir. 2015), *adhered to in part on reh'g en banc*, 824 F.3d 421 (4th Cir. 2016).

[43] This is evident from the emphasis on information recovered "over an extended period of time." *Id.* Further, the court relied on the concurrences in *United States v. Jones*, which discussed the mosaic theory at length. *See id.*; s*ee also* Orin Kerr, *Fourth Circuit Adopts Mosaic Theory, Holds that Obtaining "Extended" Cell-Site Records Requires a Warrant*, WASH. POST: VOLOKH CONSPIRACY (Aug. 5, 2015), https://www.washingtonpost .com/news/volokh-conspiracy/wp/2015/08/05/fourth-circuit-adopts-mosaic-theory-holds-that-obtaining-extended-cell-site-records-requires-a-warrant/ [https://perma.cc/D72L-T9JM].

[44] *Graham*, 824 F.3d at 428.

[45] *See* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 613–14 (5th Cir. 2013).

[46] *Graham*, 824 F.3d at 427–28; *Carpenter*, 819 F.3d at 888; *Davis*, 785 F.3d at 511; *Historical Cell Site Data*, 724 F.3d at 613–14. Interestingly, the Fourth Circuit originally rejected this argument, relying on the idea that possession of a cell phone is not a completely voluntarily act in this era: "Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *Graham*, 796 F.3d at 356 (quoting City of Ontario v. Quon, 560 U.S. 746, 760 (2010)). "Modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* (alteration in original) (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)). Further, the Third Circuit has stated that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d

C. *How the Third-Party Doctrine Operates within the Fourth Amendment Framework*

As a general principle, an individual possesses no reasonable expectation of privacy over information voluntarily conveyed to a third-party.[47] While the Court established the third-party doctrine prior to *Katz*, the Court has since reaffirmed the principle in the post-*Katz* era.

One such occasion was *United States v. Miller*, which established that the third-party doctrine applies not only to information conferred to individuals, but also to information revealed to companies.[48] The Court reaffirmed this principle four years later in *Smith v. Maryland*.[49]

In *Smith*, the Court held that the defendant had no reasonable expectation of privacy over phone numbers dialed from his phone.[50] The Court supported this conclusion based on two rationales. First, the defendant had no subjective expectation of privacy because he knew the telephone company was receiving his dialing information.[51] Second, he voluntarily conveyed the information to the company in order to place a phone call, and thus assumed the risk that the company would relay the phone numbers he dialed to the police.[52]

An important aspect of *Smith* was the distinction between "address" information and "content" information. The Court classified the dialed telephone numbers as address information that had no reasonable expectation of privacy because the defendant voluntarily revealed the numbers to the company to place the call.[53] *Smith* contrasts this address information with the telephone conversation in *Katz*, which is protected content information

---

304, 317 (3d Cir. 2010); *see also* Zanders v. State, 58 N.E.3d 254, at 263 (Ind. Ct. App. 2016).

[47] SIMMONS & HUTCHINS, *supra* note 18, at 118. The third-party doctrine is often traced back to *Hoffa v. United States*, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

[48] United States v. Miller, 425 U.S. 435, 442 (1976) (citing Katz v. United States, 389 U.S. 347, 351 (1967)) (holding that when an individual gave financial information to a bank he "knowingly expose[d]" that information to the public, and thus had no reasonable expectation of privacy over the information).

[49] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[50] *Id.* at 745.

[51] *Id.* at 735.

[52] *Id.* at 744. This rationale in *Smith* is particularly important because the Court was applying the third-party doctrine to a technological advancement. *See* Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 12–14 (2013).

[53] *Smith*, 442 U.S. at 742 ("[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.").

expected to remain private.[54] In other words, society understood that the telephone company must record dialed phone numbers to place calls, but there was no expectation that the telephone company could hear the content of those calls.[55]

The application of the third-party doctrine has encountered problems in the digital age.[56] These problems arise because the distinction between address and content information has disappeared.[57] In digital communications, third parties must have access to *both* address and content information to send messages.[58] When a text message or email is sent, the sender knows that the third-party intermediary has access to the content of that message.[59] How could a phone company send a text, or an Internet Service Provider (ISP) send an email, if they could not access the contents of the message?[60] Third parties

---

[54] *Id.* at 741 ("[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.").

[55] Another example can be illustrated in the form of standard mail. A sender of mail understands that a third-party (the postal workers) must see the address of the letter. However, there is no expectation that the postal workers will open the envelope and read the contents of the letter. Thus, the content information of a letter is protected, but the address of the letter is not protected.

[56] *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("This approach [to the third-party doctrine] is ill suited to the digital age."); s*ee also* Bedi, *supra* note 52, at 15 ("The Third Party Doctrine has proven difficult to apply in the Internet context.").

[57] SIMMONS & HUTCHINS, *supra* note 18, at 128 ("[I]n the context of electronic communication, one of the distinctions between address information and content information disappears. Third party companies (such as internet service providers) record and store content information the same way that they record or store address information.").

