SOCIAL NETWORKS, GOVERNMENT SURVEILLANCE, AND THE FOURTH AMENDMENT MOSAIC THEORY

MONU BEDI[*]

[*] Assistant Professor, DePaul University College of Law. A.B. Dartmouth College, M.Phil. University of Cambridge, J.D. Harvard University. I would like to thank Joshua Dressler, Keith Guzik, Orin S. Kerr, Rebecca Moosavian Ellen Podgor, Zoe Robinson, Christine S. Scott-Hayward, Christopher Slobogin, Mark Tunick, and Ari Waldman for their feedback. I would also like to thank my research assistant, Kristi Mankowski, for her help. This paper was presented at the 2014 Law and Society Conference in Minneapolis, MN as well as the 2014 Law and Society Social Media and the Law Symposium co-sponsored by the Charleston Law Review in Charleston, SC.

The mosaic theory—first articulated by the Supreme Court in United States v. Jones *two years ago—has turned out to be an empty promise of Fourth Amendment protection. However, this may have less to do with the theory itself and more to do with the context in which it has been applied. Introduced as a mechanism to combat long-term GPS police surveillance, scholars have widely criticized the theory as untenable and too costly. Its application jeopardizes long-standing police investigative tactics, including the use of undercover informants and even short-term human surveillance.*

This Article provides the first application of the mosaic theory to social networking communications over the Internet. The refrain of "the sum is greater than the parts" remains. Only this time it is a group of communications, not a person's movements, that informs the relevant analysis. This Article employs the principle of associational rights—referenced by Justice Sotomayor in Jones*—as a key ingredient to explaining why these social networking communications, in the aggregate, merit privacy protection. This is not simply an academic exercise. In light of the news that the NSA has been collecting messages over sites such as Facebook, courts need a Fourth Amendment framework to protect these communications where one currently does not exist. This narrow use of the theory also has the benefit of preserving the current Fourth Amendment landscape and the police's ability to use a wide range of investigative tactics.*

INTRODUCTION

The Fourth Amendment and technology have always had a volatile relationship. As technology advances, courts and scholars have struggled to update privacy protection.[1] The Supreme Court introduced the mosaic theory as one way to combat extended electronic surveillance of a suspect's movements, though the consensus appears to be that it is not sustainable in the larger Fourth Amendment framework.[2] This Article deploys the mosaic theory in the Internet context—particularly social networking sites—where it provides an effective way to protect communications that would otherwise not pass the reasonable expectation of privacy test under the Fourth Amendment.

The mosaic theory was first introduced in *United States v. Jones* through the

[1] *See, e.g.*, Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479 (2011) [hereinafter Kerr, *Equilibrium-Adjustment*] (discussing, in part, how courts respond to technological advances when it comes to Fourth Amendment jurisprudence).

[2] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (contending that long-term GPS monitoring can create an aggregate record of information that amounts to an unreasonable search); *id.* at 958 (Alito, J., concurring) (asserting that the aggregate amount of personal information compiled through long-term police surveillance is a violation of current societal expectations).

respective concurrences of Justices Sotomayor and Alito.[3] The case dealt with extended GPS surveillance of the defendant's vehicle for approximately one month, during which time the police gathered significant amounts of data on the car's movements.[4] While the majority disposed of the case on a Fourth Amendment technicality,[5] the concurrences raised the mosaic theory as a way to protect against this long-term surveillance.[6]

The hurdle for the justices was the longstanding Public Disclosure Doctrine, which says that an individual does not have a reasonable expectation of privacy in her public movements.[7] Voluntary disclosure to the public alone vitiates Fourth Amendment protection. Using a mosaic-based approach, the concurrences argued that the aggregate of public movements—even if individually not protected—qualifies for protection under the Fourth Amendment reasonable expectation of privacy test.[8] The concurring opinions focused on how society would react to this kind of extended government intrusion into a person's private life.[9] Specifically, an individual would not reasonably expect that the government would record a large collection of her public movements such that it could ascertain her private information,

[3] *Id.* at 954-57 (Sotomayor, J., concurring) (opining that long-term GPS monitoring creates an aggregate record of information that violates a society's reasonable expectation of privacy); *id.* at 957-64 (Alito, J., concurring) (asserting that this long-term monitoring is a violation of current societal expectations, while also acknowledging that technological advances change expectations). The theory was first introduced by the D.C. Circuit in *United States v. Maynard*, which was subsequently appealed to the Supreme Court. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) *aff'd sub nom. Jones*, 132 S. Ct. 945 (introducing the mosaic theory's concern with the ability of police to deduce intimate personal information based on long-term surveillance records).

[4] *Jones*, 132 S. Ct. at 948 (majority opinion) ("It relayed more than 2,000 pages of data over the 4-week period.").

[5] *Id.* at 950 (holding that the Court only need ensure an individual's privacy from physical governmental trespasses, in accordance with the original expectations of the Fourth Amendment).

[6] *Id.* at 954 (Sotomayor, J., concurring) (claiming that a Fourth Amendment search occurs when an individual's reasonable expectation of privacy is violated); *id.* at 964 (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

[7] *See* Hester v. United States, 265 U.S. 57, 58 (1924) (explaining that the defendant forfeited any Fourth Amendment protections from search or seizure when the legal violations at hand were disclosed via "[t]he defendant's own acts, and those of his associates").

[8] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (opining that societal expectations of privacy are violated when the government is able to aggregate information and uncover otherwise non-disclosed behavior); *id*. at 964 (Alito, J., concurring) (emphasizing that societal expectations of privacy do not include an assumption that the government can secretly monitor one's every move for long periods of time).

[9] *Id.* at 955-56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

including her "political and religious beliefs, sexual habits, and so on."[10]

Scholars have questioned the viability of the mosaic theory, particularly as it relates to the status of government investigative practices.[11] Accepting this theory puts routine government surveillance in jeopardy of Fourth Amendment restrictions.[12] It seems that even the brief surveillance of an individual could reveal private information. For instance, a single trip to a particular religious gathering or political function could reveal compromising or otherwise personal information that an individual would like to keep secret. More generally, people may disagree as to what society thinks is reasonable or unreasonable surveillance.[13] Perhaps even short-term monitoring of a person's public movements in a remote area where police are not likely to find themselves would also qualify as an unreasonable intrusion.[14]

To make matters worse, this theory also severely curtails the application of

[10] *Id.* at 956 (Sotomayor, J., concurring). According to Professor Orin Kerr, the concurrences opted to use the probabilistic model of reasonable expectation, which was the first model of reasonable expectation under his four-part structure. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 346 (2012) [hereinafter Kerr, *The Mosaic Theory*] ("[T]he mosaic theory rests on a probabilistic conception of the reasonable expectation of privacy test."); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 508 (2007) [hereinafter Kerr, *Four Models*] (establishing the probabilistic model as one of four used by the Supreme Court to evaluate the reasonable expectation of privacy question).

[11] *See infra* Part II.B.2 (illuminating the potentially irreconcilable difference between relying on either objective disclosure, as was the standard in the past, or subjective societal expectations of privacy, which is the more recent proposal).

[12] *See* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 385 (2013) (emphasizing government difficulty in ascertaining and respecting the "boundaries between observational and surveillance practices that are liberty enhancing and those that are liberty denying"); Kerr, *The Mosaic Theory*, *supra* note 10, at 335-36 (2012) (highlighting the uncertainty not only as to which surveillance methods will be counted toward the aggregate record under the mosaic theory, but also whether each method would need to be subject to different regulation based on respective degrees of invasiveness).

[13] *See* Kerr, *The Mosaic Theory*, *supra* note 10, at 330-31 (highlighting the ambiguity in various formulations of the mosaic theory as to which expectations of privacy deserve protection). Even Justices Sotomayor and Alito seem to disagree on the appropriate perspective from which to conduct this reasonableness analysis. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("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."); *id.* at 964 (Alito, J., concurring) ("[A]sk whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.").

[14] *See Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring) (opining that even short-term surveillance creates a detailed personal record that may constitute an unreasonable intrusion under the reasonable expectation of privacy test).

the Third Party Doctrine, the corollary to the Public Disclosure Doctrine (collectively the "Doctrines").[15] The Third Party Doctrine states that any information disclosed to another person or entity—much like the public generally—loses any Fourth Amendment protection.[16] This doctrine allows law enforcement to use undercover agents and surreptitiously gather information without a warrant.[17] However, under the mosaic approach, one could also argue that these communications, taken in the aggregate, can reveal private information about this person (e.g., disclosures about religious or privately held beliefs) and thus should be protected, particularly if the agent goes to great lengths in gaining the confidence of the suspect.[18]

The theory also faces significant practical hurdles.[19] Where should courts draw the line as to when the Fourth Amendment attaches? Is it one month, two weeks, or something short of continuous monitoring? There does not appear to be a principled way to make this determination.[20] Assuming these public movements should be protected, the theory also does not explain how police would satisfy the Fourth Amendment probable cause and warrant requirements, which necessitate specifying the location and item to be seized.[21] The mosaic theory is not concerned with a specific location but rather with the continuous surveillance over a period of time. Does this mean that one of the locations the suspect will travel to will contain evidence of a crime or is it the

[15] Gray & Citron, *supra* note 12, at 402 ("[A]dopting a mosaic approach to the Fourth Amendment may require abandoning or dramatically altering two important lines of Fourth Amendment law: the public observation doctrine and the third party doctrine." (citations omitted)).

[16] Lopez v. United States, 373 U.S. 427, 437-38 (1963) (holding that information disclosed to an undercover agent was not "seized" under the Fourth Amendment when the discloser voluntarily gave the information to the agent); *see id.* at 449 (Brennan, J., dissenting) ("The assumption, manifestly untenable, is that the Fourth Amendment is only designed to protect secrecy.").

[17] *Id.* at 465 (Brennan, J., dissenting) (claiming that undercover agent's inherent deception does not offend constitutional principles).

[18] *See* Gray & Citron, *supra* note 12, at 406 (expressing concern over the lack of protection awarded to information unwittingly, though voluntarily, shared with a private agent by a defendant who is unaware of the agent's identity).

[19] *See infra* Part II.B.3.

[20] The majority in *Jones* raised this concern with the mosaic theory as proposed by the concurrences. United States v. Jones, 132 S. Ct. 945, 954 (2012) (claiming that the mosaic theory produces vexing problems regarding unprecedented differentiation between long-term and short-term surveillance and the nature of the crime investigated).

[21] Warden v. Hayden, 387 U.S. 294, 301 (1967) ("Protection of these interests was assured by . . . requiring the use of warrants, which particularly describe 'the place to be searched, and the persons or things to be seized' . . . ." (quoting McDonald v. United States, 335 U.S. 451, 455 (1948))); *see also* U.S. CONST. amend. IV (requiring the Government to "particularly describ[e] the place to be searched, and the persons or things to be seized"). This assumes of course that the mosaic theory application of the Fourth Amendment triggers the probable cause and warrant requirements. *See infra* Part II.B.3.

person herself who has committed a crime or some combination of the two? And how can the police state a particular location when the mosaic contemplates long-term surveillance over many locations?

Interestingly, scholars have not introduced this theory in the Internet context, or more specifically, as a way to protect social networking communications.[22] Much like the development of electronic surveillance, here too, technology has frustrated the ability to protect information under the Fourth Amendment. The problem, again, is the Third Party Doctrine, only this time the voluntary disclosure is made to an Internet service provider ("ISP") instead of another person.[23] Nearly all communications over the Internet—including social networking sites—are housed in these proprietary systems for various periods of time in order to facilitate the transmission.[24] Under a strict application of this doctrine, none of these communications merit Fourth Amendment protection.[25] Scholars have presented different ways to protect these communications, though they have not adequately accounted for social networking communications.[26]

The issue is particularly relevant because of the recent news that the National Security Agency ("NSA") has been monitoring communications from e-mail servers such as Google, Yahoo, and Facebook, to name a few.[27] Under the Third Party Doctrine, the government may be free to collect this

[22] Scholars invoking this theory in the Internet context have simply focused on the collection of raw data over this medium without discussion of the unique nature of social networking communications. *See, e.g.*, Erin Smith Dennis, *A Mosaic Shield:* Maynard*, The Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 740-41 (2012) (discussing the mosaic theory in light of digital cable and the Internet, among other things, with no mention of social networking communications); David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. & CRIMINOLOGY 745, 763 (2013) (detailing concerns over the aggregate of information that can be gleaned from Internet usage via URL and online shopping records).

[23] *See infra* Part III.A (addressing the difficulty in affording protection to voluntarily disclosed information held on ISPs, though users subjectively do not intend for this information to be available to others). By signing up for Facebook, for instance, a user acknowledges that the company may hold her information. *See infra* note 317 (discussing the legal terms through which Facebook users permit the company to hold this information).

[24] *See infra* notes 312-314 and accompanying text (discussing the various ISP data storage techniques used by e-mail and social networking companies).

[25] *See* Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 329 (2011) (arguing that Facebook users are not entitled to Fourth Amendment protection because they voluntarily acknowledge that their information will be stored by a third party).

[26] *See infra* note 329 and accompanying text (discussing a number of Fourth Amendment theories to protect information stored in ISPs).

[27] *See infra* Part III.A (discussing recent NSA monitoring of e-mail exchanges).

information without any Fourth Amendment scrutiny.[28] A mosaic-based theory can provide a constitutional solution that is both conceptually and practically sound.[29] The refrain of "the sum is greater than the parts" continues to apply; only this time it is a group of communications, not public movements, that informs the analysis.[30] In order to apply a mosaic-based approach, there still needs to be some norm or value that would justify why a collection of social networking communications merits privacy protection, even if on their own, the communications do not.[31] For the reasons already mentioned, it won't do to simply say that society finds this type of intrusion unreasonable.[32]

Perhaps ironically, Justice Sotomayor's concurrence in *Jones* provides a direction here, when she states that the long-term GPS surveillance may chill "associational and expressive freedoms."[33] Because her statement was relatively brief, it is not clear how she intended to incorporate this right of association.[34] Moreover, the right of association contemplates two

[28] *See infra* Part III.A. Though this type of activity may still be illegal under applicable law, this Article is concerned with Fourth Amendment not legislative protection. *See infra* Part I.C (explaining that while federal courts remain divided on whether metadata collection is illegal under the Fourth Amendment, the D.C. Circuit has held that prolonged data collection does violate the Constitution). Finding Fourth Amendment protection in these communications does not mean that the government cannot otherwise acquire this information for national security or other reasons but rather that it would have to satisfy the reasonableness requirements of the Fourth Amendment before conducting this activity. *See infra* Part III.A; *infra* note 239.

[29] *See* United States v. Jones, 132 S. Ct. 945, 956-57 (2012) (Sotomayor, J., concurring) (presenting potential issues that need not be resolved in *Jones* resulting from application of the mosaic theory to these longer-term surveillance projects, but claiming the issues are "difficult," not "impossible" to solve).

[30] *See* United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010) ("[T]he whole of one's movements is not exposed constructively even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.").

[31] *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (highlighting the chilling effect that the government's creation of aggregated personal data records may have on individuals' freedoms of expression and association).

[32] *See, e.g.*, Kerr, *The Mosaic Theory*, *supra* note 10, at 349 (opining that relying on societal perspective is particularly flawed when technology is involved because few individuals appreciate the extent of technological surveillance in everyday life, thus discrediting their opinions as to reasonableness).

[33] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.").

[34] Scholars have debated whether she wanted the First Amendment to apply directly or only indirectly through the Fourth Amendment reasonable expectation of privacy test. *See* Jonathan Witmer-Rich, *Surveillance, Chilling, and the First and Fourth Amendments*, PRAWFSBLAWG (July 15, 2013, 2:21 PM),

conceptually distinct types of association: expressive and intimate.[35] Expressive associations focus on the right to associate with others for purposes of engaging in First Amendment speech involving political, economic, religious, and cultural ends, whereas intimate associations focus on the right to develop close ties and bonds with others such that one can share personal thoughts, experiences, and beliefs.[36]

Incorporating expressive associational rights into Fourth Amendment jurisprudence is not a new concept and pre-dates *Jones*.[37] While these discussions did not contemplate a mosaic-based application, scholars have argued that this principle should be incorporated into a determination of reasonable expectation of privacy, especially in the face of electronic monitoring.[38] It is important to note that expressive associational rights would not apply directly, but rather the underlying norm would become part of the Fourth Amendment calculus.[39] In the mosaic context, this would mean assessing whether long-term surveillance by the government stymies individuals from engaging in these expressive associations such that the movements garner Fourth Amendment protection.[40] But it is not clear whether this value can be incorporated in this way without also jeopardizing the Doctrines. If the concern is people gathering in political or religious groups, it would appear that any type of surveillance, regardless of length or use of undercover informants, could deter this behavior for fear that the government is watching.[41]

However, little attention has been paid to intimate associations and how protecting these types of relationships may play a role when applying the reasonable expectation of privacy test under the Fourth Amendment.[42]

---

http://prawfsblawg.blogs.com/prawfsblawg/2013/07/surveillance-chilling-and-the-first-and-fourth-amendments.html, *archived at* http://perma.cc/42LE-SLRG (arguing that, while other bloggers think Justice Sotomayor was making a First Amendment argument, the opinion actually "is not flagging the First Amendment—it is one of the factors that suggests to Justice Sotomayor that people may have a reasonable expectation of privacy in whether their movements are tracked (at least long-term) by GPS").

[35] *See infra* notes 265-267 and accompanying text.

[36] John D. Inazu, *Virtual Assembly*, 98 CORNELL L. REV. 1093, 1099 (2013) [hereinafter Inazu, *Virtual Assembly*] (opining that intimate associations are those "small and selective groups that we form with those who are closest to us").

[37] *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 806 (1994) (explaining that courts understood, as early as the 1970s, that "First Amendment concerns could well trigger special Fourth Amendment safeguards").

[38] *See infra* Part II.C.

[39] *See infra* Part II.C.

[40] *See infra* notes 277-278 and accompanying text (discussing long-term surveillance as a deterrent for individuals who would engage in otherwise protected associational activities).

[41] *See infra* Part II.C.

[42] *See, e.g.*, Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After Lawrence*, 57 UCLA L. REV. 1, 21 (2010) (discussing the Court's protection of intimate

Deriving from both First Amendment and due process principles, these relationships seek to preserve bonds between family, close friends, or those with whom one can share personal aspects of one's life.[43] Perhaps the thinking is that since this type of personal relationship typically happens in a person's home or over the phone—places where Fourth Amendment protection already applies—there is less of a need to incorporate this value.[44] But it turns out that using this principle in conjunction with a mosaic approach can effectively protect social networking communications over the Internet.

Social networking sites have revolutionized how people communicate.[45] The Internet is no longer simply a place to transmit information efficiently and quickly. It is now a space to develop and maintain relationships. This Article uses Facebook as the exemplar for this type of activity, though its analysis would apply to any social networking platform where the communications are stored on third party servers.[46] Facebook allows users to send messages, post pictures and updates, and video-conference, among other activities.[47] Combined, these tools provide a platform to create social bonds, which psychologists and scholars alike have found to be just as real as face-to-face

associations in the past under First Amendment and due process principles of "interpersonal liberty," as opposed to Fourth Amendment "personal privacy").

[43] Roberts v. U.S. Jaycees, 468 U.S. 609, 617-18 (1984) ("[B]ecause the Bill of Rights is designed to secure individual liberty, it must afford the formation and preservation of certain kinds of highly personal relationships a substantial measure of sanctuary from unjustified interference by the State.").

[44] *See* United States v. Karo, 468 U.S. 705, 714 (1984) (explaining that surveillance within a private dwelling certainly "violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence"); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[A] man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited.").

[45] *See infra* Part III.B (discussing the various changes that social networking sites have brought to personal Internet communication, prompting this analysis of a somewhat novel realm of privacy protection).

[46] For instance, the arguments herein may apply to Google+, Google's answer to Facebook. Ryan Lytle, *The Beginner's Guide to Google+*, MASHABLE (Oct. 27, 2013), http://mashable.com/2013/10/27/google-plus-beginners-guide/, *archived at* http://perma.cc/M88G-BK6S (addressing Google+'s vast social networking capability, including several features that mirror group interaction on Facebook). That said, Facebook remains the dominant Internet social media tool. *See, e.g.*, Helen Leggatt, *Facebook Dominates Social Logins, but Google+ Gaining Ground*, BIZREPORT (July 19, 2013), http://www.bizreport.com/2013/07/facebook-dominates-social-logins-but-google-gaining-ground.html, *archived at* http://perma.cc/9SKC-Q9ME ("[D]ata showed Facebook dominating social logins with 52% of the total. Google+ came second with 24%, and Yahoo third at 17%.").