[58] This is unlike past communications. For example, in *Smith*, while the phone company needed the address information (telephone numbers) to complete the call, they did not need access to the content of the call itself. *Smith*, 442 U.S. at 737. Similarly, for traditional mail, the government must have access to the address to deliver mail. There is no need for the government to know the contents of the letter to complete the delivery.

[59] The Sixth, Eleventh, Fifth, and Fourth Circuits relied on the voluntary consent rationale to determine that the Fourth Amendment does not protect a defendant's CSLI. *See supra* Part II.B.

[60] Apple is known for encrypting their "iMessages," which provides users with a sense of security. However, Apple encrypts the messages; this means Apple also has the ability to break the encryption if desired. *See* Greg Kumparak, *Apple Explains Exactly How Secure iMessage Really Is*, TECHCRUNCH (Feb. 27, 2014), http://techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/ [https://perma.cc/2ML5-LVAS] ("[B]ecause Apple is encrypting messages/data once for each device and has control over the key infrastructure, they may . . . be able to throw another public key into the mix—thereby allowing messages sent to you after that point to be read by whoever has the corresponding private key."). Thus, the message may be encrypted, but if Apple so desires, they can read the message. Interestingly, several phone applications have been able to remedy this problem by using encryption technology. The sender's text message is encrypted until it reaches its destination, and thus the phone company cannot view the content of the text. *See* Chris Stobing, *How and Why to Encrypt Your Text Messages*,

can access this content information just like the phone company in *Smith* had access to address information (telephone numbers) required to place the call.[61]

Under traditional third-party doctrine rationale, this content information is unprotected because senders knowingly share it with a third-party.[62] However, some courts place a heavier emphasis on the address/content distinction and protect any content information in these communications.[63] These two conflicting approaches have resulted in a circuit split.

III. THE CURRENT COMPETING FRAMEWORKS FOR DIGITAL COMMUNICATIONS AND THE INHERENT FLAWS IN EACH

There are two approaches to applying the third-party doctrine to digital communications. Some circuits use a strict third-party doctrine analysis, while some circuits focus more on the address/content distinction.[64] Courts are currently trying to determine which approach to follow, and have little guidance on the issue.[65] Both approaches have flaws, and this presents the opportunity for the Court to solve the dispute using the mosaic theory.

A. *Traditional Third-Party Doctrine Applies—No Protection for Digital Communications*

The first solution to this problem strictly applies the third-party doctrine. This argument relies on the sender voluntarily exposing the message to the intermediary.

1. *Rationale Behind the Strict Use of the Third-Party Doctrine*

The third-party doctrine requires the sender to voluntarily reveal information to a third-party. Emails, text messages, and other digital

---

HOW-TO GEEK (Aug. 25, 2015), http://www.howtogeek.com/226535/how-and-why-to-encrypt-your-text-messages [https://perma.cc/P6VN-D8CH]. However, the place of encrypted information in Fourth Amendment jurisprudence is also unsettled. *See generally* Lee Tien, *Doors, Envelopes, and Encryption: The Uncertain Role of Precautions in Fourth Amendment Law*, 54 DEPAUL L. REV. 873 (2005) (examining the extent to which one has the right to protect their own privacy).

[61] *See, e.g.*, Helena Horton, *Snapchat Just Reserved the Rights to Store and Use All Selfies Taken with the Device*, TELEGRAPH (Oct. 30, 2015), http://www.telegraph.co.uk/technology/news/11966036/Snapchat-just-reserved-the-rights-to-store-and-use-all-selfies-taken-with-the-device.html [https://perma.cc/U8RE-FQZN].

[62] *See infra* Part III.A.

[63] *See infra* Part III.B.

[64] SIMMONS & HUTCHINS, *supra* note 18, at 131.

[65] In 2015, for example, a court stated: "Indeed, it is unclear whether even the *contents* of emails stored on an Internet Service Provider's (ISP) servers are entitled to Fourth Amendment protection." United States v. Ortega, No. CR415-134, 2015 WL6566011, at *1 n.2 (S.D. Ga. Oct. 30, 2015).

communications travel through a third-party to reach the intended recipient. Because the sender knows the third-party can see, copy, and store the messages, they lose any expectation of privacy in these communications.[66]

Under this view, electronic communications are no different than the phone numbers dialed in *Smith*. The phone numbers lacked Fourth Amendment protection because the defendant knew he had to reveal phone numbers to complete the call.[67] Similarly, the sender of an email understands they must share the content of their message with the ISP for the message to reach the recipient. Therefore, email messages lose any expectation of privacy in the communication.[68]

Some argue that because the Fourth Amendment protects letters sent through standard mail,[69] and an email is just an electronic form of standard mail, the Fourth Amendment should also protect the content of email. However, these situations are different.[70] In standard mail, the sender expects the contents of the letter to remain enclosed in the envelope. In contrast, the sender of email knows that the intermediary will have access to the content of the message.[71] This difference is why the email/standard mail analogy is flawed.[72]

---

[66] Individuals should know they have no privacy in emails because news organizations have recently reported that messages sent through a third-party are not protected information. *See* Steven Musil, *Google Filing Says Gmail Users Have No Expectation of Privacy*, CNET (Aug. 13, 2013), http://www.cnet.com/news/google-filing-says-gmail-users-have-no-expectation-of-privacy [https://perma.cc/F3M5-D9JQ].

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

[68] Rehberg v. Paulk, 598 F.3d 1268, 1281 (11th Cir.) ("A person . . . loses a reasonable expectation of privacy in emails, at least after the email is sent to and received by a third party."), *vacated on other grounds*, 611 F.3d 828 (11th Cir. 2010); *In re* Search Warrant for Contents of Elec. Mail, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009) ("[S]ubscribers are, or should be, aware that their personal information and the contents of their online communications are accessible to the ISP and its employees and can be shared with the government under the appropriate circumstances."). Additionally, courts have used the third-party doctrine to determine that individuals have no privacy over the Internet Protocol (I.P.) addresses they use because when an individual uses their computer to connect to their email, they must knowingly share their I.P. address with third parties. United States v. Caira, No. 14-1003, 2016 WL 4376472, at *3 (7th Cir. Aug. 17, 2016). Once an I.P. address is known, the government can then contact the owner of the I.P. address (usually the internet provider) to discover much more information about the end user of the I.P. address such as account information and physical address information. *See id.* at *1–2.

[69] *E.g.*, United States v. Jacobsen, 466 U.S. 109, 114 (1984).

[70] "Some people seem to think that [emails] are as private as letters, phone calls, or journal entries. The blunt fact is, they are not." *Search Warrant*, 665 F. Supp. 2d at 1224.

[71] In 2013, Google argued this point convincingly: "As numerous courts have held, the automated processing of email is so widely understood and accepted that the act of sending an email constitutes implied consent to automated processing as a matter of law." *See* Defendant's Motion to Dismiss at 19, *In re* Google Inc. Gmail Litigation, No. 5:13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013). The brief cites several opinions from state courts asserting that individuals should know that messages sent

2. *Problems with Strictly Applying the Third-Party Doctrine*

Strictly applying the third-party doctrine has a major problem: the more technology progresses, the more individuals share with third parties. In the information age, individuals live much of their lives online. Every text, post shared on Facebook, or document uploaded to the cloud is shared with a third-party. This trend shows no sign of slowing down as technology advances. Individuals now wear watches that interact with the Internet,[73] drive cars that relay information through GPS to third parties, and keep daily schedules through companies like Google.

Because of this increased sharing, a strict application of the third-party doctrine will diminish the Fourth Amendment's value. Unlike the 1970s, when *Smith* was decided, technology now requires sharing information with third parties on a daily basis.[74] The strict application of the third-party doctrine has strong legal support, but legal realism may require a different approach.[75] In reality, the promises of the Fourth Amendment will decay if courts do not update it for the information age.

B. *Distinguishing Address and Content Information—Examining the Solution Proposed by* Quon *and* Warshak

Some courts have adopted a solution reliant upon the address/content distinction. This solution assigns privacy protection based upon what *type* of information is transmitted.

---

through the Internet are subject to transmission and recording, and thus voluntarily consent to this risk. *Id.* at 19–20.

[72] A better analogy can be drawn to a postcard. Email, like a postcard, reveals both the address information *and* the content information to the third-party intermediary. *See* NANCY FLYNN & RANDOPLH KAHN, E-MAIL RULES 173 (2003) ("The common analogy is that standard e-mail is like sending a 'postcard written in pencil through the postal mail.' A postcard, because anyone who sees the message along the way can freely read it . . . ."); Micalyn S. Harris, *E-mail Privacy: An Oxymoron?*, 78 NEB. L. REV. 386, 387 (1999) ("E-mail has been likened to . . . [the] use of postcards through the United States Postal Service.").

[73] The Apple Watch is one example. *See About Bluetooth and Wi-Fi on Apple Watch*, APPLE, https://support.apple.com/en-us/HT204562 [https://perma.cc/BT3G-C4ED].

[74] Some even argue that because of the necessity to use new technology, individuals are not truly consenting to sharing information with third parties. *See supra* note 46.

[75] *See* SIMMONS & HUTCHINS, *supra* note 18, at 131 (citing United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010)) (commenting that *Warshak* was a victory for legal realism over legal formalism).