[47] *See infra* Part III.B (highlighting an individual's ability to construct an online identity through Facebook).

relationships.[48] These Internet relationships embody the same principles of autonomy, identity, and community as are found in traditional relationships.[49] Indeed, for many young users, this type of relationship formation has replaced face-to-face meetings.[50]

Enter the mosaic theory with a focus on intimate associations.[51] While individual social networking communications would not be protected because of the Third Party Doctrine, in the aggregate, these communications are more than just a bundle of transmissions—together they are constitutive of an intimate relationship. If courts care about the government not interfering in these relationships in the face-to-face context, via direct application of intimate associational rights, they should similarly care about these relationships on the Internet when assessing Fourth Amendment protection.[52] This means finding that the underlying social networking communication passes the Fourth Amendment reasonable expectation of privacy test, because it is part-and-parcel of an intimate relationship.[53]

The application of the mosaic doctrine in this narrow context has the benefit of preserving the viability of the Doctrines.[54] The government, without a warrant, can still use undercover agents and collect incriminating statements from potential suspects. This may sound puzzling, because the aggregate of face-to-face communications between a suspect and an undercover informant may also be constitutive of an intimate relationship, particularly if the agent takes time to develop a close bond with the suspect. This may incorrectly suggest an application of my mosaic principle. Here, the government plays a substantive role in the relationship, unlike in the social networking context, where the government acquires the information directly from the ISP—an entity that simply serves to facilitate the transmission.[55] There is also neither a

[48] John A. Bargh & Katelyn Y.A. McKenna, *The Internet and Social Life*, 55 ANN. REV. PSYCHOL. 573, 586-87 (2004) (opining that online relationships are not only similar to face-to-face interactions but often voluntarily result in "real world" contact once these personal relationships develop); James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1154 (2009) (discussing the strength of online relationships).

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

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

[51] *See infra* Part III.B (explaining how the mosaic theory can be applied to protect social media communications).

[52] *See infra* Part III.B (discussing the similarities between face-to-face relationships and relationships formed over the internet, justifying the application of intimate associational rights to relationships formed online).

[53] *See infra* Part III.C.1 (clarifying which types of social media communications are part of intimate relationships and therefore have reasonable expectation of privacy protection).

[54] *See infra* Part III.C.2 (explaining how application of the mosaic theory to social media communications does not conflict with the Doctrines).

[55] The key here is that the possibility of betrayal, as found in the undercover context, is assumed in any intimate relationship; otherwise there would be no trust, an essential element of such a relationship. Anthony Evans, *Elements of Trust: Risk and Perspective-Taking*, 47

disruption of the Public Disclosure Doctrine nor of the government's unfettered ability to monitor a person's public movements. Because this capability does not interfere with a person's ability to develop intimate relationships, the government is free to conduct this type of surveillance of individuals without a warrant.[56]

Applying the mosaic theory to social networking communications over the Internet also faces less practical hurdles than applying it to GPS police surveillance.[57] The probable cause and warrant requirements would play out no differently than any search of a physical location. Police would specify the nature of the incriminating information (e.g., a particular e-mail or photograph) and the individual or individuals to whom it was sent.[58] The end result is a narrowly applied mosaic that protects a person's ability to develop relationships online without otherwise altering the basic Fourth Amendment landscape, most notably the police's ability to investigate suspects and take advantage of the Doctrines.

The Article is divided into three parts. Part I details the history of the Doctrines and how they survived earlier technological advancements. This Part also discusses the recent news of the NSA collection of Verizon call data and puts this surveillance in the appropriate doctrinal and historical context. Part II focuses on the mosaic theory as articulated in *United States v. Jones*. It lays out the basic refrain and argues that the theory ultimately suffers from conceptual, doctrinal, and practical difficulties. Part III discusses how the mosaic theory can effectively provide Fourth Amendment protection to social networking communications over the Internet, where such protection currently does not exist. It highlights the recent news of the NSA working with Facebook, among others, to monitor communications and the resultant privacy implications. This Part then argues that social networking communications, in the aggregate, are constitutive of intimate associations that should be protected under the Fourth Amendment and suggests how this protection can be achieved without fundamentally altering the current Fourth Amendment landscape.

J. EXPERIMENTAL PSYCHOL., 171, 171 (2011) (explaining how the possibility of betrayal affects one's decision to trust, an essential element of personal relationships).

[56] *See infra* Part III.C.2 (explaining how physical surveillance of a suspect's public movements will not affect the suspect's ability to form intimate relationships via social media).

[57] *See infra* Part III.C.3 (detailing the types of social media communications and relationships that would be protected).

[58] *See infra* Part III.C.3 (suggesting ways that the government could apply for a search warrant to access the protected communications).

I. BACKGROUND OF THE THIRD PARTY AND PUBLIC DISCLOSURE DOCTRINES

A. *The Beginnings of the Doctrines:* Katz *and the Reasonable Expectation of Privacy*

Early Fourth Amendment cases readily acknowledged the Doctrines. The reason centers on the fact that historically the Fourth Amendment only protected physical intrusions onto an individual's property.[59] Only this type of government intrusion required probable cause and a warrant issued by a magistrate.[60] *Olmstead v. United States*[61] stands as a principal expression of this concept of privacy.[62] The government, without a warrant, tapped the defendant's phone lines by making physical intrusions into parts of the phone lines that were not on the defendant's property.[63] The Court found that the government did not violate the Fourth Amendment because it never trespassed onto the defendant's land.[64]

This decision led the way to other decisions concerning disclosure to

---

[59] Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that a defendant's Fourth Amendment rights are not violated "unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house").

[60] U.S. CONST. amend. IV; United States v. Ventresca, 380 U.S. 102, 105-07 (1965) (discussing the Fourth Amendment requirements needed to sustain a search performed pursuant to a warrant issued by a magistrate). The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV. There are narrow exceptions to the warrant requirement, such as the automobile exception, exigency, search incident to arrest, but invocation of any such exception assumes that Fourth Amendment protection would otherwise apply. *See Ventresca*, 380 U.S. at 106-07 ("[E]xceptions to the requirement that searches and seizures be undertaken only after obtaining a warrant are limited."). If there were no reasonable expectation of privacy in the first instance, there would be no need to carve out an exception. *See, e.g.*, Stephen P. Jones, *Reasonable Expectations of Privacy: Searches, Seizures, and the Concept of Fourth Amendment Standing*, 27 U. MEM. L. REV. 907, 950-51 (1997) (explaining that requiring an exception to the warrant requirement in automobile searches precludes a conclusion that there is no reasonable expectation of privacy therein); Kerr, *Four Models*, *supra* note 10, at 507-08 (explaining that the Fourth Amendment only requires a search warrant when there is a reasonable expectation of privacy).

[61] 277 U.S. 438.

[62] *Id.* at 466.

[63] *Id.* at 456-57 ("The insertions were made without trespass upon any property of the defendants.").

[64] *Id.* at 464-66 ("The Amendment does not forbid what was done here. . . . There was no entry of the houses or the offices of the defendants.").

informants and the public at large. In *Lopez v. United States*,[65] for instance. the Court found no constitutional problem with an undercover informant who recorded incriminating statements made by the defendant that the government later used against him at trial.[66] As long as an informant did not trespass on a defendant's land, the Fourth Amendment did not apply to any statements made to the informant.[67] It is of no consequence that a defendant may be under the "misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[68] This misplaced belief does not change the fact that the defendant voluntarily disclosed the information and thus took the risk that the government might obtain it without a warrant and use it against him at trial.[69] This became known as the Third Party Doctrine.[70]

Similarly, as long as the police did not trespass on a person's property, any surveillance of the person's public movements was not protected under the Fourth Amendment and no warrant was required.[71] In *Hester v. United States*,[72] the Court found no issue with the government observing the movements of the defendant outside his home from a distance away.[73] Because

[65] 373 U.S. 427 (1963).

[66] *Id*. at 439 ("And the device was not planted by means of an unlawful physical invasion of petitioner's premises under circumstances which would violate the Fourth Amendment.").

[67] *Id.* ("[The device] was carried in and out by an agent who was there with the petitioner's assent."); *see* Hoffa v. United States, 385 U.S. 293, 302-03 (1966) (holding no right of privacy was violated because "[the informant] did not enter the suite by force or stealth"); Lewis v. United States, 385 U.S. 206, 210-12 (1966) (explaining that the Fourth Amendment was not violated because the government agent was invited into petitioner's home, even though the invitation was under false pretenses). Using deceit to enter a defendant's property does not constitute a trespass and therefore use of any information disclosed to the government agent upon entry would not violate the Fourth Amendment. *E.g.*, *Lewis*, 385 U.S. at 209-10 (highlighting the difference between information revealed by an undercover agent engaged in unwelcome ransacking and information obtained from intended disclosures, even if the agent's motives were unknown); On Lee v. United States, 343 U.S. 747, 752–53 (1952) ("[T]he claim that Chin Poy's entrance was a trespass because consent to his entry was obtained by fraud must be rejected.").

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

[69] United States v. Miller, 425 U.S. 435, 443 (1976) (finding that it did not matter that the defendant gave personal bank records to bank for limited purpose because act of disclosure alone vitiates all expectation of privacy).

[70] *See* United States v. White, 401 U.S. 745, 749 (1971) (holding that there is no expectation of privacy in information that is revealed to third parties); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 583-85 (2011) (discussing the history of the Third Party Doctrine).

[71] Hester v. United States, 265 U.S. 57, 59 (1924) ("[T]he special protection accorded by the Fourth Amendment to the people in their 'persons, houses, paper, and effects,' is not extended to the open fields.").

[72] *Id.*

[73] *Id.* at 58-59 (holding that the defendant had voluntarily disclosed his illegal activity by

the defendant's actions were out in the open for all to see, these movements garnered no Fourth Amendment protection.[74] This became known as the Public Disclosure Doctrine, which says that there is no privacy protection for a person's movements in public.[75]

Katz v. United States[76] dramatically altered how the Court conceptualized Fourth Amendment protection.[77] Privacy was no longer restricted to physical intrusions on a person's property.[78] Any situation where a person has a reasonable expectation of privacy qualifies for protection.[79] As the Court famously observed, "the Fourth Amendment protects people, not places."[80]

In *Katz*, 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.[81] Even though the device was not installed on the defendant's property, the Court found that this recording violated the defendant's Fourth Amendment right to privacy.[82] In his concurrence, Justice Harlan articulated the now well-known two-part test for the application of Fourth Amendment protection: a person must subjectively expect privacy and this expectation must be objectively reasonable.[83]

---

engaging in it in open view, which precluded a finding of any Fourth Amendment seizure by government agents). The Court found that the government was not trespassing on the property because they were observing from an open field outside the house, an area that the Fourth Amendment did not protect. *Id.* For a discussion of how courts have wrestled with the constitutional trespass and the open fields doctrines, see James Tomkovicz, *Beyond Secrecy's Sake: Towards an Expanded Version of the Fourth Amendment Privacy Province*, 36 HASTINGS L. J. 645, 714-21 (1985) (discussing the ways that courts tried to deal with the open fields doctrine once the reasonable expectation of privacy test was introduced).

[74] *Hester*, 265 U.S. at 58.

[75] *See, e.g.*, 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); 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.'").

[76] 389 U.S. 347.

[77] *See id.* at 353 ("[T]he reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

[78] *Id.* (holding that the trespass doctrine was no longer controlling).

[79] *Id.* ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied . . . .").

[80] *Id.* at 351.

[81] *Id*. at 348 ("[T]he Government was permitted . . . to introduce evidence of the petitioner's end of telephone conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls.").

[82] *Id.* at 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

[83] *Id.* at 361 (Harlan, J., concurring) ("My understanding of the rule . . . is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of

Here, the Court found both requirements were met. The defendant purposefully entered the telephone booth, shut the door behind him, and paid the toll that permits him to place a call.[84] The Court found that, collectively, these actions exhibited an expectation of privacy and that this belief was reasonable.[85] Thus, the government was required to obtain a warrant before intercepting the call.[86]

Because a defendant's subjective expectation is easily satisfied, the key part of the test focuses on the reasonableness requirement of the second prong.[87] But the term "reasonable expectation of privacy" has remained, even today, a murky concept. The basic premise seems straightforward enough: Is this belief one that society determines is reasonable? But, as it turns out, scholars have struggled with exactly what this means and how courts have conducted this analysis.[88]

To date, the Supreme Court has not adopted a single test for this assessment.[89] Professor Orin Kerr has attempted to provide a comprehensive

privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"); *see* Eric D. Bender, Note, *The Fourth Amendment in the Age of Aerial Surveillance: Curtains for the Curtilage?*, 60 N.Y.U. L. REV. 725, 753 (1985) ("The essential focus of *Katz* analysis is on the *reasonableness* of expectations of privacy."). Another way of viewing the first component is that the defendant must *exhibit* a subjective expectation of privacy, not merely *have* such an expectation. *Id.* at 743 ("The first part of the *Katz* test requires the courts to determine whether the dweller exhibited an actual, subjective expectation of privacy in the curtilage.").

[84] *Katz*, 389 U.S. at 352 (majority opinion) ("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 broad-cast to the world.").

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

[86] *Id.* at 358. There are exceptions to the warrant requirement (e.g., consent, exigent circumstances) that were not applicable here. *See* United States v. Karo, 468 U.S. 705, 717 (1984) (citing cases that discuss the various warrant exceptions).

[87] *See, e.g.*, 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) (citing cases showing that "defendant's subjective expectation was easily satisfied, [and that] Fourth Amendment protection generally hinged upon satisfying the reasonableness requirement of the second prong").

[88] *See, e.g.*, Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002) (explaining that when courts decide what creates a reasonable expectation of privacy, they are asking what constitutes a search); Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 29 (1988) (explaining that, in defining a reasonable expectation of privacy, "the Court has produced a series of inconsistent and bizarre results that it has left entirely undefended"); Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1107 (1987) (suggesting that legitimizing a subjective expectation of privacy as reasonable is "distressingly unmanageable").

[89] *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 715 (1987) ("We have no talisman that

account of the various tests or models the Court has used over time in defining reasonable expectation of privacy.[90] He argues that since *Katz*, the Court has used one, or a combination, of four tests or models in making this assessment.[91] The first looks at whether a reasonable person would think that the information should be protected:[92] Based on customs or social expectations, would someone expect the information to remain private?[93] A second focuses on whether the kind of information obtained is worthy of protection:[94] Is there something special about the nature of the information such that it merits protection?[95] A third test considers whether the government's conduct violates some established legal norm or right:[96] Did the

determines in all cases those privacy expectations that society is prepared to accept as reasonable."); Oliver v. United States, 466 U.S. 170, 177 (1984) ("No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion not authorized by warrant."); *see also* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(a), at 380 (3d ed. 1996) ("The Supreme Court . . . has never managed to set out a comprehensive definition of the word 'searches' as it is used in the Fourth Amendment.").

[90] *See* Kerr, *Four Models*, *supra* note 10, at 506 (explaining that the singular label "'reasonable expectation of privacy' . . . masks several distinct but coexisting approaches").

[91] *Id.* ("Four approaches predominate, together reflecting four different models of Fourth Amendment protection.").

[92] *Id.* at 508-12 ("According to this approach, a reasonable expectation of privacy depends on the chance that a sensible person would predict that he would maintain his privacy.").

[93] *Id.* The inquiry here is descriptive, not normative. It looks at what people actually think. *Id.*; *see also* Bond v. United States, 529 U.S. 334, 337 (2000) (finding that an officer's "probing tactile examination" of defendant's luggage on a bus violated his reasonable expectation of privacy because the probing had exceeded the usual handling of passenger bags); Minnesota v. Olsen, 495 U.S. 91, 98 (1990) (finding that defendant had reasonable expectation of privacy in a friend's apartment for the night because "staying overnight in another's home is a longstanding social custom").

[94] Kerr, *Four Models*, *supra* note 10, at 512-15 (suggesting that defining a "reasonable expectation of privacy" may require a "normative assessment of the value of the information").

[95] *See, e.g.*, Dow Chemical v. United States, 476 U.S. 227, 238 (1986) (holding that aerial photographs of chemical plant did not violate reasonable expectation of privacy because they only revealed the outline of building and no intimate details); United States v. Jacobson, 466 U.S. 109, 123 (1984) (holding that a field test performed on package did not violate reasonable expectation of privacy because it could only disclose the crime and reveal no other personal information); United States v. Karo, 468 U.S. 705, 714 (1984) (holding that the monitoring of a beeper placed in a can of ether that was later brought inside the home and which revealed details about the home violated reasonable expectation of privacy).

[96] Kerr, *Four Models*, *supra* note 10, at 516-19 ("If the government broke the law in order to obtain the information it did, the government conduct violated a reasonable expectation of privacy.").

government violate some law or other policy in obtaining the information?[97] And the fourth considers whether the conduct should be protected as a matter of public policy:[98] What are the overall consequences of allowing this police practice?[99]

While *Katz* did not alter the general applicability of the Doctrines, it did impact how the Court has conceptualized "reasonable expectation" in this context.[100] Under the aforementioned classification scheme, it would appear that the Court, when assessing disclosures to the public or others, has favored the second model and its focus on the nature of the communication.[101] Simply

[97] *See* Florida v. Riley, 488 U.S. 445, 451 (1989) (holding that investigators flying helicopter over property did not violate the defendant's reasonable expectation of privacy because there was no violation of Federal Aviation Administration altitude regulations, which only applied to fixed-wing aircraft); *Dow Chemical*, 476 U.S. at 249 (Powell, J., dissenting) (arguing that because aerial photographs interfered with trade secret protections, defendant had reasonable expectation of privacy in the photographs); Rakas v. Illinois, 439 U.S. 128, 148 (1978) (holding that passengers in car had no reasonable expectation of privacy in the car because they lacked a property right in the car or a possessory right in the items seized). *But see* California v. Greenwood, 486 U.S. 35, 43 (1988) (finding that in the context of the government searching the defendant's trash, state law does not govern reasonable expectation of privacy analysis).

[98] Kerr, *Four Models*, *supra* note 10, at 519-22 ("Judges must consider the consequences of regulating a particular type of government activity, weigh privacy and security interests, and opt for the better rule.").

[99] Kyllo v. United States, 533 U.S. 27, 40 (2001) (finding that use of a thermal imaging device to detect the interior temperature of a house eroded the assurances against invasion of home by the government); Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (finding that allowing the government to monitor phone numbers was not consistent with "a free and open society" and would "impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society").

[100] United States v. Miller, 425 U.S. 435, 442 (1976) ("We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."); United States v. White, 401 U.S. 745, 749 (1971) (reaffirming the principle that the defendant bears the risk of betrayal after disclosure to a third party, including an informant); *see infra* Part I.B (discussing the persistence of the Doctrines despite technological advances).

[101] *See* United States v. Sparks, 750 F. Supp. 2d 384, 392 (D. Mass. 2010) ("Rather than using [an approach focused on what a person would deem as reasonable expectations of privacy], in the context of governmental use of new technologies, the Supreme Court repeatedly has focused on whether the nature of the information revealed is private and thus worthy of constitutional protection."); Kerr, *Four Models*, *supra* note 10, at 511-12 (analyzing Supreme Court considerations of the nature of the information in question when deciding Fourth Amendment cases); *see infra* Part I.B; *see also* Kerr, *The Mosaic Theory*, *supra* note 10, at 349 (citing the above quote from *Sparks*); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588-90 (2009) [hereinafter Kerr, *Third-Party Doctrine*] (arguing for a consent-based approach to the Third Party Doctrine); Sonia K. McNeil, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199, 216-18 (2011) (arguing that individual utility consumption data is sensitive and that the Third Party Doctrine should

put, the voluntary disclosure of the information is sufficient to vitiate any privacy protection.[102] The fact that the defendant may believe that the information will remain secret does not change the nature of the disclosure. The Court summarizes it in the following way:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[103]

The focus on the nature of the communication may also explain why some scholars have characterized the Doctrines as waiver or consent principles.[104] Understood in this way, a person 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.[105] It is not relevant that the individual makes this disclosure thinking that the information or her movements will remain private—the voluntary nature of the act vitiates all privacy protection.[106]

B. *Survival of the Doctrines Through Early Technological Advancements*

Post-*Katz*, the Doctrines survived early technological advances in surveillance. In *United States v. Knotts*,[107] the Court had an opportunity to discuss the ramifications of the Public Disclosure Doctrine as it relates to

not defeat privacy protections for this data).