1. *Rationale Behind the Address/Content Distinction*

In *United States v. Forrester*, a case with similar facts to *Smith*, the Ninth Circuit addressed the privacy of digital communications.[76] However, the court in *Forrester* decided that *Smith* should be interpreted narrowly for digital communications.[77] The court distinguished information voluntarily given to a third-party to direct the message (address information), from information given to a third-party that is the actual message itself (content information).[78]

The court believed that content information is more worthy of protection than address information: "[T]he Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information . . . ."[79] The Ninth Circuit affirmed this principle in *Quon v. Arch Wireless Operating Co.*: "[I]t is not reasonable to expect privacy in the information used to 'address' a text message, such as the dialing of a phone number to send a message. However, users do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider."[80]

In 2010, the address/content theory appeared again in *United States v. Warshak*.[81] In *Warshak*, the government subpoenaed the defendant's ISP to obtain the defendant's emails.[82] The court determined this violated the defendant's reasonable expectation of privacy because the emails were similar to the content of the phone conversation in *Katz*.[83] Particularly, the court focused on the intimate information that is shared via email.[84] Similar to *Quon* and *Forrester*, the court relied on the comparison of email to standard mail and the content of a telephone call.[85]

---

[76] United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

[77] *See id.* at 509–11.

[78] *Id.*

[79] *Id.* at 510. The court argued that electronic address information does not reveal anything more than a phone number does. *Id.* With address information, the government can only make "educated guesses" about what the information is being used for, whereas content information is more like the phone call in *Katz*, and should be protected because it reveals exact details about the communication. *Id.* Further, the court relied heavily on the analogy of email to standard mail. *Id.* This analogy is weak. *See supra* Part III.A.1.

[80] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008) (holding that text messages sent via an electronic pager are protected information under the Fourth Amendment), *rev'd on other grounds*, City of Ontario v. Quon, 560 U.S. 746 (2010).

[81] United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010).

[82] *Id.* at 283. This was significant. Over several months, the government subpoenaed about 27,000 emails. *Id.*

[83] *Id.* at 286.

[84] *Id.* at 284 (referencing the following exchanged via email: "[l]overs exchang[ing] sweet nothings," individuals making online purchases, sharing business plans, and communicating doctor-patient appointment information).

[85] *Id.* at 285–86 ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth

2. *Problems with Applying the Address/Content Distinction*

There are three problems with the *Quon* and *Warshak* framework. First, it disregards the third-party doctrine and is problematic if applied to other third-party scenarios. Second, distinguishing between address and content information is difficult, and this difficulty will persist as technology advances. Third, the Supreme Court is not eager to adopt this framework.

First, *Quon* and *Warshak* conflict with the third-party doctrine.[86] Consent, not type of information, is the basis of the third-party doctrine.[87] Both *Quon* and *Warshak* focus on the sensitive information in emails;[88] this logic departs from *Smith*. The phone numbers in *Smith* lacked protection because the defendant voluntarily provided them to a third-party; the fact that phone numbers are not sensitive information was not why the Court found they lacked protection.[89] Further, the Court protected the phone conversation in *Katz* because there was no expectation anyone was recording the call—the sensitive content of the call was not a factor.[90]

Similarly, in standard mail, the Fourth Amendment does not protect address information because the sender knows the intermediary will see the address. On the other hand, the Fourth Amendment protects the contents of the letter inside the envelope because there is no expectation the intermediary will

---

Amendment protection."). As discussed earlier, the analogy of email to standard mail is flawed. *See supra* Part III.A.1.

[86] In *Quon*, the court shockingly stated that it was "irrelevant" that a third-party had access to the information being transferred. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008).

[87] In *Hoffa*, the Court did not ask if the information was sensitive or deserving of protection, rather, the Court asked if the defendant voluntarily offered that information to a third-party. Hoffa v. United States, 385 U.S. 293, 302 (1966). More recently, an Indiana state court illustrated this point stating:

> *Miller*, *Smith*, and its progeny do not categorically exclude third-party records from Fourth Amendment protection. . . . It is the act of voluntary conveyance—not the mere fact that the information winds up in the third party's records—that demonstrates an assumption of risk of disclosure and therefore the lack of any reasonable expectation of privacy.

Zanders v. State, 58 N.E.3d 254, 263 (Ind. Ct. App. 2016).

[88] *See supra* Part III.B.1.

[89] Smith v. Maryland, 442 U.S. 735, 744 (1979). In finding that a reasonable expectation of privacy did not exist, the Court stated: "[P]etitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed." *Id.*

[90] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("The critical fact in this case is that '[o]ne who occupies it, [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted." (alterations in original) (quoting *id.* at 352 (majority opinion))).

open the envelope and read the letter. The possibility that letters may contain sensitive information is not the thrust of the Fourth Amendment analysis.

For these reasons, email is more comparable to a postcard because the sender knows the intermediary will see the address *and* content of the message.[91] Thus, *Quon* and *Warshak* focus on the wrong things: they focus on the type of information sent, not the consent of the sender.

If courts apply the logic in *Quon* and *Warshak* to traditional third-party scenarios, problems arise. Assume Jim asks his friend, Nathan, to deliver five $20 bills to Gary. Clipped to the money is a hand-written note showing Gary's address and a message that reads: "Here is the $100 I owe you for the cocaine." In this scenario, Nathan is clearly acting as an intermediary (like an ISP for email). His job is to transmit the money and the note to the intended recipient, Gary. Nathan sees the address needed to deliver the note, and he can also see the content of the note itself (like an ISP can see the content of an email). If we focus on the *type* of information, like *Quon* and *Warshak* propose, the Fourth Amendment protects the entire note (even though it was voluntarily given to a third party) because it possesses content information. This result is hard to live with.[92]

Secondly, this proposed framework faces practical difficulties. While a clear distinction between address and content information once existed, that line is now blurred.[93] Is a detail-revealing website URL[94] protected content information or unprotected address information?[95] What about

---

[91] Just like extra effort is taken to protect letters sent through the mail, the sender of an email can encrypt the email so that it is only readable by the recipient, and not the intermediary. *See* Jesse Emspak, *CNBC Explains: How to Encrypt Your Email*, CNBC (Jan. 9, 2014), http://www.cnbc.com/2014/01/08/ns-how-to-encrypt-your-email.html [https://perma.cc/2HNR-UU44].

[92] The authors of *Quon* and *Warshak* would likely respond that the address/content distinction should only be applied to digital communications sent through third parties. However, due to the reliance of their arguments on the comparison between email and standard mail, that response is hard to swallow. *See* United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008).

[93] *See* SIMMONS & HUTCHINS, *supra* note 18, at 131.

[94] URL stands for Uniform Resource Locator or Universal Resource Locator. This is the "address" of every website on the Internet. *See URL*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/URL [https://perma.cc/MYY2-A3ZP].

[95] For example, if I visit "http://www.elevenwarriors.com/ohio-state-football/2015-national-championship/2015/01/48289/instacap-ohio-state-rides-ezekiel-elliott-to-a-42-20-win-over," that URL is the address of my communication with the Internet. It reveals that I was reading about the 2014–2015 Ohio State Buckeyes winning the College Football National Championship. Tim Shoemaker, *Instacap: Ohio State Rides Ezekiel Elliott to a 42–20 Win over Oregon to Win the National Championship*, ELEVEN WARRIORS (Jan. 13, 2015), http://www.elevenwarriors.com/ohio-state-football/2015-national-championship/2015/01/48289/instacap-ohio-state-rides-ezekiel-elliott-to-a-42-20-win-over [https://perma.cc/D6VF-ZNFL]. Does this become content information? For a full discussion on the classification of

communications that have undefined recipients such as a Facebook post to "friends?" Under the *Quon* and *Warshak* framework, the Fourth Amendment may protect the Facebook post—even though the information is displayed to potentially hundreds of people—because it contains content information. It is hard to fathom that a communication to potentially hundreds of people possesses a reasonable expectation of privacy.

Finally, the Supreme Court is not eager to endorse the *Quon* and *Warshak* proposal. In 2010, the Court had the opportunity to adopt this framework,[96] but the Court expressly refused to decide if the address/content distinction should control future technological problems.[97] If the Court believed this was the best solution moving forward, it would have endorsed the theory in 2010.

IV. APPLYING THE MOSAIC THEORY TO DIGITAL COMMUNICATIONS

The current proposed frameworks analyzing digital communications under the Fourth Amendment fail to deliver desirable results. Luckily, courts have a better alternative: the mosaic theory. The mosaic theory does not focus on the consent of the sender, nor does it focus on the type of information sent. The mosaic theory simply helps determine when the aggregation of personal information violates an individual's reasonable expectation of privacy. Thus, the mosaic theory is not a major change in Fourth Amendment jurisprudence—it is a tool courts should use when determining if an individual's reasonable expectation of privacy has been violated.

A. *A Look at the Benefits of the Mosaic Theory*

The mosaic theory has three benefits. First, it protects the large amounts of information for which the Supreme Court has indicated concern. Second, it saves the application of third-party doctrine. Third, it presents a flexible framework that courts can apply to future technologies.

1. *Protection of Large Amounts of Digital Information*

The mosaic theory protects large amounts of information that can reveal extremely personal information. The D.C. Circuit applied this rationale to GPS tracking in *Maynard*.[98] The court believed that a large compilation of small movements revealed intimate details about an individual's life: "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and

---

URLs, see Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2134–50 (2009).

[96] *See* City of Ontario v. Quon, 560 U.S. 746 (2010).

[97] *See* Simmons, *supra* note 28, at 265.

[98] *See generally* United States v. Maynard, 615 F.3d 544, 561–63 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation."[99] The court distinguished this from the smaller pieces of information that compose the mosaic; that information reveals much less.

The court also noted that a reasonable person does not expect his or her daily movements and activities to be monitored constantly by the government.[100] This constant surveillance is a new phenomenon, and it would have been almost impossible prior to the digital age.[101]

These same concerns exist with digital communications. Like physical movements, one email or text message may not reveal much about an individual's life. Several months of communications, however, will surely reveal purchasing habits, political preferences, medical information, and extended conversations between friends and lovers. Further, like GPS data points, collecting months of communication would most likely not have been feasible for police prior to the digital age. However, with current technology, police just let their suspects conduct their daily lives, and they can gain access to a wealth of information via the third-party intermediary.[102]

The mosaic theory solves these problems. It protects large amounts of information that are now routine in daily life, and it honors the reasonable person's expectation that the government is not constantly monitoring every movement and communication.