[102] Kerr, *Four Models*, *supra* note 10, at 511-12 ("In all of these cases, the Court held that providing information to the third party eliminated any reasonable expectation of privacy no matter how unlikely it was that the friend would betray the suspect's confidence.").

[103] *Miller*, 425 U.S. at 443.

[104] *See, e.g.*, Kerr, *Third-Party Doctrine*, *supra* note 101, at 588-90 (analyzing the Doctrines under consent and waiver principles); McNeil, *supra* note 101, at 216-18 (considering the Third Party Doctrine as one of consent).

[105] *See, e.g.*, Fabio Arcila, *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 37-47 (2012) (discussing how under the Public Disclosure Doctrine, a defendant assumes the risk the information will be disclosed to the government); Kerr, *Third-Party Doctrine*, *supra* note 101, at 588-90 (arguing that the Third Party Doctrine should be viewed as a form of consent where the disclosure eliminates expectations of privacy because the target voluntarily consents to the disclosure); McNeil, *supra* note 101, at 216-18 (discussing and ultimately disagreeing with the argument that the Third Party Doctrine should be interpreted as a doctrine of consent).

[106] *See, e.g.*, *Miller*, 425 U.S. at 443; Kerr, *Third-Party Doctrine*, *supra* note 101, at 588-89 (discussing that a person consents or waives his or her right to privacy when that person discloses information to an informant, even if he or she does not know that the person is working for the government).

[107] 460 U.S. 276 (1983).

short-term surveillance using a beeper-based technology.[108] The police lawfully placed a beeper inside a container of chemicals purchased by the defendant.[109] The authorities suspected that the defendant had been purchasing the chemicals to manufacture illicit drugs.[110] The beeper emitted a signal, which allowed the authorities to track the package for an entire afternoon.[111] 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.[112] At that point, the authorities lawfully searched the cabin and arrested the defendant on charges of manufacturing illicit drugs.[113]

The defendant contended that the consistent monitoring of the beeper signal without a warrant violated the defendant's reasonable expectation of privacy under the Fourth Amendment.[114] The Court rejected this claim, likening the surveillance of the beeper signal to traditional visual surveillance of a car.[115] The Court stated that "[t]he governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways."[116] In doing so, the Court reaffirmed the Public Disclosure Doctrine and found that a person has no Fourth Amendment protection over movements in public.[117] The Court reasoned:

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

[108] *Id*. at 280-85 (deciding the case by applying the Public Disclosure precedents).

[109] *Id.* at 276 ("In this case, a beeper was placed in a five-gallon drum containing chloroform purchased by one of the respondent's codefendants.").

[110] *Id.* at 278 (stating that suspicion arose from an employer disclosure that the defendant stole chemicals that could be used in the manufacture of illicit drugs).

[111] *Id.* The police also relied on visual surveillance. *Id.*

[112] *Id.* (describing the defendant's travel from Minnesota to Wisconsin). The police used a helicopter to further monitor the beeper signal to its ultimate destination. *Id.*

[113] *Id.* at 279 ("Relying on the location of the chloroform derived through the use of the beeper and additional information obtained during three days of intermittent visual surveillance of respondent's cabin, officers secured a search warrant. . . . [O]fficers discovered a fully operable, clandestine drug laboratory in the cabin.").

[114] *Id.* The defendant did not challenge the warrantless installation of the beeper in the container. *Id.* n.*.

[115] *Id.* at 285 ("A police car following [the defendant] at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin owned by respondent, with the drums of chloroform still in the car.").

[116] *Id.* at 281. The Court made clear that the police did not use the beeper technology to monitor the container's movements inside the cabin. *Id.* at 285. All the movements monitored would have been visible to the naked eye outside the cabin. *Id.*

[117] *Id.* at 281-82.

travelling over particular roads in a particular direction . . . .[118]

Under the aforementioned reasonable expectation models, it would appear that the Court relied on the second model, or the nature of the information, in reaching its conclusion.[119] Because the movements of the car were disclosed to the public at large, these movements were not worthy of protection. It did not matter that, without the beeper system, the police would not have been able to follow the defendant to his ultimate destination.[120] The Court noted that this technological advancement simply augmented traditional police surveillance by providing a more efficient means to monitor a defendant's movements through public streets.[121] The Court, however, specifically left open the possibility of a different constitutional conclusion if the surveillance had lasted for a full day or longer.[122]

Relying on the same second model of privacy, the Court distinguished *Knotts* from *United States v. Karo*,[123] another case involving the monitoring of a container via a beeper system.[124] The critical difference centered on the nature of the information that was disclosed. The police in *Karo* were monitoring the container as it sat inside the home, not as it made its way through the public streets.[125] Because this information could not otherwise be verified but for entering the home, the Court found that the defendant had a reasonable expectation of privacy in it and thus the police monitoring required a warrant.[126]

In *Smith v. Maryland*,[127] the Court analyzed how the warrantless installation of an automated surveillance device affects the application of the Third Party Doctrine.[128] The government requested, and the phone company agreed, to

[118] *Id.*

[119] *See* Kerr, *Four Models*, *supra* note 10, at 543 ("The private facts model was used to regulate . . . the use of tracking devices in *United States v. Karo* and *United States v. Knotts*." (citations omitted)).

[120] *See Knotts*, 460 U.S. 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.").

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

[122] *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 will be needed." (citing Zurcher v. Stanford Daily, 436 U.S. 547, 566 (1978))).

[123] 468 U.S. 705 (1984).

[124] *Id.* at 715.

[125] *Id.*

[126] *Id.* at 714, 723.

[127] 442 U.S. 735 (1979).

[128] *Id.* at 742-46 (considering whether the defendant had a reasonable expectation of privacy in the numbers he dialed).

install a pen register at its central offices to record the numbers dialed from the defendant's home.[129] A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses from the phone; it does not record the substance of the conversation.[130]

In the instant case, the government used the pen register to ascertain that the defendant had made calls to the victim's house.[131] On the basis of this information, the government obtained a warrant and searched the defendant's house.[132] This ultimately led to the defendant being charged and convicted of robbing the victim.[133]

The defendant contended that the police violated his Fourth Amendment rights by monitoring the pen register and acquiring the victim's number without first obtaining a warrant.[134] The Court disagreed and found that the defendant had no reasonable expectation of privacy in the numbers dialed on his phone.[135] Like in *Knotts*, the Court seemed to adopt the second model of reasonable expectation by focusing on the nature of the information obtained.[136] The Court explained that "[w]hen he used his phone, [the defendant] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[137] This voluntary disclosure vitiated any privacy protection and the government could obtain the information without violating the Fourth Amendment.[138] Similar to a situation where a defendant discloses

[129] *Id.* at 737 (describing the installation of the pen register). Because the company acted on police request, the installation and use of the pen register constitutes "state action" under the Fourth Amendment. *Id.* at 739 n.4.

[130] *Id.* at 736 n.1.

[131] *Id.* at 737 (describing the findings resulting from review of the pen register).

[132] *Id.* ("The register revealed that on March 17 a call was placed from petitioner's home to McDonough's phone. On the basis of this and other evidence, the police obtained a warrant to search petitioner's residence." (citations omitted)).

[133] *Id.* at 737-38.

[134] *Id.* at 741. The defendant did not question the lawful installation of the register. *Id.* Because it was installed at the company's headquarters with the company's permission, there was no issue as to whether the police invaded or otherwise trespassed on the defendant's property. *Id.*

[135] *Id.* (differentiating the case at bar from *Katz* by stating that "pen registers do not acquire the *contents* of communications"). As for a subjective expectation of privacy in the numbers dialed, the Court found this unlikely because "phone users realize that they must 'convey' phone numbers to the telephone" in order to make the calls. *Id.* at 742. The numbers dialed in fact are part of the monthly bills generated by the companies. *Id.*

[136] *See* Kerr, *Four Models*, *supra* note 10, at 512 ("The private facts model focuses on the information the government collects, and considers whether it is worthy of constitutional protection.").

[137] *Smith*, 442 U.S. at 744.

[138] *Id.* (finding that the petitioner did not have a "reasonable expectation of privacy" because of his disclosure to the telephone company).

information to another person, the defendant in the instant case assumed the risk that the phone company would reveal the information to the government.[139] In affirming the application of the Third Party Doctrine, the Court made clear that conveying the information to a machine instead of a human being did not change the constitutional analysis.[140] The Court reasoned:

> 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.[141]

This conclusion is similar to the one in *Knotts*. Here too, the presence of the technological advancement did not alter the disclosure analysis. The respective advancement simply constituted a more efficient means of information gathering compared to its human counterpart.[142]

Justice Marshall's dissent is worth mentioning as it portends the concurrences in *United States v. Jones* and their discussion of how integral technology has become in our daily lives and what this means for the viability of the Doctrines.[143] Justice Marshall took issue with how the majority analogized the instant situation to the traditional case of a defendant disclosing information to another person. In the latter, "the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communication[]."[144] For Justice Marshall, this notion of choice is implicit in the concept of assumption of risk that the government may acquire the information.[145] He questioned whether this choice is realistically present in the case of disclosing numbers to the phone company when making phone calls has become such a personal and professional necessity in our daily lives.[146]

---

[139] *Id.* (holding that the petitioner assumed the risk that the third party would release the information to the government).

[140] *Id.*

[141] *Id.* at 744-45 (citation omitted).

[142] Indeed, the defendant conceded that if "he had placed his call through an operator, he could claim no legitimate expectation of privacy." *Id.* at 744.

[143] Justice Stewart filed a separate dissent in which he argued that the numbers dialed were on the same constitutional footing as the content of the conversations. *Id.* at 746-47 (Stewart, J., dissenting). Like the actual numbers, the content of the conversation itself must also be electronically transmitted by telephone company equipment. *Id.* If the latter are nonetheless constitutionally protected under the Fourth Amendment, it follows that the former should be as well. *Id.*

[144] *Id.* at 749 (Marshall, J., dissenting).

[145] *Id.* (arguing that the defendant should have a choice in whom he confides confidential information).

[146] *Id.* at 749-50 ("[U]nless a person is prepared to forgo use of what for many has

He went on to say that allowing the government to monitor and collect these numbers without a warrant also interferes with individuals' First Amendment interests.[147] He cited journalists and political organizations as examples of parties that would not want their personal contacts disclosed to the government by the phone company.[148] "Permitting government access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society."[149]

C. *NSA Collection of Verizon Call Data*

Federal courts recently discussed *Smith v. Maryland* in connection with the revelation last summer that the NSA was monitoring Americans' call logs. The initial leak indicated that the government was monitoring the metadata of thousands of Verizon subscribers, including numbers dialed, the origins of the calls, and the lengths of the calls.[150] There was no evidence that the government was otherwise monitoring the content of the calls.[151]

The Foreign Intelligence Surveillance Act ("FISA"), initially enacted in 1978, and its subsequent amendments, authorize the government to collect this type of data for national security reasons.[152] This Act also created a specialized

become a personal or professional necessity, he cannot help but accept the risk of surveillance.").

[147] *Id.* at 751 (expressing concern about the scope of potential privacy implicated by this decision).

[148] *Id.* (expressing concern about the disclosure of the personal contacts of an unpopular political organization).

[149] *Id.*

[150] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, *archived at* http://perma.cc/BC3D-2M5N (describing the extent of government collection of the phone records of U.S. citizens). This article leaked the FISA Court's order that allowed the government to monitor these call logs. *See In re* Application of the FBI for an Order Requiring Prod. of Tangible Things from Verizon Business Network Services, Inc., No. BR 13-109 (FISA Ct. Aug. 29, 2013) (classified version *available at* http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order, *archived at* http://perma.cc/BRW9-8Y53).

[151] *See* Greenwald, *supra* note 150 (stating that it was unknown if this was the only communications company targeted or if this company had been targeted in the past).

[152] *See* 50 U.S.C. §§ 1801-62 (2012). The Patriot Act further authorized amendments to the Act, which expanded the government's ability to collect information in international investigations from citizens. *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, title II, §§ 215, 218 (codified at 50 U.S.C. §§ 1804(a)(7), 1823(a)(7), 1861-62 (2012)) (describing access to business records and oversight by Congress); Jeremy C. Smith, Comment, *The USA Patriot Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 N.C. L. REV. 412, 420-25 (discussing how the Patriot Act has broadened the scope of the government's ability to conduct

federal court to hear requests from the government to acquire this type of information.[153] There is a debate as to whether these requests are granted on something less than a warrant based on probable cause and whether this still satisfies the reasonableness requirement under the Fourth Amendment.[154]

In the instant situation, the government received authority from the FISA Court to collect this metadata from Verizon subscribers for both domestic and international calls.[155] This triggered outcries from individuals and scholars alike as to whether these activities passed constitutional muster.[156] Whether the government's approval process satisfied the Fourth Amendment reasonableness requirement (i.e., getting a warrant based on probable cause) assumes in the first instance that the government's acquisition of the metadata falls within the purview of the Fourth Amendment.

Federal courts disagree on how this issue should be resolved. The FISA Court and a New York federal court—in response to a lawsuit filed by the

surveillance of citizens).

[153] *See* 50 U.S.C. §§ 1803, 1805 (stating the requirements for designating judges and issuing orders).

[154] *Compare In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (per curiam) (finding that FISA and Patriot Act Amendments satisfy Fourth Amendment because they are issued by a neutral magistrate), *with* Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons From Justice Powell and the* Keith *Case*, 41 U.C. DAVIS L. REV. 1259, 1299 (2008) (finding that the FISA Court's probable cause standard is lower than the probable cause standard under Fourth Amendment), *and* Smith, *supra* note 152, at 425 (finding that FISA Court orders are granted on something less than a warrant supported by probable cause). The ACLU has brought suit on behalf of the Verizon customers alleging that the government's surveillance practices violate the Fourth Amendment. *See* Complaint at 10, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (arguing that the surveillance exceeds its statutory authority and violates the First and Fourth Amendments).

[155] *See In re* Application of the FBI for an Order Requiring Prod. of Tangible Things from [Redacted], BR 13-158, 2013 U.S. Dist. LEXIS 157765, at *1 (FISA Ct. Oct. 11, 2013) (renewing an order requested by the FBI compelling the production of call records from a telephone company); *In re* Application of the FBI for an Order Requiring Prod. of Tangible Things from [Redacted], BR 13-109, 2013 U.S. Dist. LEXIS 134786 (FISA Ct. Aug. 29, 2013) (granting an order requested by the FBI to compel a telephone company to disclose call records).

[156] *See, e.g.*, James Joyner, *FISA, Blanket Searches, and the Fourth Amendment*, OUTSIDE THE BELTWAY (June 7, 2013), http://www.outsidethebeltway.com/fisa-blanket-searches-and-the-4th-amendment/, *archived at* http://perma.cc/36XS-MKQN ("[C]an information obtained this way, bypassing the protections required for traditional searches, then be brought in to traditional cases? If so, that would indeed be a worrisome erosion of Americans' civil liberties."); James Kilmek, *Government Surveillance: They're Watching You But Is It Legal?*, PHANDROID (June 13, 2013), http://phandroid.com/2013/06/13/fisa-4th-amendment-surveillance/, *archived at* http://perma.cc/U3G8-CDVV ("There's been a lot of talk about government surveillance by the NSA, pursuant to the Patriot Act, and whether it's legal.").

ACLU—recently found that this information does not fall under the Fourth Amendment and thus the NSA is free to collect it.[157] Citing *Smith v. Maryland*, the decisions made clear that Verizon telephone users voluntarily convey this information to the telephone company in the normal course of business and thus assume the risk that the company will provide the information to the government.[158] Referencing *United States v. Jones*, the FISA Court also noted that the "Supreme Court may some day revisit the third party disclosure principle in the context of the 21st century communication technology, but that day has not arrived."[159]

The D.C. District Court reached a different conclusion, granting a preliminary injunction to stop the NSA from collecting this metadata.[160] Interestingly, the court found that—even though a Verizon customer voluntarily disclosed this information in the normal course of business—the widespread data collection over multiple years distinguished this case from *Smith v. Maryland* where the government only collected a limited amount of data for a small-scale investigation.[161] The court seemed to rely on *Jones* and

[157] *See ACLU*, 959 F. Supp. 2d at 752 (holding that telephone metadata was not protected by the Fourth Amendment); *In re Application of the FBI for an Order Requiring Prod. of Tangible Things from [Redacted]*, BR 13-158, 2013 U.S. Dist. LEXIS 157765, at *4 (holding that telephone metadata was not protected by the Fourth Amendment); *Application of the FBI for an Order Requiring Prod. of Tangible Things from [Redacted]*, BR 13-109, 2013 U.S. Dist. LEXIS 134786, at *7-9 (holding that telephone metadata was not protected by the Fourth Amendment).

[158] *Application of the FBI for an Order Requiring Prod. of Tangible Things from [Redacted]*, BR 13-109, 2013 U.S. Dist. LEXIS 134786, at *7-9 (holding that the Third Party Doctrine precluded a reasonable expectation of privacy in cellphone metadata). There was no allegation that the government trespassed on any individual's property or otherwise monitored the content of the calls. *ACLU*, 959 F. Supp. 2d at 749-53; *Application of the FBI for an Order Requiring Prod. of Tangible Things from [Redacted]*, BR 13-109, 2013 U.S. Dist. LEXIS 134786, at *7-9.

[159] *Application of the FBI for an Order Requiring Prod. of Tangible Things from [Redacted]*, BR 13-158, 2013 U.S. Dist. LEXIS 157765, at *6. The court also cited to *Jones* and noted that the Justices' concerns about "the precise, pervasive monitoring by the government of a person's location" were not relevant here since the government was not monitoring the precise location of individuals. *Id.* at *5. More generally, federal circuits are in disagreement as to whether cell phone location data is covered by the Fourth Amendment. *Compare In re* Application of the United States of America For Historical Cell Site Data, 724 F.3d 600, 609-10 (5th Cir. 2013) (citing *Smith v. Maryland* and thus finding that cell phone site data is not protected under Fourth Amendment), *with In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317-18 (3d Cir. 2010) (finding that cell phone site data is protected because cell phone customers do not meaningfully volunteer to disclose this information to their cell phone providers).

[160] *See* Klayman v. Obama, 957 F. Supp. 2d 1, 9-10 (D.D.C. 2013).

[161] *Id.* at 32-34 ("In *Smith,* the Court considered a one-time, targeted request for data regarding an individual suspect in a criminal investigation . . . which in no way resembles

the mosaic theory as a mechanism by which this type of metadata would be constitutionally protected.[162]

II. THE MOSAIC THEORY AND COMBATTING LONG-TERM SURVEILLANCE EFFORTS

A. United States v. Jones

The D.C. Circuit, in *United States v. Maynard*,[163] first articulated the contours of the mosaic theory.[164] The case involved the use of a GPS device to monitor the movements of the defendant who, along with his co-conspirators, was suspected of running a drug conspiracy.[165] The government, without complying with the terms of the warrant received, installed a GPS device on the defendant's car while it was parked in a public parking lot.[166] The device transmitted signals of the car's location to a government computer every few seconds.[167] Using this device, the government monitored the defendant's movements over twenty-eight days, which produced 2,000 pages of data.[168] This information allowed the government to coordinate the defendant's movements with his co-conspirators.[169] This evidence ultimately helped convict the defendant of drug conspiracy charges.[170]

On appeal, the defendant argued that the warrantless use of a GPS device to track his movements for a month violated his reasonable expectation of privacy under the Fourth Amendment.[171] The D.C. Circuit agreed. The court began by explaining why the *Knotts* holding was not applicable.[172] In that case, the

---

the daily, all-encompassing, indiscriminate dump of phone metadata that the NSA now receives as part of its Bulk Telephony Metadata Program." (citation omitted)). The NSA surveillance, unlike the collection in *Smith*, included information about whether the call was completed and how long it lasted. *See id.* at 35 n.57 ("[T]he pen register in *Smith* did not tell the government whether calls were completed or the duration of any calls . . . whereas that information is captured in the NSA's metadata collection.").

[162] *Id.* at 32-37 (finding that the sum of the bulk data collection far exceeds its individual parts); *see infra* Part II.B.1.

[163] 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[164] *Id.* at 562 ("As with the 'mosaic theory' often invoked by the Government in cases involving national security information, 'What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene.'" (quoting CIA v. Sims, 471 U.S. 159, 178 (1985))).