2. *Saving the Third-Party Doctrine*

The mosaic theory preserves the traditional third-party doctrine. Unlike the *Quon* and *Warshak* proposal, applying the mosaic theory to digital communications will not affect the third-party doctrine analysis.[103]

---

[99] *Id.* at 562.

[100] *Id.* at 563 ("A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'" (citation omitted) (quoting Nader v. Gen. Motors Corp., 255 N.E.2d 765, 772 (N.Y. 1970) (Breitel, J., concurring))).

[101] *Jones*, 132 S. Ct. at 963 (Alito, J., concurring) ("Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance."); *see also infra* note 109.

[102] Remember that in *Warshak* the police had access to roughly 27,000 emails sent by the defendant. *See supra* note 82. It is doubtful that law enforcement could obtain all of these communications in the pre-digital era.

[103] Interestingly, one commentator has recommended using the mosaic theory as one factor when determining a standard for voluntary disclosure of digital communications. *See* Margaret E. Twomey, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 MICH. TELECOMM. & TECH. L. REV. 401, 416 (2015).

Further, the mosaic theory does not create confusion on how to apply the third-party doctrine. The *Quon* and *Warshak* framework created new questions: what is content information, and what is address information? This address/content distinction is sloppy and troublesome for future forms of technology. The mosaic theory does not concern itself with this distinction. It only asks how much information, and how revealing is that quantity of information.

The mosaic theory simply acts as a large information exception to the third-party doctrine. The third-party doctrine applies traditionally until a mosaic threshold is met. At that point, Fourth Amendment protection activates for the large quantity of information.

3. *A Test that Stands the Test of Time*

A major benefit to the mosaic theory is its flexibility. With the quick advancements in technology,[104] a new Fourth Amendment framework should have the ability to develop with technology. Much like the reasonable expectation of privacy, the mosaic theory does not propose a bright-line test that is specific and limited to a certain technology.[105]

The mosaic theory simply asserts that, when law enforcement aggregates enough information to reveal an intimate portrait of an individual's life, that individual's reasonable expectation of privacy is violated. Thus, as technology develops, and new methods of communication are created, the question will remain the same: is the government aggregating so much information that an individual's reasonable expectation of privacy is violated?

B. *The Feasibility of Applying the Mosaic Theory to Digital Communications*

The mosaic theory is a viable solution to provide Fourth Amendment protection to digital communications. First, a new framework is needed because the current proposed solutions are not desirable and the Supreme Court is unlikely to adopt these solutions. Second, the mosaic theory aligns with the Court's recent concern for large quantities of information.

---

[104] United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016) ("[S]ometimes new technologies—say, the latest iterations of smartphones or social media—evolve at rates more common to superbugs than to large mammals.").

[105] Some see this as the downfall of the *Riley* decision. *See* Simmons, *supra* note 28, at 264 (arguing the Court missed the opportunity to issue a broad ruling for the future of the Fourth Amendment, and instead decided to issue a narrow decision that only applies to cell phone searches pursuant to the search incident to lawful arrest doctrine). The purposeful ambiguity and nature of the broad rule allowed the *Katz* Test to be flexible enough to adapt to new situations over the past fifty years.

1. *Rejection of the* Quon *and* Warshak *Framework and the Failure of the Third-Party Doctrine to Protect Sensitive Information*

First, applying the mosaic theory to digital communications is feasible because the Court has not endorsed either of the current solutions. The Court had the opportunity to endorse the *Quon* and *Warshak* framework in 2010 and passed on the opportunity.[106] This indicates the Court's reluctance to rely on the address/content distinction like the circuit courts have.

However, the alternative to the *Quon* and *Warshak* framework will not please the Court either. In *Jones* and *Riley*, the Court showed sensitivity for large amounts of digital data.[107] The strict application of the third-party doctrine does not protect large amounts of digital communications. Thus, the Court is unlikely to strictly apply the third-party doctrine.

This leaves the mosaic theory as a perfect middle ground for the Supreme Court. The mosaic theory enables the Court to protect large amounts of information transferred through a digital intermediary, while simultaneously respecting the third-party doctrine.

2. *Taking the Court's Guidance from* Jones *and* Riley

The Court has indicated that, in the digital era, the amount of information obtained by law enforcement is crucial to the Fourth Amendment analysis. Both *Jones* and *Riley* exemplify the Court's concern for the quantity of information accessible to law enforcement via technology.

In *Jones*, a concern for large amounts of information was evident. Particularly, Justice Sotomayor, in a concurring opinion, doubted that individuals expect the government to track their movements over a long period of time: "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[108] Four more justices doubted that society expected long term monitoring of their movements.[109] The Court's emphasis on large amounts of data is clear because it upheld the GPS tracking in *United States v.*

---

[106] *See supra* notes 96–97 and accompanying text.

[107] *See infra* Part IV.B.2.

[108] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

[109] Justice Alito, in a concurring opinion joined by Justices Ginsberg, Breyer, and Kagan, stated:

> [L]onger term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, 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.