[165] *Id.* at 549.

[166] *Jones*, 132 S. Ct. 948.

[167] *Id.*

[168] *Id.*

[169] *Id.*

[170] *Id.*

[171] *Id.* at 949.

[172] United States v. Maynard, 615 F.3d 544, 556 (D.C. Cir. 2010).

beeper device was used to monitor the defendant's movements during a discrete journey for a few hours, whereas the instant case involved surveillance for approximately one month.[173] The court in fact pointed out that the *Knotts* decision explicitly left open the question of whether this type of prolonged surveillance violated a defendant's Fourth Amendment privacy rights.[174] The court's analysis centered on the Public Disclosure Doctrine and its implications in the instant case.[175] While public movements are generally not protected, the court reasoned that the facts of this case suggest a different conclusion:

> [T]he totality of Jones's movements over the course of a month—was not exposed to the public: First, unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.[176]

As to the first, the court seemed to move away from *Knotts*'s reliance on the second model of reasonable expectation of privacy, the nature of the information, and instead focused on the first model, whether someone would think this information is private.[177] In defining "'exposed' to the public," the court explained that the phrase does not mean what the police can "physically and may lawfully do but rather what a reasonable person expects another might actually do."[178] It is unlikely that a stranger would observe someone for such a long period of time.[179] Because of this practical limitation, a person has a reasonable expectation of privacy in this type of long-term surveillance.

The second consideration lays out the basic premise of the mosaic theory. Even though the individual or discrete movements lose protection based on their disclosure to the public view, the aggregation of these movements may constitute something worthy of protection. The court gave the example of a single trip to a gynecologist's office, which may reveal little about a woman, compared with the same trip followed by a visit weeks later to a baby supply

---

[173] *Id.*

[174] *Id.*

[175] *Id.* at 558.

[176] *Id.*

[177] *See infra* Part II.B.1.

[178] *Maynard*, 615 F.3d at 559. The court analogized its reasoning to the case of government surveillance of a defendant who happened to be spotted by a helicopter flying above. There was no reasonable expectation of privacy "not because the airplane was operating where it had a 'right to be' but because this type of air travel at 1,000 feet is a sufficiently routine part of modern life" that persons should expect that they might be observed. *Id.* (quoting Florida v. Riley, 448 U.S. 445, 453 (1989) (O'Connor, J., concurring)).

[179] *Id.* at 560.

store, which tells a different story.[180] The point here is that individual trips "viewed in isolation" may not reveal private information but numerous trips viewed collectively may reveal significant personal details.[181] According to the court, the "difference is not one of degree but of kind."[182] Prolonged exposure reveals a fuller picture of person's life—one that at some point crosses the line of constitutionally permissive surveillance.[183]

The court made it clear that its holding would not prohibit or affect visual surveillance of persons or vehicles.[184] It noted that long-term visual surveillance comparable to the instant case would expend significant time and resources and thus would be practically infeasible.[185] The unique nature of GPS technology thus seemed to underscore the court's analysis. This was a qualitatively different tool than the beeper technology referenced in *Knotts*, which simply augmented the government's ability to conduct visual surveillance. GPS technology, according to the court, "has occasioned a heretofore unknown type of intrusion into an ordinary and hitherto private enclave."[186]

The Supreme Court affirmed the D.C. Circuit decision under the name *United States v. Jones*. However, the Court found that the government unconstitutionally trespassed when it installed the GPS device on the defendant's car and thus there was a clear violation of the Fourth

[180] *Id.* at 562. I assume the point here is that the first observation would reveal nothing specific about the woman but the longer surveillance would reveal that the woman is pregnant.

[181] *Id.*

[182] *Id.*

[183] The court cited to a number of cases that found that longer-term surveillance revealed intimate details of a person's life. *Id.* (citing Galella v. Onassis, 353 F. Supp. 196, 227-28 (S.D.N.Y. 1972) ("Plaintiff's endless snooping constitutes tortious invasion of privacy . . . [he] has insinuated himself into the very fabric of Mrs. Onassis' life."); People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) ("[Prolonged GPS monitoring] yields . . . a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits.").

[184] *Maynard*, 615 F.3d at 565. ("We have already explained why Jones's argument does not 'logically . . . prohibit' much visual surveillance: Surveillance that reveals only what is already exposed to the public—such as a person's movements during a single journey—is not a search."). The court noted that the government could not point to a single actual example of visual surveillance that will be affected by the holding. *Id.* ("[W]e note preliminarily that the Government points to not a single actual example of visual surveillance that will be affected by our holding the use of the GPS in this case was a search.").

[185] The court referred to a chief of police who indicated that this type of surveillance for the vast majority of cases is impossible. *Id.* ("According to the former Chief of the LAPD, keeping a suspect under 'constant and close surveillance' is 'not only more costly than any police department can afford, but in the vast majority of cases it is impossible.'").

[186] *Id.*

Amendment.[187] Because any subsequent monitoring was fruit of this initial violation, the majority did not address the issue of the long-term GPS tracking and the Public Disclosure Doctrine.[188] Nevertheless, Justices Sotomayor and Alito both filed separate concurrences raising concerns about this type of surveillance.

Justice Sotomayor, along the lines of the D.C. Circuit, found that this type of GPS tracking violated a person's reasonable expectation of privacy.[189] She, too, seemed to rely on the first model of reasonable expectation, focusing on societal expectation: "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."[190] She also noted that this type of technology-based surveillance may chill "associational and expressive freedoms" and fundamentally "alter the relationship between citizen and government in a way that is inimical to democratic society."[191] She did not elaborate on this point so it is not clear where she was going. Perhaps, her focus on expressive associations suggests reliance on the third model of reasonable expectation—incorporating expressive associational values—to protect this type of surveillance. This theory will be discussed in greater detail in Part II.C.

Justice Sotomayor ended her analysis by raising a more fundamental point. If voluntary disclosure triggers the loss of protection, she questioned the very viability of the Doctrines in today's electronics-dominated society and whether secrecy should thus be a necessary condition for privacy.

> [I]t 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

[187] *Id.* ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."). The Court made clear that *Katz*'s reasonable expectation of privacy test was not intended to upset or supplant the original constitutional trespassory conception of privacy. *Id.* at 952 ("But as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.").

[188] *Id.* at 954 ("We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.").

[189] *Id.* at 955 (Sotomayor, J., concurring). Justice Sotomayor suggested that even short-term surveillance using this technology would frustrate privacy interests. *Id.* ("In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention.").

[190] *Id.* at 956.

[191] *Id.* (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 132 S. Ct. 1534 (2012)).

> 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.[192]

Justice Sotomayor's point certainly has intuitive appeal given the pervasiveness of these practices. But while these disclosures via technology have become central to our current lives, chucking the Doctrines would be deleterious to the bread and butter of government investigative practices even as it would, perhaps, bring expectations of privacy more in line with current practices.[193]

Justice Alito, in a separate concurrence, also expressed concern about long-term monitoring using GPS technology.[194] He, too, seemed to rely on the first model of reasonable expectation of privacy and found this type of tracking "involved a degree of intrusion that a reasonable person would not have anticipated."[195] 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.[196] Still, he seemed to recognize that what is reasonable is a moving target and that the level of availability and use of technological advancements shapes an average person's expectations about their privacy of their movements.[197] For now, though, "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."[198] Interestingly, Justice Alito did leave open the possibility that long-term GPS tracking may be constitutional in certain extraordinary offenses where such long-term monitoring might have been mounted using previously available techniques.[199]

B. *The Problem of Defining Reasonable Expectation of Privacy*

The mosaic theory presents a constitutional framework intended to counter the effects under traditional Fourth Amendment disclosure analysis. Proponents of the theory argue that such privacy endures in long-term surveillance even if it is lacking in the individual components that make up the

---

[192] *Id.* at 957 (citations omitted).

[193] *See infra* Part II.B.2.

[194] *Jones*, 132 S. Ct. at 957-64 (Alito, J., concurring) (rejecting the majority's trespass-based holding but concluding that long-term GPS monitoring constituted a search under the Fourth Amendment).

[195] *Id.* at 964.

[196] *Id.* at 963.

[197] *Id.*

[198] *Id.* at 964.

[199] *Id.*

surveillance.[200] Professors Gray and Citron describe it in the following way:

> [T]he core insight that drives the mosaic theory of Fourth Amendment privacy is that we can maintain reasonable expectations of privacy in certain quantities of information and data even if we lack reasonable expectations of privacy in the constituent parts of those wholes.[201]

Scholars have raised numerous issues—from conceptual to practical—with the implementation of this theory. The consensus appears to be that the theory would come at the cost of abandoning entrenched doctrinal principles and would be difficult to administer on the ground.[202] This Article does not seek to catalogue all the various arguments but provides a brief overview of the concerns raised.

1. Conceptual Difficulties

The first thing to note is the logical inconsistency in the theory. As the dissent in the D.C. Circuit's denial of an en banc hearing in *Maynard* puts it, "[t]he sum of an infinite number of zero-value parts is also zero."[203] If there is no reasonable expectation of privacy in a specific public movement, how can there be any such expectation in a collection of these movements? It would appear that they stand or fall together. The problem is articulating a

[200] Gray & Citron, *supra* note 12, at 397.

[201] *Id.*

[202] *See* Arcila, *supra* note 105, at 53 (commenting on widespread critiques of mosaic theory but arguing that these critiques are problematic because they refuse to acknowledge that Fourth Amendment law should change with the times and embrace mosaic theory); Gray & Citron, *supra* note 12, at 402 (arguing that the mosaic theory would require a complete overhaul of Fourth Amendment law and would eliminate the Doctrines); Kerr, *The Mosaic Theory*, *supra* note 10, at 336-37 (commenting on how mosaic theory would require reevaluating traditional doctrinal principles about search warrants); Benjamin M. Ostrander, *The "Mosaic Theory" and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733, 1748-49 (2011) (arguing that the mosaic theory is impractical because there are too many ambiguities in how to determine the scope of the mosaic); Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 223-30 (2012) (summarizing the various justices' opinions in *United States v. Jones* as they related to the debate about mosaic theory). *But see* Bethany L. Dickman, *Untying* Knotts*: The Application of Mosaic Theory to GPS Surveillance in* United States v. Maynard, 60 AM. U. L. REV. 731, 737-41 (2011) (arguing that the mosaic theory is a good evolution of Fourth Amendment law); Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment*, 14 N.C. J. L. & TECH. 431, 457-59 (2013) (arguing in support of reading *United States v. Jones* as reinforcing Fourth Amendment protections through the mosaic theory approach); Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 17-32 (2012) [hereinafter Slobogin, *Making the Most*] (proposing a statute to be used to implement mosaic theory into Fourth Amendment law).

[203] United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting).

justification for the collection of observations that would also not apply in the discrete observation case.

The D.C. Circuit and the *Jones* concurrences rely on the first model of privacy and its focus on societal or individual expectations. But scholars have pointed out the weakness of relying on what society or an individual deems reasonable when construing Fourth Amendment protection.[204] Kerr finds that this is a poor way to answer this question, particularly when dealing with technological advancements.[205] Individuals, by and large, do not have a good sense of the relevance of technology when it comes to surveillance.[206] He finds that these practices are typically hidden and that most people would be guessing as to whether privacy invasions are common or rare.[207]

Even assuming perfect knowledge of technological advances and their relative use, individuals may reasonably disagree as to when this technology-enhanced surveillance intrudes on Fourth Amendment privacy.[208] Take again the D.C. Circuit's example of a single trip to the gynecologist compared with the additional trip weeks later to the baby supply store. It may certainly be true that the first trip reveals nothing specific about the woman's personal life, whereas the second trip does reveal important personal information. But what if the woman in the first trip went straight from the gynecologist's office to a baby supply in a matter of hours? One might say that surveillance of this person over these few hours reveals the same amount of private information as the longer surveillance, and thus both should be protected. Perhaps the response from an advocate of the mosaic theory would be that while this surveillance reveals private information, the length of the surveillance is not

[204] *See, e.g.*, Arcila, *supra* note 105, at 71-72 (arguing that the general public use of GPS makes the reasonableness test a bad one); Gray & Citron, *supra* note 12, at 413-14 (arguing that reasonableness is a bad standard for Fourth Amendment cases because use of GPS devices which make private knowledge public is so widespread that such an invasion of privacy will be considered reasonable solely because of this common usage); Kerr, *The Mosaic Theory*, *supra* note 10, at 349 (arguing that reasonableness is a bad standard for Fourth Amendment cases because "[m]ost individuals lack a reliable way to gauge the likelihood of technological surveillance methods").

[205] Kerr, *The Mosaic Theory*, *supra* note 10, at 349.

[206] *Id.*

[207] *Id.*

[208] Scholars have attempted to use computer modeling to suggest when GPS surveillance constitutes a search. *See* Steven Bellovin et al., *When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 N.Y.U. J.L. & LIBERTY 555, 604 (2014) (discussing how to use computer modeling to analyze the usefulness of mosaic theory, specifically in the GPS context). *But see* Orin Kerr, *No, Machine Learning Does Not Resolve How the Mosaic Theory Applies*, VOLOKH CONSPIRACY (June 3, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/03/no-machine-learning-doesnt-resolve-how-the-mosaic-theory-applies/, *archived at* http://perma.cc/J9U9-TW3M (arguing that this computer theory still fails to posit a workable model as to when the monitoring constitutes a mosaic).

something society would find unreasonable. But it is not clear that even short-term surveillance is automatically safe under this reasonableness assessment. Imagine the police use GPS to monitor the movements of an individual who lives high up in the Colorado mountains where visual surveillance would be practically very difficult. The police monitor the individual's car for a few hours in the middle of night, during which time the individual makes a number of trips to an adult dance club. Given the secluded area where the individual lives, the timing of the surveillance, and the personal nature of the trips, someone may find that short-term monitoring too is unreasonable and should also be prohibited.

This reliance on the first model of reasonable expectation of privacy also runs counter to the Court's prior precedent involving technological advances. As mentioned earlier, *Smith* and *Knotts* both focused on the second model, or the nature of the information, in concluding that the disclosure to the third party or public vitiates privacy protection.[209] But even where the Court has relied on societal expectation and public use, its reasoning would suggest that the instant GPS tracking would be permissible. In *Kyllo v. United States*,[210] the government used a heat detection device "to explore details of the home that would previously have been unknowable without physical intrusion."[211] The police did not trespass on the defendant's property and scanned the premises from across the street.[212] The Court found that this conduct still violated the Fourth Amendment partly because the device was "not in general public use" and thus a person would not reasonably expect the device to be employed.[213] The implication here is that if the device were in routine use and part of everyday life, an individual cannot reasonably expect that its use would violate her privacy rights. While this type of thermal imaging technology remains uncommon, GPS tracking evidence is ubiquitous.[214] It is part of cell phones, computers, cars, and tablets.[215] As Professors Gray and Citron write, "[g]iven

[209] *See supra* Part I.B.

[210] 533 U.S. 27 (2001).

[211] *Id*. at 40.

[212] *Id.* at 29-30.

[213] *Id.* at 34. The Court also relied on the fourth model of reasonable expectation of privacy and found that to allow this conduct "would be to permit police technology to erode the privacy [inside a person's home] guaranteed by the Fourth Amendment." *Id.*; *see* Kerr, *Four Models*, *supra* note 10, at 520, 522 n.103.

[214] *Kyllo*, 533 U.S. at 29-30.

[215] Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 677, 713-14 (2011) (discussing the widespread nature of modern technological devices). Furthermore, unlike in *Kyllo*, the target in *Jones* was not a person's home but his car, suggesting a less bright-line rule of privacy. *See Kyllo*, 533 U.S. at 34 ("While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences is at issue, in the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in

this state of affairs, it is hard to make the case for a mosaic theory of the Fourth Amendment based solely on social expectations to the extent they are a function of common practice."[216]

If we are going to use the first model of reasonable expectation, we still need agreement as to the perspective from which this assessment should be made. The D.C. Circuit and *Jones*'s respective concurrences seem to give very different answers. The D.C. Circuit focuses on the question of the likelihood of whether a stranger would observe these long-term movements.[217] Justice Sotomayor, on the other hand, focuses on government power and when the government can learn details about an individual's personal life.[218] Alito articulates yet another standard, focusing on societal expectations of law enforcement investigative practices.[219] Recognizing that these approaches are quite different, Kerr asks, "[i]f courts adopt the mosaic theory, which version should they use?"[220]

These issues are compounded when one asks exactly what should count as part of the mosaic of movements warranting protection. The facts of *Jones* related to constant surveillance for over a month.[221] But imagine a GPS device that records the location of a car for an hour but then turns off for the rest of day. Or suppose the police monitor an individual for five days and then give up the surveillance for twenty days, after which they restart the investigation for an additional five days. Have the cops monitored the suspect for an entire month in violation of *Jones*, or are these just instances of short-term surveillance (thirty hours and ten days, respectively) that do not run afoul of the Fourth Amendment?[222] It is not clear how an advocate of the mosaic theory

the common law, of the minimal expectation of privacy that *exists,* and that is acknowledged to be *reasonable.*").

[216] Gray & Citron, *supra* note 12, at 414.

[217] *United States v. Maynard*, 615 F.3d 544, 560 (D.C. Cir. 2010); Kerr, *The Mosaic Theory*, *supra* note 10, at 331.

[218] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); Kerr, *The Mosaic Theory*, *supra* note 10, at 330.

[219] *Jones*, 132 S. Ct. at 963-64 (Alito, J., concurring); Kerr, *The Mosaic Theory*, *supra* note 10, at 330-31.

[220] Kerr, *The Mosaic Theory*, *supra* note 10, at 330. Compare, for instance, Alito's and the D.C. Circuit's respective standards. *Jones*, 132 S. Ct. at 963-64 (Alito, J., concurring) (discussing the amount of resources a similar type of surveillance would have taken before GPS technology was developed); *Maynard*, 615 F.3d at 560. What a private actor would do as far as long-term surveillance is quite different from what government actors may do. A private investigator, for instance, may be paid quite handsomely by one client to monitor somebody's movements for an extended period of time. The same cannot be said of law enforcement with its limited resources. Using one standard instead of the other would lead to different conclusions about the reasonableness of the surveillance.

[221] *Jones*, 132 S. Ct. at 948.

[222] *See* Kerr, *The Mosaic Theory*, *supra* note 10, at 333 (discussing the constitutional question of time as it relates to surveillance under the Fourth Amendment).

would respond.

2. Rejection of the Public Disclosure and Third Party Doctrines

The most troubling part of adopting the mosaic theory is that it requires the abandonment of, or dramatic alterations to, the Doctrines. The basic problem is the inherent conflict between the first and second models of reasonable expectation. While the Doctrines embrace a per se rule focusing solely on disclosure and why this vitiates privacy, the mosaic theory rests on society's opinion and what it deems reasonable.[223]

Consider the Public Disclosure Doctrine. The fact that public movements are not protected under the Fourth Amendment is critical to law enforcement investigations.[224] Visual warrantless surveillance remains a central part of police surveillance.[225] It is not clear to what extent these practices will remain constitutional with the introduction of the mosaic theory. For instance, it is common for officers to track vehicles and aggregate information from various sources over a period of time.[226] As Gray and Citron point out, the "mosaic theory puts these practices and the line of doctrine endorsing them in obvious jeopardy, particularly when officers are too successful and their investigations produce too much information."[227] This danger is compounded by the fact that law enforcement may use a combination of visual and technology-based surveillance (*a la Knotts*) when investigating a suspect. "How, after all," ask Gray and Citron, "are we to distinguish 'between the supposed invasion of aggregation of data between GPS-augmented surveillance and a purely visual surveillance of substantial length'?"[228] It won't do here to simply say that a specific duration of technology-dependent surveillance violates the expectation of privacy. The problem is that the Public Disclosure Doctrine treats all public movements the same, regardless of how much information is disclosed or how long it is observed.[229] To carve out exceptions based on what society thinks is unreasonable leaves vulnerable investigative techniques that are essential to effective law enforcement.

The Third Party Doctrine would also be on shaky ground. Here, too, the

[223] *Id.* at 348.

[224] *See* LAWRENCE F. TRAVIS III, INTRODUCTION TO CRIMINAL JUSTICE 179 (7th ed. 2012).

[225] *See id.* ("The bulk of surveillance conducted by police agencies is physical surveillance."); Sarah Stillman, *The Throwaways*, NEW YORKER, Sept. 3, 2012, at 38 ("By some estimates, up to eighty per cent of all drug cases in America involve [informants] . . . .").

[226] Gray & Citron, *supra* note 12, at 387.

[227] *Id.* at 405.

[228] *Id.* (quoting United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting)).

[229] *Id.* at 402-03 ("Adopting a mosaic approach to quantitative privacy seems to require abandoning the public observation doctrine . . . .").

mosaic theory would upset the voluntary disclosure principle that stands at the heart of this doctrine.[230] Shifting the focus to what society or an individual deems reasonable (the first model of reasonable expectation of privacy) would surely frustrate the use of undercover informants or other surreptitious data collection techniques that do not require a warrant. Imagine a scenario where an informant is deep undercover for a significant period of time gaining the trust of a suspect. Or imagine an informant who dupes a suspect into allowing her into her home and disclosing private and incriminating information. Or perhaps the government simply acquires a wealth of financial records from a suspect's bank. Currently, all of these types of law enforcement tools do not trigger Fourth Amendment protection because the individual voluntarily discloses the information to another person or entity.[231] However, under the mosaic theory, none of these tactics are secure.[232] Societal expectations may find that these methods, too, impinge on Fourth Amendment rights as they involve unreasonable duplicity and reveal private information. Police would thus find themselves in the new position of having to secure a warrant based on probable cause before engaging in these practices.

For some, this conclusion may be welcomed, particularly in today's technological world where disclosures to various entities and individuals have become ubiquitous.[233] Justice Sotomayor, in fact, raises this possibility in her concurrence.[234] This Article does not take such a drastic approach, nor would such a course be desirable. Any such rejection would come at the cost of jettisoning or severely curtailing essential law enforcement investigative

---

[230] *See id.* at 405; David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 86 (2013) (discussing how Third Party Doctrine is undercut by use of quantitative data as marker of Fourth Amendment protection).

[231] *See supra* notes 67-69.

[232] *But see* Arcila, *supra* note 105, at 53-54 (arguing that the historically well established "private-public space distinction to a never-before-seen context ignores the prospect that rules that worked well in the past might no longer work given changed circumstances" and that "GPS tracking is not just different in degree").

[233] Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 39-40 (2011) (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"); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 654-64 (2011) [hereinafter Strandburg, *Home*] (arguing that the Third Party Doctrine should not be applied to certain Internet communications); *see* Benjamin Priester, *Five Answers and Three Questions After* United States v. Jones *(2012), the Fourth Amendment GPS Case*, 65 OKLA. L. REV. 491, 511 ("Each of the three opinions in *Jones* noted the potentially disturbing implications of advanced technology for reducing privacy."). Interestingly, Professor Slobogin, pre-*Jones*, presents a theory of Fourth Amendment protection over public surveillance by law enforcement, rejecting the Doctrines. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007).

[234] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

techniques that have historically not been subject to warrant and probable cause requirements.[235]

3. Practical Hurdles

The implementation of the mosaic theory also raises a host of practical problems. First and foremost, what constitutes too much surveillance? Where should courts draw the line between permissible observation and unreasonable intrusion? Is it twenty-eight days? Two weeks? And what should constitute an "extraordinary offense" such that long-term monitoring would be constitutionally acceptable? The majority in *Jones* recognized these practical difficulties, stating that:

> [I]t remains unexplained why a 4-week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation. . . . What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist?[236]

The Court found that relying on the mosaic theory would force the justices to "grapple with these 'vexing problems.'"[237]

Beyond this initial determination, there remain other unanswered questions regarding the application of this theory. Assuming Fourth Amendment privacy protection applies, the next question centers on the requirements necessary before police can conduct the surveillance. The Court aims for reasonableness here by balancing the invasion of privacy against the legitimate government interest in conducting the search.[238] This traditionally requires the government to obtain a warrant based on probable cause.[239] It is not clear how these requirements—assuming they apply—would be handled in a long-term

---

[235] *See supra* note 228 and accompanying text.

[236] *Jones*, 132 S. Ct. at 954 (majority opinion) (citation omitted).

[237] *Id.*

[238] *See* United States v. Place, 462 U.S. 696, 703 (1983) ("We must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.").

[239] Over time, the warrant requirement has given way to a general reasonableness requirement where, depending on the circumstances of the search, such specific requirements are not necessary. *See* Kentucky v. King, 131 S. Ct. 1849, 1853-54 (2011) (no warrant required for exigent circumstances); California v. Carney, 471 U.S. 386, 392 (1985) (no warrant required for search of car when probable cause exists); Terry v. Ohio, 392 U.S. 1, 33 (1968) (no warrant required for limited frisk of persons based on reasonable suspicion rather than probable cause); Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 395 (1988) (discussing the resurgence of the general reasonableness standard and how this may obviate the need for a warrant). The practical hurdles assume that the court would require a warrant and probable cause before the government can conduct mosaic searches.

surveillance context.[240] Courts have not addressed this type of public surveillance because it has never been constitutionally protected in the first instance.

Probable cause to search a location requires that there is a fair probability that evidence pertaining to the crime will be found in the stated location.[241] But under the mosaic theory, the government is not interested in a specific location but rather the continuous surveillance over a period of time.[242] Does this mean that one of the locations the suspect will travel to will contain evidence of a crime? Or is the surveillance targeted at the person herself who has committed a crime? Or some combination of the two?[243] A recent case illustrates this difficulty.[244] The government sought to collect GPS location evidence in an effort to locate a fugitive.[245] As part of the warrant application, the police established that probable cause existed and that this monitoring would help find the fugitive and bring him to justice.[246] The magistrate judge rejected the application, saying that the Fourth Amendment requires probable cause that the information itself is evidence of a crime, not probable cause that it will help find the individual.[247]

Similar issues arise with the warrant requirement. Under the Fourth Amendment, warrants must "particularly decrib[e] the place to be searched, and the person or things to be seized."[248] The prototypical case would involve searching an individual's home for evidence of a crime.[249] The warrant would detail the location of the home and the relevant items to be seized.[250] This gets

---

[240] *See* Kerr, *The Mosaic Theory*, *supra* note 10, at 336-37 & nn.143-56 (discussing how to implement the Fourth Amendment requirements to the mosaic theory and whether the warrant requirement and/or probable cause is required or whether something less would be sufficient).

[241] Illinois v. Gates, 462 U.S. 213, 273 (1983) ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place."); Warden v. Hayden, 387 U.S. 294, 307 (1967) (discussing how police must believe items found in a search will be useful for government's case in criminal suit).

[242] Kerr, *The Mosaic Theory*, *supra* note 10, at 338.

[243] *Id.*

[244] I*n re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 535 (D. Md. 2011) (discussing the use of GPS surveillance to locate a fugitive).

[245] *Id.*

[246] *Id.*

[247] *Id.*

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

[249] *See generally* Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 912 (2010) ("Doctrinally, homes receive greater protection than many contexts of search and seizure . . . .").

[250] *See* Wilson v. Layne, 526 U.S. 603, 612 (1999) (discussing how a warrant in a stolen

tricky in the mosaic theory context.[251] There is no specific place to search; rather, the police want to aggregate searches across many places. Should they have to specify an overall geographic jurisdiction or spell out all the places the suspect may travel? The same difficulties apply to the items supposedly being seized. Under the mosaic theory, there does not appear to be any tangible evidence being seized. But the whole point of the warrant requirement is to narrow the location search and specify the evidence to be seized.[252] As Kerr argues, "[t]he theory of mosaic searches flips this understanding on its head" because "[m]osaic investigations are deemed searches [i.e violations of the Fourth Amendment] precisely because they are *not* limited" and reveal a collection of personal information.[253]

Professor Christopher Slobogin proposes a bright-line statutory rule that may answer some of these questions regarding the implementation of the mosaic theory.[254] Under his framework, the government's surveillance efforts require increasing restraint the longer the aggregate surveillance lasts.[255] Probable cause and a warrant are required for surveillance that lasts longer than forty-eight hours in the aggregate.[256] Probable cause here is defined as an "articulable belief that a search will more likely than not produce . . . significant evidence of wrongdoing," and the warrant "must describe with

goods case must mention the specific location to be searched); Andresen v. Maryland, 427 U.S. 463, 480 (1976) (discussing general proposition that warrants must contain description of objects to be seized); Weeks v. United States, 232 U.S. 383, 398 (1914) (discussing the need for a warrant before papers may be seized); Stern, *supra* note 249, at 913 ("The warrant must issue based on a showing of probable cause and satisfy other procedural requirements or risk exclusion of the evidence at trial.").

[251] Kerr, *The Mosaic Theory*, *supra* note 10, at 339.

[252] *Id.*

[253] *Id.*

[254] Slobogin, *Making the Most*, *supra* note 202, at 16-37 (proposing substantive rules to govern physical and transaction surveillance and making "an important distinction between targeted searches and general searches, with the former regulated under proportionality theory and the latter regulated under political process theory"). Kerr finds that Slobogin's proposal is statutory, not constitutional, and thus does not answer how the mosaic theory should apply. Kerr, *The Mosaic Theory*, *supra* note 10, at 347 n.202.

[255] Slobogin, *Making the Most*, *supra* note 202, at 24 (contending that his proposed statutory framework for targeted public searches relies on "the proportionality principle's stipulation that the justification for a search be roughly proportional to its intrusiveness"). Surveillance that lasts between twenty minutes and no longer than forty-eight hours requires reasonable suspicion, and surveillance that lasts less than twenty minutes requires good faith that it can accomplish a legitimate law enforcement objective. *Id.* (suggesting three guidelines for targeted public searches depending on length of time). Slobogin sets a parallel statutory framework for the collection of electronic data. *Id.* at 28 (proposing that a targeted data search that takes place over more than a forty-eight-hour period requires probable cause while a targeted data search for less than that time requires reasonable suspicion).

[256] *Id.* at 24. Slobogin makes an exception for exigent circumstances, which is not relevant for the instant analysis. *Id.*

particularity the person or place targeted, the evidence sought, and, if applicable, the duration of the search."[257] This statute would appear to answer the concerns about the nature of the probable cause and the particularity requirements of the warrant.[258] Before the police can conduct long-term surveillance of a suspect, they would have to believe that this effort will reveal some inculpatory evidence and, thereafter, secure a warrant that specifies at least the name of the person and what possible evidence could be found.[259]

This type of statutory scheme may provide one potential workable implementation of the mosaic theory, but it comes at too high a price. Slobogin explicitly states that his framework "does not differentiate between [surveillance] using technology and [surveillance] with the naked eye," and thus rejects the implications of the Doctrines.[260] As previously stated, this rejection runs counter to longstanding precedent and would stymie a major artery of police investigation.[261]

C. *Using Associational Rights in Fourth Amendment Calculus*

It seems that part of the problem with the mosaic theory is its use of societal expectation as the marker for reasonable expectation. Justice Sotomayor's reference in *Jones* to government surveillance preventing "associational and expressive freedoms," and Justice Marshall's dissent in *Smith v. Maryland* noting that government collection efforts may deter political associations and journalistic activity may suggest a way to reconceptualize the mosaic theory using the third model: to focus on protecting a legal norm or right.[262] The

[257] *Id.* at 20.

[258] *Id.* at 21 ("The definition of 'warrant' tracks the Fourth Amendment language, adjusted for the surveillance context.").

[259] *Id.*

[260] *Id.* at 17-18.

[261] *See supra* notes 225-233 and accompanying text (analyzing the mosaic theory's rejection of the Doctrines).

[262] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms."); Smith v. Maryland, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting) ("Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society."). Justice Marshall's dissent pre-dates *Jones*'s mosaic theory, but it can still provide a clue as to how the Justices see the interaction between the Fourth and First Amendments. It would seem that Justice Harlan, in his dissent in *United States v. White*, where the majority allowed an informant to wear a wire, was probably the first to connect these two principles. United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting) ("Authority is hardly required to support the proposition that words would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed."). Justice Harlan found that this type of monitoring may well "smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life" and that the risks of "Orwellian

refrain of "the sum is greater than its parts" remains. Only this time, the rationale for protecting an individual's public movements is that together these movements constitute this person's right to express herself and associate with whomever she wants.[263] Allowing the government to conduct surveillance would deter this person's ability to exercise this freedom.[264]

The Court has understood "freedom of association" in two distinct senses.[265] The first relates to "expressive association[s]" where the focus is on the right to associate for purposes of engaging in those activities protected by the First Amendment, including "political, social, economic, educational, religious, and cultural ends."[266] The second, deriving from both First Amendment and due process principles, relates to "intimate association[s]," which involve close ties amongst a small group of individuals with whom one shares "not only a special community of thoughts, experiences, and beliefs but also distinctively personal aspects of one's life."[267]

Big Brother" technology may be "used to unearth 'political' crimes." *Id.* at 770 & n.3, 787. This connection between the First and Fourth Amendment channels the classic article on the Fourth Amendment in which Anthony Amsterdam argues that the level of protection this Amendment affords depends on what rights we think citizens should have in a democratic society. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 377 (1974) ("[T]he limits of American society's effective control over the largest part of the spectrum of police powers and potential abuses depend upon the scope given to the fourth amendment.").

[263] *See supra* note 262 and accompanying text.

[264] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms."); *Smith*, 442 U.S. at 751 (Marshall, J., dissenting) ("The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide.").

[265] Roberts v. U.S. Jaycees, 468 U.S. 609, 617 (1984).

[266] *Id.* at 622; *see* U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; of the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."); NAACP v. Alabama, *ex rel* Patterson, 357 U.S. 449, 462 (1958) ("It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association . . . .").

[267] *Roberts*, 468 U.S. at 617-20. This right of intimate association is also tied up with Fourteenth Amendment rights. *See id.* at 619 (citing Griswold v. Connecticut, 381 U.S. 479 (1965) (holding that a state statute prohibiting use of contraceptives violates the right to marital privacy grounded in the Due Process Clause of the Fourteenth Amendment)). Scholars, too, have pointed out that this right to intimate associations encompasses First Amendment and Fourteenth Amendment considerations. *See* John D. Inazu, *The Unsettling "Well-Settled" Law of Freedom of Association*, 43 CONN. L. REV. 149, 158-67 (2010) [hereinafter Inazu, *The Unsettling "Well-Settled" Law*] (analyzing the Court's approach to intimate association and the move from an emphasis on associational relationships between people in *Griswold* to Justice Brennan's focus on the right of individual autonomy in *Eisenstadt v. Baird*); Joshua P. Roling, Note, *Functional Intimate Association Analysis: A*

These rights of association protect not only against laws directly aimed at suppressing these associational rights but also those government practices that indirectly affect them or otherwise chill someone from engaging in these protected associations.[268] The notion of the government chilling constitutional rights or deterring individuals from exercising these rights is typically associated with free speech rights.[269] But there is no reason why the concept would not equally apply to associational rights. While Justice Sotomayor's reference in *Jones* to chilling associational freedoms did not cite precedent, the

Doctrinal Shift to Save the Roberts *Framework*, 61 DUKE L.J. 903, 909-10 (2012) ("In *Roberts*, the Court separated two recognized sources of constitutional support for the right of association—the First and Fourteenth Amendments—and concluded for the first time that the freedom of association encompasses two distinct rights.").

A number of scholars have noted the distinction between intimate and expressive associations and the relative First Amendment rights accorded to each. *See* Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 637 (2004) (observing that the Court has distinguished "expressive" association from "intimate" association, with the former being linked to public advocacy); Inazu, *The Unsettling "Well-Settled" Law*, *supra*, at 156-57 (stating that intimate associations get more protection than non-intimate expressive associations); Inazu, *Virtual Assembly*, *supra* note 36, at 1099 ("Intimate associations receive the highest level of constitutional protection."); Patrick P. Garlinger, Note, *Privacy, Free Speech, and the Patriot Act: First and Fourth Amendment Limits on National Security Letters*, 84 N.Y.U. L. REV. 1105, 1129 n.138 (2009) ("I draw a distinction analogous to that drawn by the Supreme Court in *Roberts v. U.S. Jaycees* between 'intimate association,' or associating with others personally, and 'expressive association,' or associating with others to convey a message.").

[268] *Compare NAACP*, 357 U.S. at 462-63 (holding that exposure of NAACP membership lists during investigation would impermissibly chill free association), *with* Laird v. Tatum, 408 U.S. 1, 10 (1972) (rejecting standing of individuals claiming that existence of an Army civilian surveillance program chilled their free expression and associational rights). *See* Leslie Kendrick, *Speech, Intent, and the Chilling Effect*, 54 WM. & MARY L. REV. 1633, 1636-37 (2013) (discussing problems with the relationship between speaker's intent, the First Amendment, and the chilling effect of associations); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 785-87 (2008) [hereinafter Strandburg, *Freedom of Association*] (explaining that there are at least three types of burdens imposed by relational surveillance in the form of network analysis: "chilling of protected association by revealing its existence, structure, and membership; chilling of protected association because of the potential for network analysis to mistake legitimate association for illegitimate association; and harms to self-determination and chilling of exploratory associations because of the potential for network analysis to treat individuals as 'members' of a group with which they did not want to associate themselves").

[269] Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 685 (1978) ("The chilling effect concept has been recognized most frequently and articulated most clearly in decisions chiefly concerned with the procedural aspects of free speech adjudication.").

Court has previously acknowledged that the chilling effect can apply here.[270] In *Laird v. Tatum*,[271] for instance, plaintiffs brought suit against the Army for its "alleged surveillance of lawful and peaceful civilian political activity."[272] The plaintiffs argued that the presence of this "system of gathering and distributing information . . . constitutes an impermissible burden on [them] and other persons similarly situated which exercises a present inhibiting effect on their full expression and utilization of their First Amendment rights."[273] The Court dismissed the case on standing grounds because plaintiffs could not articulate a specific harm or otherwise show how this surveillance specifically chilled their First Amendment rights to peacefully assemble.[274] The Court acknowledged, however, that if they had presented such harm—above and beyond simply disagreeing with the Army practice—plaintiffs could bring a claim for chilling their associational rights.[275] Scholars too have recognized that the chilling applies to associational rights.[276]

There does appear to be a natural conflict between associational rights and the government's ability to monitor and collect information about an individual over a significant period of time.[277] Allowing the latter could deter an individual from exercising her rights to engage in various associational activities—whether they are social, professional, political, or religious—for fear the government may be watching.[278] But given the brevity of Justices

[270] *See supra* note 268 (citing *NAACP*, *Laird*, and several journal articles that discuss the chilling effect of government surveillance on association); *see also* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.").

[271] 408 U.S. 1.

[272] *Id.* at 2.

[273] *Id.* at 10 (emphasis omitted) (quoting Tatum v. Laird, 444 F.2d 947, 954 (D.C. Cir. 1971)).

[274] *Id.* at 13.

[275] *Id.* at 13-14.

[276] *See supra* note 268.

[277] *See* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 115 (2007) ("Government information gathering can also implicate other First Amendment protections, such as freedom of association and freedom of the press."). Justice Marshall's dissent clearly focuses on the second type of association though it is not clear whether Justice Sotomayor is invoking one or both these types of associations.

[278] Already in the civil context, the Court has found that the government's effort to collect information can chill First Amendment liberties, including but not limited to surveillance of political activities, identification of anonymous speakers, and discovery of political ties. *See, e.g.*, *Laird*, 408 U.S. at 1 (finding that government surveillance of political activities can implicate the First Amendment); Talley v. California, 362 U.S. 60, 64 (1960) (finding that law prohibiting anonymous speech runs afoul of First Amendment doctrine); NAACP v. Alabama, *ex rel* Patterson, 357 U.S. 449, 449 (1958) (finding that the government cannot compel disclosure of the names and addresses of NAACP members because the group engages in expressive activities); Doe v. 2theMart.com Inc., 140 F. Supp.

Sotomayor's and Marshall's respective concurrence and dissent, it is not clear exactly how they envision these expressive rights should apply in the Fourth Amendment context. There appear to be two logical options.[279] First, as some scholars argue, expressive associational rights could serve as additional protection to information not otherwise falling under the purview of the Fourth Amendment.[280] While this position may have merit, the extent to which these rights apply directly to a situation of government surveillance is beyond the scope of this Article.

My purpose is to examine the mosaic theory in the larger Fourth Amendment framework. This leads to the second logical option—and the focus of this Article—whereby associational rights are incorporated into the reasonable expectation of privacy test. A handful of scholars have suggested this approach, particularly in today's technologically dominated society where the government can collect information quite easily.[281] While these proposals

2d 1088, 1097 (W.D. Wash. 2001) (holding that a government civil subpoena to an ISP to disclose the identity of a speaker may have a chilling effect and thus must pass the heightened standard); Solove, *supra* note 277, at 143 (discussing relevant cases).