Id. at 964 (Alito, J., concurring).

Knotts,[110] but four Justices concurred that law enforcement violates an individual's reasonable expectation of privacy when tracked over a long period of time.

In *Riley*, the Supreme Court held that law enforcement could not search a cell phone pursuant to the search incident to lawful arrest doctrine.[111] The Court partially relied on the immense storage capacity of cell phones,[112] and the reality that large amounts of information can reveal intimate details.[113] The Court pointed to the amount of information cell phones hold, stating: "One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy."[114] The Court's decision also showed mosaic reasoning: "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions . . . ."[115]

These decisions illustrate the Court's recent and growing concern for large amounts of data in the information age. The mosaic theory addresses this concern by protecting large amounts of data.

C. *Addressing Counterarguments to the Mosaic Theory*

Three concerns accompany the mosaic theory. The first concern is conceptual—the legal ground on which it stands. The second concern is practical—how can courts actually implement the theory? The third concern is speculative—what are the potential implications of the mosaic theory applied to traditional communications?

1. *Conceptual Concerns*

How can one piece of information not possess a reasonable expectation of privacy, but many of those same pieces of information *do* contain a reasonable expectation of privacy? This is a conceptual concern of the mosaic theory, and

---

[110] United States v. Knotts, 460 U.S. 276, 285 (1983) (holding that GPS tracking occurring over the course of one day did not violate the Fourth Amendment).

[111] *See* Riley v. California, 134 S. Ct. 2473, 2484–85 (2014).

[112] "[T]he Court's rationale was that smartphones typically store vast amounts of information about their users . . . ." United States v. Carpenter, 819 F.3d 880, 889 (6th Cir. 2016) (explaining that, while *Riley* relied on the collection of large amounts of data, the defendant's claim that the collection of his CSLI violated his Fourth Amendment rights fails because CSLI does not contain a similar amount of data).

[113] *Riley*, 134 S. Ct. at 2494–95 ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" (citation omitted) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))). The Court also showed concern for the intimate types of information that cell phones can contain. *Id.* at 2490.

[114] *Id.* at 2489.

[115] *Id.*

a dissent by a D.C. Circuit judge echoed this criticism: "The sum of an infinite number of zero-value parts is also zero."[116] Put differently: why is searching one piece of information tolerable, but collecting many pieces of the same information improper?[117]

The answer to this conceptual concern lies at the heart of the *Katz* Test. The mosaic theory does not reform the *Katz* Test, but rather, it attempts to help determine when an individual's reasonable expectation of privacy is violated. It is the extended observation that violates the reasonable expectation of privacy, not the content itself.

A prime example involves an individual's medical care.[118] Suppose Greg drives to his physician for a regular check-up. The doctor finds an abnormality during a routine prostate exam, and suggests Greg follow up with a prostate specialist. Greg then visits the prostate specialist who suggests he see an oncologist. Greg then sees the oncologist, who recommends Greg undergo surgery to remove a cancerous growth. Greg has the surgery a week later.

Greg traveled over public roads the entire time, and because he exposed his movements to the public, he has no reasonable expectation of privacy over his individual trips to his physician, the specialist, the oncologist, and the surgery center.[119] Each of these trips, by themselves, only reveals a small amount of information, such as: a doctor's appointment, a prostate issue, something cancer related, and a trip to a surgery center. Individually, these pieces of information do not show Greg's medical status. However, when this information is aggregated, a clear picture—a mosaic—of Greg's health materializes.

This example shows how an individual can lack an expectation of privacy over one piece of information, but can gain an expectation of privacy when the information is aggregated. Greg can reasonably expect that no one will track him long enough to diagnose his exact medical status.[120]

2. *Practical Concerns*

A practical concern facing the mosaic theory (in both GPS data and digital communications) is the establishment of the mosaic threshold: at what point does the aggregation of information violate an individual's Fourth Amendment rights?[121]

---

[116] United States v. Jones 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting from the denial of rehearing en banc).

[117] Bedi, *supra* note 22, at 1839–40.

[118] This example is loosely based on an example from *Maynard* examining trips to a gynecologist and to a baby store. United States v. Maynard, 615 F.3d 544, 561–63 (D.C. Cir. 2010), *aff'd in part sub nom*. United States v. Jones, 132 S. Ct. 945 (2012).

[119] *See supra* note 25 and accompanying text.

[120] *See supra* Part IV.B.2.

[121] The four Justice concurrence in *Jones* found that twenty-eight days of GPS surveillance was too much. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). In

Many scholars have addressed this question.[122] This Note does not attempt to determine where the cutoff for a mosaic lies. The courts will decide this, and they should embrace the challenge, as it will contribute to the mosaic theory's success.