[279] Scholars have opined as to which of these two avenues is supported by Justice Sotomayor's concurrence. *See* Witmer-Rich, *supra* note 34 (responding to other users on the blog who view Justice Sotomayor's concurrence in *Jones* as a First Amendment analysis and explaining why he views it as a Fourth Amendment issue).

[280] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1506 (2000) ("[T]he First Amendment right to freedom of association imposes some limits on the extent to which the government may observe and profile citizens . . . ."); Matthew Lynch, *Closing the Orwellian Loophole: The Present Constitutionality of Big Brother and the Potential for a First Amendment Cure*, 5 FIRST AMEND. L. REV. 234, 284-304 (2007) (arguing to expand First Amendment rights to protect against widespread government surveillance); Solove, *supra* note 277, at 116 (providing framework for how the First Amendment could apply in surveillance context); Strandburg, *Freedom of Association*, *supra* note 268, at 796 ("[M]erely using the First Amendment as a trigger or booster for Fourth Amendment scrutiny will not be sufficient to serve the distinctive interests in freedom of association implicated by relational surveillance. A direct resort to the First Amendment, in addition to any appropriate Fourth Amendment analysis, is needed."); Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1396-1402 (2012) (finding that First Amendment framework can apply to political and other protected associations on the Internet).

[281] *See, e.g.*, Amar, *supra* note 37, at 759 ("We need to read the [Fourth] Amendment's words and take them seriously: they do not require warrants, probable cause, or exclusion of evidence, but they do require that all searches and seizures be reasonable."); Suzanne M. Berger, Note, *Searches of Private Papers: Incorporating First Amendment Principles into the Determination of Objective Reasonableness*, 51 FORDHAM L. REV. 967, 990 (1983) ("Proper incorporation of the first amendment factor at the threshold stage of fourth amendment inquiry will more fully serve the underlying purposes of both these amendments."); Courtney Burten, Note, *Unwarranted! Privacy in a Technological Age: The Fourth Amendment Difficulty in Protecting Against Warrantless GPS Tracking and the Substantive Due Process and First Amendment Boost*, 21 S. CAL. INTERDISC. L.J. 359, 385

pre-date *Jones* and the introduction of the mosaic theory, they can still be instructive on how associational principles can potentially apply in this context. Scholars have focused on First Amendment expressive associational rights in their discussion of incorporating these values into the Fourth Amendment framework.[282] As one law review note explains, "we ought to build on the Fourth Amendment's traditional relationship to the First Amendment by allowing their overlap to push Fourth Amendment standards in a more exacting direction" and "begin to reformulate the current Fourth Amendment reasonable expectation of privacy test to more directly incorporate First Amendment values."[283]

The Court has never excluded the possibility of such a framework, though it has found that where Fourth Amendment privacy already applies, the warrant requirement adequately protects any First Amendment expressive association interests.[284] In *Zurcher v. Stanford Daily*,[285] for instance, the Court was confronted with a search of a college newspaper office where the police first secured a warrant based on probable cause.[286] The Court found that any First Amendment interests relating to the ability of the press to gather, analyze, and disseminate news were sufficiently protected by the preconditions for a warrant.[287] Similarly, in *Stanford v. Texas*,[288] where the police searched the

(2012) ("[T]he substantive due process concept of privacy can be incorporated into Fourth Amendment doctrine."); Garlinger, *supra* note 267, at 1108 (arguing that "reliance on the First Amendment is unlikely to solve the problem of overreaching government information gathering" because "a litigant must meet too high a burden to prove a link between the compelled disclosure of Internet activity data and a chilling effect").

[282] *See* Berger, *supra* note 281, at 970-71 ("[B]oth current case law and the underlying purposes of the first and fourth amendments mandate consideration of these first amendment interests."); Burten, *supra* note 281, at 380 (drawing on Justice Sotomayor's analysis in *Jones* of how to measure society's reasonable expectation of privacy); Garlinger, *supra* note 267, at 1129 ("[O]ne might say that the First Amendment protects 'expressive privacy'—privacy that is designed to cultivate autonomy in furtherance of democratic debate, whereas the Fourth Amendment protects 'intimate privacy.'").

[283] Garlinger, *supra* note 267, at 1141-42.

[284] *See* Solove, *supra* note 277, at 128 (remarking that while the Court gives lip-service to the additional First Amendment principle at stake, the resultant standard used is no different than any Fourth Amendment situation).

[285] 436 U.S. 547 (1978).

[286] *Id*. at 551 (explaining that the police officers' search of the Stanford Daily's office was pursuant to a warrant that was issued on finding that there was probable cause that the office contained negatives, photographs, and film that would be relevant to the identity of perpetrators of the previous night's felonious activities).

[287] *Id.* at 565 ("Properly administered, the preconditions for a warrant—probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness—should afford sufficient protection against the harms that are assertedly threatened by warrants for searching newspaper offices."). The Court noted that the warrant requirement in this case should be executed with "scrupulous exactitude" but that in the end, this standard merely required following the typical protection of Fourth Amendment. *Id.* at

home of an individual connected with the Communist Party, the Court held that the gathering of evidence violated the Fourth Amendment because the warrant was not particularized enough.[289] As to the many First Amendment interests, the Court concluded that strict adherence to the typical warrant requirements protected these rights.[290] In each of these cases, Fourth Amendment protection already applied.[291]

Hence, these holdings would not foreclose the possibility of using expressive associational principles in the first instance as a way to apply the reasonable expectation test and thus secure Fourth Amendment scrutiny.[292] Indeed, the Court has previously used statutory law and other legal norms to find Fourth Amendment protection, relying on the third model of reasonable expectation of privacy.[293] It stands to reason that constitutional values *a fortiori* could be incorporated into this calculus. As the law review note cited above states, "Because the First Amendment depends on a certain level of privacy to enable the exercise of free speech and association, the First Amendment might require that the Fourth Amendment floor be raised for data that implicates such concerns."[294] Most government investigations and related surveillance involve crimes such as murder, conspiracy, and robbery and not

564-65 ("[T]he prior cases [before the Supreme Court] do no more than insist that the courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search.").

[288] 379 U.S. 476 (1965).

[289] *Id.* at 485-86 ("[T]he Fourth and Fourteenth Amendments guarantee to John Stanford that no official of the State shall ransack his home and seize his books and papers under the unbridled authority of a general warrant.").

[290] *Id.* (recognizing that there is a constitutional requirement for a standard of "scrupulous exactitude" when issuing warrants in order to remain faithful to First Amendment freedoms). *But cf.* Roaden v. Kentucky, 413 U.S. 496, 504 (1973) (finding that seizure of film at a local theater without warrant was unreasonable "because prior restraint of the right of expression, whether by books or films, calls for a higher hurdle in the evaluation of reasonableness"). *See generally* United States v. U.S. District Court (*Keith*) 407 U.S. 297, 313 (1972) (stating that national security cases "often reflect a convergence of First and Fourth Amendment values not present in 'ordinary' crime").

[291] *Zurcher*, 436 U.S. at 565-66 ("Nor, if the requirements of specificity and reasonableness are properly applied, policed, and observed, will there be any occasion or opportunity for officers to rummage at large in newspaper files or to intrude into or to deter normal editorial and publication decisions."); *Stanford*, 379 U.S. at 486 (finding that Fourth Amendment protection is already in place for the process of obtaining warrants).

[292] *Cf.* Amar, *supra* note 37, at 806 ("[T]he vehicle for this integration [of the First Amendment into the Fourth Amendment analysis] is of course not the warrant, not probable cause, but constitutional reasonableness.").

[293] Kerr, *Four Models*, *supra* note 10, at 516-19 ("[T]he positive law model is only an occasional guide to Fourth Amendment protection. Some [Supreme Court] opinions embrace it and others reject it.").

[294] Garlinger, *supra* note 267, at 1144-45.

crimes that directly invoke speech or other associational crimes.[295] Still, as Solove explains, "[e]ven where the criminalized activity is not itself expressive or associational, there may be a chilling effect sufficient to trigger First Amendment procedural protections."[296] Here, the defendant could argue that the police's conduct invokes the Fourth Amendment because the threat of government surveillance (and subsequent use of evidence at trial) would chill or deter individuals from associating with others on political or religious grounds.[297] This type of chilling can be distinguished from *Laird* where there was no discernable harm.[298] Here, the threat of use of evidence in criminal cases provides the specifiable harm that underscores the chilling analysis.[299]

Using First Amendment principles this way has the benefit of avoiding the aforementioned problems associated with societal expectation as the marker for reasonable expectation of privacy.[300] At least with expressive associational interests, there is some independent principle beyond simply what a person or society thinks is reasonable that can inform when Fourth Amendment protection applies.[301] Nevertheless, the problems of where to draw the line and what becomes of the Doctrines remain. Assuming that surveillance can chill this type of expressive association, how long must the surveillance be before triggering the reasonable expectation privacy test? One month? Two weeks?

[295] Solove, *supra* note 277, at 156.

[296] *Id.* Solove's focus is on information gathering rather than surveillance. *Id.* ("In many cases involving government information gathering about First Amendment activities, the government is collecting data to generate evidence for use in criminal cases.").

[297] *Id.* ("People might be chilled in writing or saying certain things, owning certain books, visiting particular websites, or communicating with particular individuals, groups, and organizations if the government can obtain and use information about these activities in a criminal prosecution.").

[298] Laird v. Tatum, 408 U.S. 1, 13-14 (1972) ("Allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm . . . .").

[299] *Id.* ("Even if there were no criminal case brought, the fear that engaging in First Amendment activities might trigger an arrest or a potential criminal probe might be sufficiently daunting to chill such activities."). Insisting that the chilling effect associated with the *potential* of police surveillance is not specific enough or otherwise constitutes identifiable harm is not fatal to the argument. Again, I am not directly applying First Amendment rights to social networking communications, which means I am not strictly bound by the specific constitutional requirements under which the chilling effect applies. Rather, the point here is to use the principles embodied by the First Amendment—including the chilling jurisprudence—as a means to apply Fourth Amendment protection.

[300] *See supra* Part II.B.1 (explaining the conceptual difficulties of defining a reasonable expectation of privacy).

[301] *See* Solove, *supra* note 277, at 159 ("[T]o determine whether First Amendment procedural protections will apply, courts should first look to see whether the activity at issue is within the scope of the First Amendment. Next, courts must determine whether the government information gathering has a cognizable chilling effect on First Amendment activity.").

An advocate of this revised mosaic approach—similar to one using societal expectation—would surely point to significant lengths of surveillance as frustrating a person's expressive associational interests.[302] But it would appear that if surveillance does in fact affect this associational right, awareness that the government may be watching even for a short period could equally deter protected activity.[303] For instance, a person may not desire to attend a specific religious, political, or cultural gathering because she knows the government may be monitoring her. Again, it is not clear why numerous trips or greater amounts of data are necessary before triggering reasonable expectation. To be sure, scholars proposing revisions to Fourth Amendment jurisprudence using expressive associational principles pre-date *Jones* and the introduction of mosaic theory.[304] Ultimately, the problem is the generalized nature of the government intrusion here, regardless of its length. The threat of *any* surveillance of a person's movements necessarily implicates many potential First Amendment-related activities.[305]

In turn, this revised mosaic approach once again risks the wholesale rejection or fundamental altering of the Doctrines. Given that expressive associations may be found in even short-term public movements, it is not clear how much room is left for the Public Disclosure Doctrine.[306] Similar issues arise with keeping the Third Party Doctrine intact. The threat of undercover police officers, much like the threat of surveillance, may chill individuals from expressing themselves to others (e.g., telling them about their religious beliefs) or otherwise deter individuals from associating with others.[307] These individuals will be afraid that these undercover agents may reveal their

[302] *See id.* at 157 ("[L]imited surveillance of activities visible to the public would most likely not trigger First Amendment protection, but a more systematic campaign of public surveillance might present a different situation.").

[303] *Id.* at 156 ("A person might not want to purchase a book about making bombs or flying a plane if it will be used against him or her in a trial for conspiracy to engage in terrorist acts.").

[304] *See supra* note 280 and accompanying text (analyzing the views of scholars who posit that expressive associational rights could serve as additional protection to information that normally falls outside of Fourth Amendment protection).

[305] Solove, *supra* note 277, at 157 (explaining that the premise of the chilling effect doctrine is "that many [people] will not be willing to accept the risk and will simply change their behavior").

[306] *Id.* at 138 ("The third-party doctrine and doctrine on public surveillance have also severely curtailed the Fourth Amendment's protection of personal writings, reading habits, associations, and other First Amendment activities."); *see supra* Part II.B.2 (discussing the rejection of the Doctrines).

[307] *See* Solove, *supra* note 277, at 127 ("[G]overnment officials may use informants or pose as secret agents to infiltrate a political group. Under the 'assumption of risk' doctrine in Fourth Amendment law, information is not protected if a person revealed it to a police informant or undercover officer.").

secrets.[308] Scholars promoting the incorporation of expressive associational values in the Fourth Amendment framework seem to readily acknowledge that this strategy may come at the cost of abandoning or severely curtailing the Third Party Doctrine.[309] This Article, however, takes this outcome to be an unwanted consequence.[310]

That said, the idea of using the third model of reasonable expectation—and specifically associational principles—to underscore a mosaic approach is a good one. We just need to focus on a more discrete government intrusion and the mosaic must be employed in the right context. This Article does just that by using intimate associational rights targeted at protecting social networking on the Internet as key elements to a successful application of the mosaic doctrine.

III. USING THE MOSAIC THEORY TO PROTECT SOCIAL NETWORKING COMMUNICATIONS

A. *ISPs and the Third Party Doctrine*

Nearly all Internet communications are subject to the effect of the Third Party Doctrine.[311] The problem is that the bulk of this data is stored for various lengths of time in ISPs.[312] These servers consist of proprietary systems where information is stored so that it can be delivered to its intended recipient.[313]

[308] *Id.* at 127, 138. For this reason, some have argued for wholesale revision of the Doctrines. *See* Garlinger, *supra* note 267, at 1145 ("Although First Amendment activities might not be impacted directly enough to support a cognizable First Amendment challenge, the potential effect on privacy as an essential cognate to First Amendment interests might nonetheless justify revision of the third-party doctrine.").

[309] Burten, *supra* note 281, at 401-02 ("[W]hen determining the constitutionality of warrantless GPS tracking through the use of such technology that does not require as a prerequisite a physical intrusion, courts should examine the issue by accounting for substantive due process and First Amendment considerations when analyzing a defendant's reasonable expectation of privacy."); Garlinger, *supra* note 267, at 1141 ("Courts could thus begin to reformulate the current Fourth Amendment reasonable expectation of privacy test to more directly incorporate First Amendment values . . . .").

[310] *See supra* Part II.B.2 (discussing rejection of the Doctrines).

[311] *See* Tokson, *supra* note 70, at 604 ("If exposure to third-party equipment is sufficient to deprive information of any Fourth Amendment protection, then, as many privacy scholars have suggested, the Fourth Amendment will not apply to vast quantities of personal data and communications on the Internet." (citation omitted)).

[312] *Id.* at 585, 602-03 ("Virtually every kind of personal online data is stored and processed by third-party automated equipment in order to route communications, detect spam and viruses, block computer hackers, or generate advertising revenue."); *see* PRESTON GRALLA, HOW THE INTERNET WORKS 88-101 (8th ed. 2007) (describing how e-mails are transmitted and stored).

[313] GRALLA, *supra* note 312, at 88-101 ("The TCP [Transmission Control Protocol] 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

Facebook, Google, Hotmail, and Yahoo all utilize these ISPs to facilitate Internet transmissions.[314] Under a strict application of *Smith v. Maryland*, these communications seemingly lose any Fourth Amendment protection.[315] Similar to the disclosure of the phone numbers to an automated machine at the phone company, Internet users voluntarily disclose this information to the respective ISP and its computer system.[316] For instance, a Facebook user, before opening

can be read."); Tokson, *supra* note 70, at 602-03 (explaining how third-party automated equipment stores and processes online data in order to route e-mails and intercept spam and viruses).

[314] *See* 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) [hereinafter Kerr, *Lifting the "Fog"*] (describing how e-mails are routed by equipment owned by the ISP that processes their data); Tokson, *supra* note 70, at 602-03 (describing how e-mail service providers, such as Gmail and Hotmail, store e-mail data). Even deleted e-mails are at least temporarily stored on third party systems. *See, e.g.*, James X. Dempsey, *Digital Search & 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."); Evan E. North, Note, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1306 (2010) ("Facebook and MySpace, like [ISPs], store vast quantities of personal information on their servers."). Facebook has continued to expand its storage capacity and to increase its budget for the maintenance of its data centers. Rich Miller, *Facebook Makes Big Investment in Data Centers*, DATA CENTER KNOWLEDGE (Sept. 14, 2009), http://www.datacenterknowledge.com/archives/2009/09/14/facebook-makes-big-investment-in-data-centers, *archived at* http://perma.cc/6KA5-JDEG.

[315] Smith v. Maryland, 442 U.S. 735, 745-46 (1979) ("We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.' The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required."). Some scholars suggest that the Third Party Doctrine would not apply here because the Doctrine contemplates that the disclosure will ultimately be exposed to human observation, which is unlikely when talking about the vast amounts of data stored on an ISP. Tokson, *supra* note 70, at 616 ("[T]he automated collection of personal data without eventual exposure to a human observer does not constitute a loss of privacy in theory or law."). But this distinction would seem to go against the explicit ruling of *Smith v. Maryland* and moreover would have to explain why this difference is dispositive, particularly when Facebook employees can potentially review data. Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 19-22 (2013) ("The logical question then becomes: *what is so unique about the status of information actually being observed as opposed to potentially being observed when it comes to privacy rights?*").

[316] *See* Semitsu, *supra* note 25, at 329 (arguing that a Facebook user does not have Fourth Amendment protection, because such protection would apply to "the overwhelming majority, if not all, content on Facebook since it is information that a Facebook user

an account, acknowledges that Facebook will hold her information.[317] This voluntary choice would vitiate any constitutional protection. It does not matter that a person *subjectively* expects her communication to remain private and not reviewed by the ISP or otherwise disclosed to the government.[318] This situation is no different from one in which a person makes a disclosure to a government informant, erroneously believing that the information will be used for a limited purpose or otherwise not used against her at trial.[319] From a constitutional perspective, all that matters is that the communication—whether intended for an undercover informant or ISP—was voluntarily disclosed.[320]

voluntarily agrees to have held in third party storage"); Strandburg, *Home*, *supra* note 233, at 634 (citing scholars who have addressed the implications of the Third Party Doctrine in the Internet context and have recognized that under a strict interpretation of the doctrine, "there is virtually no Fourth Amendment protection for any information conveyed over the Internet or other digital intermediary").

[317] *Statement of Rights and Responsibilities, Sharing Your Content and Information*, FACEBOOK, https://www.facebook.com/legal/terms, *archived at* http://perma.cc/EKE3-YJ7V (last revised Nov. 15, 2013) ("We designed our Data Use Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information."). It does not matter how long the third party server stores the information; even a temporary disclosure would satisfy the Third Party Doctrine and vitiate any Fourth Amendment protection. *See, e.g.*, *Smith*, 442 U.S. at 744 (observing only that the information was voluntarily disclosed, and not the length of time that the information had been disclosed); United States v. Miller, 425 U.S. 435, 443 (1976) (holding that the Fourth Amendment does not prohibit obtaining information revealed to third party on the assumption that it would be used for a limited purpose).

[318] *See Miller*, 425 U.S. at 443 ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); United States v. White, 401 U.S. 745, 751-52 (1971) (expressing concerns with defendant's constitutionally justifiable expectations of privacy, not with "the expectations of particular defendants in particular situations"). Indeed, at least one study has shown that Internet users would consider disclosure by an ISP to be a privacy violation. *See* Tokson, *supra* note 70, at 622-26 (reporting the results of a survey of seventy-one law students who regularly use the Internet).

[319] *See Miller*, 425 U.S. at 443 (explaining that, by "revealing his affairs to another," an individual "takes the risk . . . that the information will be conveyed . . . to the Government"); *White*, 401 U.S. at 751-52 ("If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case.").

[320] *See Miller*, 425 U.S. at 443; *supra* Part I.A (explaining that, where a defendant has voluntarily disclosed his wrongdoing to a person, it matters not that he mistakenly believed it would not be shared with Government authorities). While Facebook may have its own privacy policies intended to protect users, these policies allow the ISP to disclose information to the government but, more importantly, these policies only bind Facebook and do not create Fourth Amendment protection. In other words, Facebook is free to modify

The Supreme Court has not addressed whether and how these communications should be protected under the Fourth Amendment. Lower federal courts, however, have taken divergent opinions on whether Fourth Amendment protection applies to these Internet communications. Some find that the content of the e-mails, but not the subject lines or recipient names, are protected under Fourth Amendment, despite their disclosure to ISPs.[321] These courts focus on the old distinction between content and non-content information originally created to protect mail delivered by the U.S. Postal Service.[322] Even though a letter is voluntarily disclosed to the postal official, only what is printed on the face of the envelope, including the recipient's name and mailing address, loses protection.[323] The substance of the letter remains private. The rationale for this rule is that citizens should be able to take advantage of the mail system without foregoing the privacy of their communications.[324] Other courts, however, have strictly applied the Third Party Doctrine under *Smith* and have found that e-mails do not have any Fourth

these policies (without notice) and offer less protection without any Fourth Amendment repercussions. *See Facebook Data Use Policy, Some Other Things You Need to Know*, FACEBOOK, https://www.facebook.com/about/privacy/ (last revised Nov. 13, 2013), *archived at* http://perma.cc/ASV7-BXSV; *see also* Grimmelmann, *supra* note 48, at 1183.

[321] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("[A] subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'" (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007))); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (explaining that surveillance of e-mail addresses is "conceptually indistinguishable" from that of physical mail, for which the Supreme Court has held that "the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail"); United States v. Maxwell, 45 M.J. 406, 417-19 (C.A.A.F. 1996) (analogizing America Online e-mails to letters).

[322] *See* United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable [within the meaning of the Fourth Amendment]."); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (holding that letters and sealed packages cannot be opened unless the government obtains a warrant); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1020-31 (2010) [hereinafter Kerr, *Applying*] (contending that a "content/non-content distinction" allows for the neutral application of the Fourth Amendment to the Internet, whereby "access to the contents of communications [for which people have taken steps to assure its limited audience] should be treated like access to evidence located inside").

[323] Kerr, *Lifting the "Fog," supra* note 314, at 1023 (explaining that there is no reasonable expectation of privacy in the outside of a package, but there is in the interior of a package, and, accordingly, the government must have a warrant to open a package).

[324] *See* United States v. Van Leeuwen, 397 U.S. 249, 251-52 (1970) (analogizing communications via mail to verbal free speech).

Amendment protection.[325]

No court has directly tackled social networking communications, which do not neatly fit into the content/non-content distinction. The reason for this is because sites such as Facebook allow users to do more than just send discrete e-mails. These types of sites employ a host of different tools, including posting status updates or photographs, sending and receiving instant messages, and video-conferencing.[326] The vast majority of these communications are vulnerable to government collection.[327] There are statutory provisions (e.g., the Electronic Communications Privacy Act) in place to supposedly protect all Internet communications—and thus also social networking communications—from unwarranted government intrusion, but these are not constitutionally mandated and, moreover, appear to have major gaps in protection.[328] In order to prevent users from being at the mercy of legislatures, a constitutional framework is thus required. Scholars have also posited a number of Fourth Amendment-based theories to protect Internet communications with varying degrees of success in protecting social networking communications while preserving the current Fourth Amendment landscape.[329] The purpose here is

[325] *See, e.g.*, Rehberg v. Paulk, 598 F.3d 1268, 1281-82 (11th Cir. 2010) ("A person . . . loses a reasonable expectation of privacy in emails . . . after the email is sent to and received by a third party."), *vacated*, 611 F.3d 828 (11th Cir. 2010) (holding that the individual had no clearly established privacy rights in e-mail content voluntarily transmitted over the Internet and stored at third-party ISP); *In re* Search Warrant for Contents of Elec. Mail, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009) (finding that e-mail 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").

[326] *See* Jonathan Strickland, *How Facebook Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/internet/social-networking/networks/facebook5.htm (last visited Sept. 26, 2014), *archived at* http://perma.cc/L4U-J4UV (describing the features of Facebook and various tools available to users); *Page Basics*, FACEBOOK, https://www.facebook.com/help/387958507939236/, *archived at* http://perma.cc/ST3J-3A3Q; *Video Calling: Basics & Privacy*, FACEBOOK, https://www.facebook.com/help/439078162792430/, *archived at* http://perma.cc/7TNH-Q63T.

[327] It appears that the video-chatting content is not stored in any way. *Video Calling: Basics & Privacy*, *supra* note 326.

[328] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (prohibiting access to stored electronic communications) (codified as amended at 18 U.S.C. §§ 2510-22, 2701-11, 3117, 3121-27 (2012)); *see also* Semitsu, *supra* note 25, at 292 (arguing that the ECPA ultimately does not provide comprehensive protection to social networking communications). For this reason, some scholars have proposed revised statutory schemes to fully protect Internet communications. *See* Stephen Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 243 (2012) (arguing that legislative efforts are the best way to combat the implications of the Third Party Doctrine in connection with social networking on the Internet); *see generally* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014).

[329] *See*, *e.g.*, SLOBOGIN, *supra* note 233, at 199 (arguing that disclosing to machines instead of humans should not vitiate privacy, but this would require overruling *Smith* as well

not to critically examine these theories. The focus, instead, is to resurrect the mosaic theory as an effective means to protect social networking communications while at the same time preserving the basic application of the Third Party Doctrine. To be sure, Fourth Amendment protection is pluralistic. As previously discussed, the Court itself has used different theories when applying the reasonable expectation of privacy test.[330] There is no reason why this variety should not be present in the Internet context. This Article, thus, does not seek to supplant other theories. Its aim is more modest and narrowly focused. It seeks to use the mosaic theory as a mechanism to highlight the importance of social networking on the Internet as a distinct form of communication worthy of Fourth Amendment protection.

The issue of protecting social networking communications is particularly important given the recent news that the NSA has been monitoring e-mail communications over sites such as Facebook, Gmail, and Yahoo, among others.[331] It appears that the NSA has been working with these ISPs to gather significant amounts of information from non-U.S. Internet users abroad, ostensibly related to national security concerns.[332] The release indicates,

as providing a justification for why this distinction matters for Fourth Amendment purposes); Kerr, *Lifting the "Fog," supra* note 314, at 837-38 (arguing that courts should use the content/noncontent distinction; but this aspect of Kerr's theory fails to account for many social networking communications that do not fit into this category); Strandburg, *Home*, *supra* note 233, at 654-64 (arguing that the Internet is an extension of the home and so all communications should be protected; but this theory thus rejects the ability of the government to use fake identities to garner information much like in the real world); Tokson, *supra* note 70, at 611-19 (same as Slobogin); *see also* Bedi, *supra* note 315, at 19-28 (discussing various theories proposed by scholars and their respective drawbacks); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 976-77 (2007) (discussing ways to employ the third party doctrine that may protect certain types of information); Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 167-68 (2005) (discussing proposal to limit effect of Third Party Doctrine by focusing on type of information disclosed and to whom it was disclosed).

[330] Kerr, *Four Models*, *supra* note 10, at 506.

[331] *See* Glenn Greenwald and Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, *archived at* http://perma.cc/8KQA-TEQ7 (discussing the "reignite[d] longstanding debates in the US over the proper extent of the government's spying powers" in light of recent disclosures regarding the NSA's collection of telephone and e-mail records).

[332] *See* Connor Simpson, *How Google and Facebook Cooperated with the NSA and PRISM*, YAHOO NEWS, (June 8, 2013, 10:56 AM), http://news.yahoo.com/google-facebook-cooperated-nsa-prism-145643099.html, *archived at* http://perma.cc/E6YN-THPL (explaining the legal processes by which tech companies are required to turn over such information to the NSA); *Facebook Data Use Policy: Some Other Things You Need to Know*, FACEBOOK, (last revised Nov. 15, 2013), https://www.facebook.com/full_data_use_policy (providing notice that Facebook can

however, that the government swept widely in its acquisition of information and may have also collected e-mails from U.S. citizens.[333] Expectedly, this news triggered outcries from a variety of sources, including scholars and politicians alike.[334] Many have argued that this type of surveillance—assuming it targeted citizens—is unconscionable and, more importantly, violates the Fourth Amendment.[335] Following other lower federal courts, the FISA Court does seem to suggest that at least some of these e-mails would be constitutionally protected based on the content/non-content distinction.[336] But

release information per government request). However, it does not appear that the government would require Facebook's consent in acquiring this information. *Cf. In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 147-49 (E.D. Va. 2011) (finding that the government can compel information from ISsP because of the application of the Third Party Doctrine and lack of reasonable expectation of privacy).

[333] *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 7, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, *archived at* http://perma.cc/Z9KC-RL5D (explaining that the U.S. government may have inadvertently swept American e-mails). It does not appear that e-mails from outside the United States sent by non-citizens are protected under the Fourth Amendment. *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 265-68 (1990) ("'[T]he people' protected by the Fourth Amendment . . . refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community.").

[334] *See* Randy E. Barnett, Opinion, *The NSA's Surveillance is Unconstitutional*, WALL ST. J., July 11, 2013, http://online.wsj.com/news/articles/SB10001424127887323823004578593591276402574, archived at http://perma.cc/6VHN-DUR7 (discussing problematic Fourth Amendment implications of secret blanket data-seizure programs, which, through their covertness, allow the government to more easily violate the rights of the people); Jennifer Stisa Granick & Christopher Jon Sprigman, Op-Ed., *The Criminal N.S.A.*, N.Y. TIMES, June 27, 2013, http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html, *archived at* http://perma.cc/ZA3G-B3KB; Ms. Smith, *It's Hitting the Fan: Anger Mounts over PRISM, NSA Spying Scandals*, June 12, 2013, NETWORKWORLD (June 12, 2013), http://www.networkworld.com/community/blog/its-hitting-fan-anger-mounts-over-prism-nsa-domestic-spying-scandals, *archived at* http://perma.cc/3JD5-DAMQ (describing how politicians have come out against the NSA surveillance program).

[335] *See supra* note 323. The ACLU has brought suit against the government in connection with its collection of information from ISPs. Klayman v. Obama, 957 F. Supp. 2d 1, 1-5 & n.1 (D.D.C. 2013)

[336] *See* Redacted, 2011 WL 10945618, at *26 (FISA Ct. Oct. 3, 2011). Even if Fourth Amendment protection applies, there would remain an issue as to whether surveillance for national security reasons would still be reasonable under the Fourth Amendment and what requirements would be necessary (e.g., warrant and probable cause) before the government could carry out these searches. *See, e.g.*, Glenn Sulmasy & John Yoo, Katz *and the War on Terrorism*, 41 U.C. DAVIS L. REV. 1219, 1219 (2008) (arguing that the lower courts have

under a strict application of the Third Party Doctrine, it is not clear to what extent the bulk of these communications fall under the purview of the Fourth Amendment.[337] The question of Facebook communications specifically seems to be unresolved. How should they be protected given that they do not necessarily fit into the content/non-content dichotomy? And can the Fourth Amendment apply to these communications without jeopardizing the Doctrines?

B. *Protecting Intimate Associations over the Internet*

Because my argument relies on the third model of reasonable expectation, the first step is to identify the principle or value that the mosaic seeks to promote when it comes to communications over social networks. Here, the focus should be on intimate associations rather than expressive associations as described earlier.[338] Deriving from both First Amendment and due process principles, these relationships are highly personal and foster close, intimate bonds. They stand as the cornerstone of individual liberty and thus receive the highest level of protection.[339]

Griswold v. Connecticut[340] stands as an early expression of the Court's

correctly not required a warrant for national security searches in balancing constitutional rights and national security).

[337] *See* Victor Luckerson, *You Probably Agreed to NSA Snooping When You Accepted That Website's Terms of Service*, TIME (June 14, 2013) http://business.time.com/2013/06/14/you-probably-agreed-to-nsa-snooping-when-you-accepted-that-websites-terms-of-service/, *archived at* http://perma.cc/X37T-HHAD (explaining that e-mails may not be protected under Fourth Amendment because user voluntarily allowed ISP to hold information); *supra* Part III.A and accompanying notes (discussing complications in the application of the Third Party Doctrine to Internet communications). One could argue that First Amendment rights should directly apply to this information. *See supra* note 280 and accompanying text. *But see* Will Baude, *How Could Surveillance Violate the First Amendment?*, PRAWFSBLAWG, (June 15, 2013), http://prawfsblawg.blogs.com/prawfsblawg/2013/06/how-could-surveillance-violate-the-first-amendment.html, *archived at* http://perma.cc/6HRD-XL2H (arguing that First Amendment directly applied would not help because NSA does not appear to be targeting specific groups).

[338] *See* Roberts v. U.S. Jaycees, 468 U.S. 609, 617-18 (1984) ("Our decisions have referred to constitutionally protected 'freedom of association' in two distinct senses. [In addition to expressive association,] the Court [also] has concluded that choices to enter into and maintain certain intimate human relationships must be secured against undue intrusion by the State because of the role of such relationships in safeguarding the individual freedom that is central to our constitutional scheme."); *supra* Part II.C and accompanying notes.

[339] *See Roberts*, 468 U.S. at 618 ("The Court has long recognized that, because the Bill of Rights is designed to secure individual liberty, it must afford the formation and preservation of certain kinds of highly personal relationships a substantial measure of sanctuary from unjustified interference by the State.").

[340] 381 U.S. 479 (1965).

recognition of this right to intimate associations.[341] In overturning Connecticut's ban on the use of contraceptives by married couples, the Court distinguished a political or other expressive association from a marriage, which stands as "an association that promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects."[342] The Court found that marriage "is an association for as noble a purpose as any involved in our prior decisions."[343] In *Roberts v. U.S. Jaycees*,[344] the Court further expanded the definition of this intimate associational right to include not only married couples but any close, personal relationships.[345] The Court explained that "individuals draw much of their emotional enrichment from close ties with others" and that "[p]rotecting these relationships from unwarranted state interference therefore safeguards the ability independently to define one's identity that is central to any concept of liberty."[346] It described the quintessential protected relationship as one involving close ties amongst a small group of individuals with whom one shares "not only a special community of thoughts, experiences, and beliefs, but also distinctively personal aspects of one's life."[347] The Court contrasted this type of relationship with business associations, which do not share the same level of "deep attachments and commitments" and thus are not worthy of constitutional protection.[348] For this reason, the Court found that the defendant

[341] *Id.* at 482-84 (finding that certain intimate associations are protected as penumbras of the specific guarantees in the Bill of Rights); *see* Kenneth L. Karst, *The Freedom of Intimate Association*, 89 YALE L.J. 624, 625 (1980) (arguing that *Griswold* and its progeny can all "be seen as variations on a single theme: the freedom of intimate association"); Roling, *supra* note 267, at 909 (explaining Professor Karst's view that "Griswold and its progeny can all 'be seen as variations on a single theme: the freedom of intimate association'").

[342] *Griswold*, 381 U.S. at 485-86 (holding that there is a right of privacy in marriage "older than the Bill of Rights").

[343] *Id.* (holding that its sacredness demands the constitutional protection of the marriage association).

[344] 468 U.S. 609.

[345] *Id.* at 610 (holding that certain personal relationships, not just those of married couples, are entitled to constitutional protection).

[346] *Id.* at 619-20 ("[B]ecause the Bill of Rights is designed to secure individual liberty, it must afford the formation and preservation of certain kinds of highly personal relationships a substantial measure of sanctuary from unjustified interference by the State.").

[347] *Id*. ("[Protected relationships] are distinguished by such attributes as relative smallness, a high degree of selectivity in decisions to begin and maintain the affiliation, and seclusion from others in critical aspects of the relationship.").

[348] *Id.* Other cases, such as *Lawrence v. Texas*, 539 U.S. 558 (2003), and *Boy Scouts of America v. Dale*, 530 U.S. 640 (2000), further substantiate a right to protecting essential qualities of relationships and the autonomy to define them free from government intrusion. *See* Crocker, *supra* note 42, at 21 (2010) ("*Lawrence*, *Roberts*, and *Dale* are all cases protecting different kinds of interpersonal relationships that are both expressive and identity definitional.").

company, a large nonselective organization composed largely of strangers, could not exclude women because this exclusion did not support any intimate or otherwise personal association.[349]

It is interesting that scholars invoking associational principles in the Fourth Amendment context have opted to focus on expressive associations rather than intimate associations.[350] Perhaps, the thinking is that since this type of personal relationship typically happens in a person's home or over the phone—places where Fourth Amendment protection already applies—there is less of a need to incorporate this value.[351] However, it turns out that this right is particularly relevant when it comes to social networking on the Internet and creating a workable mosaic theory.[352]

Social networking sites have revolutionized how people communicate over the Internet, making social media more than just simply a way to transmit information quickly and efficiently.[353] "[It] has created unique and different

[349] *Roberts*, 468 U.S. at 620 ("[F]actors that may be relevant include size, purpose, policies, selectivity, congeniality, and other characteristics that in a particular case may be pertinent. In this case, however, several features of the Jaycees clearly place the organization outside of the category of relationships worthy of this kind of constitutional protection.").

[350] *See supra* Part II.C and accompanying notes (discussing the incorporation of First Amendment expressive associational rights into the Fourth Amendment framework).

[351] *See* United States v. Karo, 468 U.S. 705, 717 (1984) (holding that the government is not free to monitor, without a warrant, beepers in private residences); Katz v. United States, 389 U.S. 347, 361 (1967) (holding that words spoken into a receiver in a public telephone booth, like words spoken inside a home or in any other place where defendant justifiably relies on privacy, were constitutionally protected); *see* Garlinger, *supra* note 267, at 1129 ("Put differently, one might say that the First Amendment protects 'expressive privacy'—privacy that is designed to cultivate autonomy in furtherance of democratic debate, whereas the Fourth Amendment protects 'intimate privacy.'").

[352] Scholars who have explicitly connected social networking on the Internet to the First Amendment right to intimate association have focused exclusively on the direct application of the First Amendment without consideration of incorporating this norm under the Fourth Amendment's reasonable expectation of privacy test. *See, e.g.*, Inazu, *Virtual Assembly*, *supra* note 36, at 1118-21 (discussing conceptual difficulties in the application of First Amendment, rather than the Fourth Amendment, protections of intimate, as opposed to expressive, association).

[353] *See* Bargh & McKenna, *supra* note 48, at 586-87 (describing the stages of familiarity and trust involved in the forging and maintenance of online relationships); Nicole B. Ellison et al., *The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites*, 12 J. COMPUTER-MEDIATED COMM. 1143, 1143-44 (2007) (discussing the broad use of social networking sites in both the "maintenance of existing social ties and the formation of new connections"); Charles Steinfield et al., *Social Capital, Self-Esteem, and Use of Online Social Networking Sites: A Longitudinal Analysis*, 29 J. APPLIED DEVELOPMENTAL PSYCHOL. 434, 434 (2008) (analyzing panel data from Facebook users in the relationship between Facebook use, psychological well-being, and social capital); Stephanie Tom Tong et al., *Too Much of a Good Thing? The Relationship Between*

way[s] for [individuals] to develop and maintain friendships via the [I]nternet, no matter the physical distance."[354] Social networking sites provide a safe environment where "those who are socially anxious and those who are lonely [can] turn . . . as a means of forming close and meaningful relationships with others."[355] One study found that individuals expressed their true selves more freely over social networking sites than in face-to-face encounters.[356] This may explain why for many younger users social networking sites like Facebook have replaced physical interaction as a way to develop relationships.[357]

Psychologists have found that these online relationships can be just as "real" as those that take place in face-to-face meetings.[358] Studies show, for instance, that Facebook relationships share the same breadth, depth, and quality as those developed in person.[359] Legal scholars, too, have recognized the similarity

Number of Friends and Interpersonal Impressions on Facebook, 13 J. COMPUTER-MEDIATED COMM. 531, 531 (2008) (inquiring into the curvilinear effect of sociometric popularity and social attractiveness and quartic relationship between friend count and perceived extraversion); Tom R. Tyler, *Is the Internet Changing Social Life? It Seems the More Things Change, the More They Stay the Same*, 58 J. SOC. ISSUES 195, 195 (2002) (discussing the Internet's impact, or lack thereof, on many aspects of social life); Jessica Vitak, Facebook "Friends:" How Online Identities Impact Offline Relationships (Apr. 22, 2008) (unpublished M.A. thesis, Georgetown University), *available at* http://www.academia.edu/412944/Facebook_Friends_How_Online_Identities_Impact_Offline_Relationships, *archived at* http://perma.cc/BCD2-27UM ("[F]ocusing on how people create an online identity and how that identity affects the formation and maintenance of 'friendships' in the digital world.").