A mosaic threshold operates as a broad standard, not a specific rule. Courts impose broad legal standards frequently: tort law has the reasonable person,[123] contract law has the duty of good faith,[124] criminal procedure has "meaningful interference" for seizures of property,[125] and courts use the "reasonable expectation of privacy" for Fourth Amendment searches.[126]

None of these operate as a brightly defined rule. Courts have decided when these standards are met, and then the application of the standard shapes around those decisions. Courts will do the same for a mosaic standard. The courts already have a starting point for GPS data points: less than twenty-eight days.[127] However, this twenty-eight day period may not be applicable to electronic communications; the courts are free to establish the mosaic thresholds for electronic media the way they best see fit. Differing forms of electronic communication can reveal differing amounts of personal information, and courts should have the flexibility to determine the mosaic threshold for each of these different forms. Courts will define the lower limit of these thresholds when the appropriate cases arrive.

This broad standard is a benefit of the mosaic theory. The flexibility of standards explains their continued success and application. The reasonable person changes as society changes; similarly, the mosaic threshold can change as technology changes. Without a bright line, courts have the flexibility to define different mosaic thresholds for different types of data. It might take 1,000 text messages to develop a mosaic but only 200 emails—courts will define these thresholds through litigation. The result is a flexible, broad standard, and this is preferable to a bright-line rule.

Graham, the Fourth Circuit originally found that fourteen days of surveillance qualifies as an "extended period of time" and thus violates an individual's reasonable expectation of privacy. United States v. Graham, 796 F.3d 332, 349–50 (4th Cir. 2015), *adhered to in part on reh'g en banc*, 824 F.3d 421 (4th Cir. 2016). On the other hand, the Sixth Circuit found that three days' worth of GPS data points does not violate an individual's reasonable expectation of privacy. United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012).

[122] *See* Steven M. Bellovin et al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 N.Y.U. J.L. & LIBERTY 555, 556 (2014) (discussing the use of "machine learning" to quantify when the aggregation of information constitutes a mosaic); Kerr, *supra* note 38, at 333 (discussing the problem of determining what should be aggregated and how); Ostrander, *supra* note 33, at 1748 (discussing *Maynard*'s lack of guidance for what constitutes a mosaic).

[123] W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 32, at 173–74 (5th ed. 1984).

[124] *See* E. ALLEN FARNSWORTH, CONTRACTS § 7.17, at 489 (4th ed. 2004).

[125] *See* SIMMONS & HUTCHINS, *supra* note 18, at 155.

[126] *See supra* Part II.A.

[127] *See* Simmons, *supra* note 28, at 263.

3. *Applying the Mosaic Theory to Traditional Communications*

If the Court adopts the mosaic theory, would it apply to all third-party communications? This question is fair, particularly because this Note criticizes the *Quon* and *Warshak* proposal due to the problems it poses when applied to traditional third-party communications.[128] However, several differences distinguish the *Quon* and *Warshak* framework from the mosaic theory.

First, from a practical perspective, the mosaic theory will most likely never apply to traditional forms of communication. Rarely will law enforcement have the ability to aggregate enough traditional, non-electronic information for the mosaic theory to apply.[129]

Secondly, the mosaic theory is a new doctrine that has no place in prior jurisprudence, and the Court has indicated that the Fourth Amendment should treat large amounts of information differently in today's world.[130] Therefore, if the Court wishes to use the mosaic theory as a special rule only applicable to electronic communications, it can do so. This is unlike the *Quon* and *Warshak* solution because that solution attempts to extend an established doctrine that applies to non-digital forms of communication like mail and phone conversations.

V. CONCLUSION

"Courts and commentators have for years begun to acknowledge the increasing tension, wrought by our technological age, between the third-party doctrine and the primacy Fourth Amendment doctrine grants our society's expectations of privacy."[131]

The Fourth Amendment and technology have not progressed at the same rate. The advances in technology have far outpaced Fourth Amendment development in the digital age. This has resulted in an undeniable tension between Fourth Amendment protection and technology.

Because of this tension, courts have struggled to provide Fourth Amendment protection for digital communications. Some courts strictly apply the third-party doctrine. Other courts have made bold (but misguided) attempts to reform the Fourth Amendment analysis.

In recent Fourth Amendment decisions, the Supreme Court has suggested that the size of information matters. Applying the mosaic theory to digital communications addresses this concern. Further, this solution strikes the

---

[128] *See supra* Part III.B.2.

[129] *See supra* Part IV.A.1 (discussing limits of traditional surveillance).

[130] *See supra* Part IV.B.2 (examining recent Supreme Court discussions of large amounts of information).

[131] United States v. Graham, 796 F.3d 332, 360 (4th Cir. 2015), *adhered to in part on reh'g en banc*, 824 F.3d 421 (4th Cir. 2016).

appropriate balance between strictly applying the third-party doctrine and overextending the address/content distinction to protect privacy rights.

The mosaic theory is not without flaws. However, the test provides a flexible, broad standard that gives courts the ability to shape the test over time. The Supreme Court is not an institution that has traditionally avoided tough problems, and now—in the middle of a debate about the future role of the Fourth Amendment—is not the time to start. For the sake of privacy, the Court should rise to this challenge and apply the mosaic theory to digital communications.