[354] *See* Hope Bareham, *The Creation and Maintenance of Relationships with Social Networking Sites: How Facebook Has Recreated the Way Friendships Are Formed*, DIGITAL LITERACIES BLOG, Apr. 25, 2011, http://digitallithb.wordpress.com/2011/04/25/final-paper-digital-literacies/, *archived at* http://perma.cc/9MW9-GLZN (discussing the ways in which Facebook has altered friendship formation).

[355] Tyler, *supra* note 353, at 200; *see* John A. Bargh et al., *Can You See the Real Me? Activation and Expression of the "True Self" on the Internet*, 58 J. SOC. ISSUES 33, 44-46 (2002) (discussing the benefits of online communication for individuals with certain personality types).

[356] Bargh et al., *supra* note 355, at 44-46.

[357] Bargh & McKenna, *supra* note 48, at 580-82 (describing the stages of familiarity and trust involved in the forging and maintenance of online relationships); Vitak, *supra* note 353, at 4-5; Bareham, *supra* note 354, at Discussion Section (discussing the ways in which Facebook has altered friendship formation).

[358] *See* Bargh et al., *supra* note 355, at 44-46 ("[C]ompared to face-to-face interactions, people are better able to present, and have accepted by others, aspects of their true or inner selves over the Internet."); Bargh & McKenna, *supra* note 48, at 581 ("[S]tudies reveal[] that . . . people were better able to express their 'true' selves (those self-aspects they felt were important but which they were usually unable to present in public) to their partner over the Internet than when face-to-face . . . .").

[359] *See* Bargh & McKenna, *supra* note 48, at 581 ("Results showed that on-line relationships are highly similar to those developed in person, in terms of their breadth,

between online and offline relationships.[360] Relying on psychological and social studies, Professor James Grimmelmann, for instance, cites three ways that Facebook relationships promote the same social dynamics and interpersonal values found in face-to-face relationships.[361] First, Facebook allows users to construct their own identities much like individuals do in more traditional settings. Users have full control over what pictures they post and what information they decide to include on their profile.[362] Second, Facebook and its myriad communication tools distinguish it from traditional e-mail systems, which merely allow back-and-forth messaging. Grimmelmann specifically cites to a user's ability to add someone as a contact—a fundamental act that signals a level of trust.[363] This leads to Grimmelmann's final point about Facebook's ability to encourage and engage mutual interaction.[364] He points to the wall-to-wall tool (which allows back and forth between users) and the status update tool (which allows users to express what is on their minds) as mechanisms that activate and encourage relational impulses between users.[365] By promoting these three qualities of autonomy, community, and identity, social networking sites like Facebook provide a structure under which individuals can satisfy these impulses in a virtual setting.[366] The end result is a relationship that feels just an authentic as a

depth, and quality.").

[360] *See* Grimmelmann, *supra* note 48, at 1152 ("Online interactions are no different [from daily social interactions]; you can use everything from your chat nickname to your home page to influence how other people think of you."). For a more detailed discussion, *see* Bedi, *supra* note 315, at 53-55 (detailing how Facebook promotes social dynamics by providing a forum in which people can craft social identities, forge reciprocal relationships, and accumulate social capital).

[361] Grimmelmann, *supra* note 48, at 1151-59 (explaining that Facebook supports the creation of identity, strengthens personal relationships, and provides a sense of community for users).

[362] *Id.* at 1152 ("Just as your choice of clothing and hairstyle signals how you think of yourself (and want others to think of you), so does your choice of profile photo.").

[363] *Id.* at 1154-55 ("The act of adding someone as a contact is the most fundamental. It's a socially multivalent act . . . . [It is] a form of minor intimacy that signals trust.").

[364] *Id.* at 1155-56 ("Facebook's design encourages reciprocal behavior by making the gesture-and-return cycle visible and salient.").

[365] *Id.* ("Facebook's 'Wall-to-Wall' feature, which displays the back-and-forth of Wall posts between two users, explicitly embeds this semi-public conversational mode in the site's interface design. The norms of social network sites encourage both relationships and public affirmation of them.").

[366] *Id.* at 1159 (explaining that social networking sites allow a platform for users to advertise virtual representations of social status and "coolness"). The point of the preceding analysis is less about equating the specifics of Facebook relationships with their offline counterparts and more about highlighting the similar reactions and feelings individuals experience when making either of these associations.

traditional relationship.[367]

A reader may be unconvinced that traditional relationships can really be analogized to ones over social networking sites. It certainly does not take a psychological study to point out the advantages of physically seeing and talking to someone. A couple of things can be said in response. First and foremost, this Article is not suggesting that the two types of relationships are the same. No doubt, a face-to-face relationship has different and, perhaps, superior elements to an Internet relationship. I do not take issue with this reasoning. But this argument would be more relevant if my Article were suggesting intimate associational rights should apply directly to these Internet relationships. I'm not making such a bold claim. Instead, this notion of intimate associations is simply intended to inform a Fourth Amendment analysis. Given this more narrow and modest use, the resultant analogy to face-to-face relationships need not be fully realized. What matters is that both relationships invoke similar feelings amongst the participants. Here, I take the psychology and legal studies at face value. The qualities the Court ascribes to intimate associations (e.g., close emotional bonds, sharing private information) appear to be equally present in online relationships.[368]

Invoking intimate associational privacy in this way provides a way to protect social networking communications under the Fourth Amendment even though, individually speaking, these communications have no protection on account of their disclosure to an ISP. Under a mosaic approach, these communications taken together constitute something greater than the sum of their parts.[369] As a whole, they may represent an intimate relationship rather than simply a collection of transmissions, which on their own simply transmit information.[370] This basic feature of "the sum is greater than the parts" parallels the mosaic in *Jones*. There, a handful of trips, over a short period of time, reveal nothing; but many trips, over a longer period of time, reveal intimate information.[371] Similarly, in the social networking context, the individual communication on its own is not particularly important as it simply

[367] Bargh & McKenna, *supra* note 48, at 581 ("Results showed that on-line relationships are highly similar to those developed in person, in terms of their breadth, depth, and quality."); Grimmelmann, *supra* note 48, at 1159 (highlighting that social network sites support the growth of a user's identity, relationships and community in a manner similar to the user's persona offline); *see* Bargh et al., *supra* note 355, at 44-46 ("[B]y its very nature, [Internet communication] facilitates the expression and effective communication of one's true self to new acquaintances outside of one's established social network, which leads to forming relationships with them.").

[368] *See* Bargh & McKenna, *supra* note 48, at 581.

[369] *See supra* Part II.A (finding that even though individual or discrete movements lose protection based on their disclosure to the public view, the aggregation of these movements may constitute something worthy of protection).

[370] *See* Bargh & McKenna, *supra* note 48, at 582 (detailing the opportunities offered by social networking sites for users to form close personal relationships).

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

conveys information. Yet, a collection of social networking communications taken together constitutes an intimate relationship.[372] That said, my mosaic does not turn on simply quantitative data—the more trips, the more private information that is revealed. Rather, the collection of discrete transmissions taken together creates something qualitatively different. The end result is an intimate relationship of which the communications are constituent parts. If we care about the development of face-to-face relationships (via direct application of intimate associational rights), it stands to reason that this norm should be promoted in the Internet context when applying the Fourth Amendment reasonable expectation of privacy test. To hold otherwise would raise similar chilling effect concerns as described earlier, only this time the worry would be relationship formation, not political or religious associations.[373] If the government is allowed to acquire these communications without a warrant and probable cause, a user may be deterred from forming relationships over social networking sites for fear that the government may use the information against him.[374] This theory could certainly affect the current NSA activity and its mining of Internet communications, particularly those targeted at social networking ISPs.

C. *Applying the Mosaic to Social Networking Communications*

The foregoing only sketches out the basic contours of this mosaic theory. Questions still remain. How do you define an "intimate relationship"? Are non-social networking e-mails also protected? There is also the issue of the survivability of the Third Party Doctrine. Much like in the expressive associational context described earlier, does my mosaic deter or chill too much and thus chuck this longstanding doctrine? Finally, there are practical questions about how to implement such a theory and how the government should conduct itself when collecting information from these ISPs. The following sections expand on these questions and the general implementation of this theory.

1. Conceptual Viability

The first thing to note is that the mosaic presented does not seek to protect all communications. Not all relationships would come under the moniker of intimate association. The Court's discussion of protected "relationships" in

[372] *See* Grimmelmann, *supra* note 48, at 1154 (explaining that the continued sharing of personal information in a confidential setting increases feelings of intimacy and trust).

[373] *See supra* Part II.A (describing the chilling effects on associational and expressive freedoms when surveillance allows the government to ascertain a person's habits and beliefs).

[374] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.").

Jaycees provides an answer by distinguishing between personal and business relationships.[375] Under a mosaic theory-type analysis, if the communications taken as a whole indicate the type of relationship where a person shares personal aspects of his life in a meaningful way, this would suggest an association that should be protected.[376] An ongoing relationship with many communications over a period of time with a single person over a social networking site would provide the quintessential example of a bona fide relationship.[377] Social networking sites like Facebook, however, also allow users to set up a group of contacts or "friends" so that they can communicate collectively.[378] Communications with a few select people over a period of time would also seem to qualify as an intimate association worthy of Fourth Amendment protection. By contrast, posts to a large group of individuals; business-related e-mails, regardless of how limited the number of recipients; or discrete and sporadic e-mails to an acquaintance would probably not contain the deep commitment indicative of an intimate relationship worthy of protection.

The more complicated issue is not what constitutes a relationship, but when such a relationship is created such that its constituent communications are worthy of protection. Under my theory, does reasonable expectation of privacy apply at the moment a user starts communicating with an individual or does it apply only when the intimate association is fully developed following numerous communications over time? This is not a question of where to draw the line—i.e., how many individual transmissions over how much time—but rather how we should conceive of Fourth Amendment protection in this context.

In one sense, both situations can be conceptualized using the same mosaic. In the first scenario, these early communications have the potential to be part and parcel of a fully developed relationship, whereas the second scenario is simply the actualized version of this nascent relationship. As far as the application of Fourth Amendment protection, the distinction turns out not to be relevant. As previously discussed, associational rights jurisprudence protects against not only direct government intrusion but also those policies that deter protected activity.[379] Protecting only the actualized relationship would still

[375] Roberts v. U.S. Jaycees, 468 U.S. 609, 620 (finding that business relationships lacked the elements of personal liberty that demand constitutional protection); *see supra* Part III.B (contrasting a personal relationship (which involves a community of thoughts, experiences, beliefs, and personal aspects of one's life) with a business relationship (which lacks the same level of deep attachment and commitment)).

[376] *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

[377] *See* Bargh & McKenna, *supra* note 48, at 582 (detailing how users can form and strengthen meaningful personal relationships with both new and existing friends).

[378] *See How Do I Create a Group?*, FACEBOOK, https://www.facebook.com/help/167970719931213?sr=26&sid=0Thhyd8pNnWAWL6qE (last updated Sept. 2014), *archived at* http://perma.cc/C5Q-EDUB.

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

deter people from forming these relationships on social networking platforms. Individuals might be afraid that their relationship is not sufficiently developed to pass the reasonable expectation of privacy test. To prevent this chilling effect, all of these communications—regardless of how developed the relationship is—would have to be protected under the Fourth Amendment.[380]

There is also the issue of whether and how non-social networking communications would be protected under the instant mosaic theory. The focus of this Article is on social networking sites and how these communications can constitute intimate relationships. To be sure, one typically does not talk about a "Gmail relationship" or "Yahoo relationship." Exclusively using these e-mails probably means that the sender and recipient are business associates or acquaintances.[381] These systems, although effective as means of communication, do not hold the same importance as social networking communications, which may be the only source of communications for the online relationship.[382] In any event, these e-mails may be protected by other doctrines such as the content/non-content theory discussed earlier.[383] My argument is not intended to be the only way to secure Fourth Amendment protection. In fact, it is specifically geared to applying the mosaic theory in the social networking context, something that to date has not been done.

Nevertheless, the theory could also be used to cover some of these e-mails. The argument would be that these e-mails are sometimes used to facilitate what is otherwise an intimate association and thus are equally part and parcel of the relationship. In this way, these e-mails would bolster and develop existing relationships, whether on social networking sites or offline. This same mosaic-based argument could also apply to discrete social networking communications that bolster offline intimate associations. The offline and online components together create an intimate association worthy of protection. The restrictions mentioned earlier (e.g., business relationships or widely distributed communications) would still serve as a limiting factor but, at least conceptually, there would be no barrier to including these e-mail

[380] This would also include communications to an individual that turn out never to develop into a full-fledged relationship. The same concern of the chilling effect remains. Individual users may decide not to initiate conversations for fear that their relationships may never develop into relationships worthy of protection.

[381] *See* Crocker, *supra* note 42, at 22-32, 66-67.

[382] *See* Grimmelmann, *supra* note 48, at 1154. ("If all that social network sites offered were the ability to send other users messages, they'd have little to recommend them over other electronic media, like e-mail and IM. Social network sites work for relationship building because they also provide semi-public, explicit ways to enact relationships."); *cf.* Hyo Kim et al., *Configurations of Relationships in Different Media: FtF, Email, Instant Messenger, Mobile Phone, and SMS*, 12 J. COMPUTER-MEDIATED COMM. 1183, 1202-03 (2007) (discussing the use of phones as a way to reinforce existing social networks).

[383] *See supra* Part III.A (explaining that the substantive content of an e-mail may receive Fourth Amendment protection, while the e-mail subject line and recipient list is public information undeserving of such protection).

communications into my analysis assuming a bona fide intimate relationship.[384]

2. Survival of the Third Party and Public Disclosure Doctrines

At first blush, my proposal would seem to undercut the application of the Third Party Doctrine. If the point is to protect relationship formation, it seems that allowing the government to use undercover agents to develop relationships with suspects would have a similar chilling effect. Individuals may be afraid to develop close personal associations—much like in the Internet social networking context—if they think the government is posing as their friend and may reveal their secrets.[385]

Take the following scenario. Imagine an individual who develops a close personal relationship with an undercover government informant over numerous face-to-face meetings. This individual discloses many secrets, thinking they have become good friends. It turns out that the agent was duping the individual so that the suspect would reveal incriminating statements. Currently, under the Third Party Doctrine, none of these individual communications comes under the purview of the Fourth Amendment because the person voluntarily disclosed the information to a third party. This fact alone vitiates privacy protection, regardless of the individual's misplaced trust.

Under my mosaic proposal, these communications seemingly satisfy the reasonable expectation of privacy. In the aggregate, these communications obviously create a traditional intimate association—one with the aforementioned qualities of autonomy, identity, and community.[386] This means that the underlying communications—much like their Internet counterparts—should be protected. To do otherwise, risks deterring individuals from entering into close relationships for fear their secrets may be revealed.

However, the critical difference between a face-to-face relationship and an Internet relationship is the entity to whom the disclosure is made. In the face-to-face meeting, the information is disclosed to an individual who is part and parcel of the resultant relationship. In other words, the informant plays a substantive role in the development of the relationship. As explained earlier, the crux of the Third Party Doctrine is that the individual assumes the risk that the other person may reveal the information to the government.[387] The risk of

[384] There is no need to address the content of phone calls because, while they too may further develop existing relationships, they are already protected under Fourth Amendment jurisprudence. *See* Katz v. United States, 389 U.S. 347, 347 (1967).

[385] *See supra* Part II.A (suggesting that the growth of the "virtual age" may require courts to rethink the premise that an individual has no reasonable expectation of privacy for information voluntarily disclosed over the Internet).

[386] *See supra* Part III.B (describing the role of social networking sites in forming and strengthening meaningful personal relationships).

[387] *See supra* Part I.A (explaining that, under the Third Party Doctrine, an individual cannot maintain a reasonable expectation of privacy for information voluntarily

this disclosure is thus inherent in the relationship.[388] The potential of betrayal in fact affirms the relationship as genuine or authentic. Psychologists have found that relationships require trust but that this "cannot occur without accepting the possibility of betrayal."[389] Part of what makes a relationship genuine is taking on this risk.[390] In this way, to protect these communications by relying on the promotion of intimate associations would mean undercutting the very type of relationship at stake. For this reason, my mosaic theory has no role here and does not curtail law enforcement's ability to use this tool.

The disclosure to the ISP in Internet context works differently. This entity has no part of the resultant relationship developed between the sender and recipient of the communication.[391] The ISP is simply a necessary intermediary that holds the information such that it can be delivered to the intended recipient.[392] There is no substantive interaction or engagement between the user and the ISP. In turn, the risk of an ISP disclosing information—unlike the aforementioned risk of an informant disclosing information—does not contribute to the authenticity of the intimate association created between recipient and the sender. Put differently, the ISP has no stake or interest in the relationship.[393] The fact that the ISP is a machine further bolsters this point.[394] Allowing the government to acquire this information from the ISP therefore only seeks to chill the relationship between the sender and recipient. In this way, my theory only narrowly curtails the application of the Third Party Doctrine over the Internet as it relates to disclosures to ISPs.

---

transmitted).

[388] *But see* Crocker, *supra* note 42, at 34-40 (arguing that the Third Party Doctrine and intimate associations are at odds with each other, but failing to recognize how the Third Party Doctrine can be conceptualized such that it survives as a viable mechanism without curtailing the development of intimate associations).

[389] Evans, *supra* note 55, at 171.

[390] Roy J. Lewicki et al., *Trust and Distrust: New Relationships and Realities*, 23 ACAD. MGMT. REV. 438, 448-53 (1998) ("[S]ocial structures appear most stable where there is a healthy dose of both trust and distrust."); *see* Iris Bohnet & Richard Zeckhauser, *Trust, Risk and Betrayal*, 55 J. ECON. BEHAV. & ORG. 467, 467-72 (2004).

[391] *See* Tokson, *supra* note 70, at 602. ("Virtually every kind of personal online data is stored and processed by third-party automated equipment in order to route communications, detect spam and viruses, block computer hackers, or generate advertising revenue.").

[392] *Id.* (describing the exposure of personal online data to the automated equipment of online service providers).

[393] Though working from a different normative framework, Christopher Slobogin seems to makes a similar point when comparing disclosures to individuals from those to institutional third parties. SLOBOGIN, *supra* note 233, at 159-60, 199 (finding that unlike institutional third parties, human third parties have an autonomy interest that trumps the target's privacy interest).

[394] *Id*. ("[T]his mass of data is in many cases functionally anonymous, and the chance of it being directly observed by another human being (in the absence of direct government involvement) is extremely low.").

For instance, my approach would not affect the government's ability to acquire social networking communications through online duplicity.[395] A government agent, for instance, can serve as a Facebook friend and engage in a relationship much like an informant would do in a face-to-face context.[396] This person can garner the trust of the suspect and solicit incriminating information. This transmission—because it is revealed to the undercover officer—would have no Fourth Amendment protection.[397] There is nothing problematic here. Again, the possibility of betrayal is part of any relationship—whether offline or online—and thus invoking the protection of intimate associations has no role.

The government also remains free to acquire the non-content portion of e-mails or the subject line and recipient's name.[398] For one thing, none of these pieces of data are really identifiable in the social networking context.[399] More importantly, this information is not substantive in nature and thus cannot be part of an intimate relationship in the same way a content-laden communication would be.[400] This type of non-content data does not contain any substantive information and so would not garner any special attention.[401]

For similar reasons, my mosaic theory would not affect—at least at a conceptual level—the aforementioned NSA efforts to gather metadata from Verizon or other carriers. Here too, the government is only acquiring the non-content portion of the call or the number dialed, the length of the call, and other non-substantive information.[402] Because the substantive portion remains private, the mosaic theory has no role to play.

The theory also does not disrupt the Public Disclosure Doctrine. The

---

[395] *See* Crocker, *supra* note 42, at 53 ("Police are now reportedly making regular use of social networking sites. . . . Having revealed information about oneself to other persons, one could no longer have an expectation of privacy.").

[396] *See* Semitsu, *supra* note 25, at 320-21 (describing a case in which the FBI contacted a suspect's Facebook friend in order to learn information about the suspect's Facebook postings, and ultimately secured an arrest without resorting to a warrant or a subpoena).

[397] *See* Katz v. United States, 389 U.S. 347, 351 ("[W]hat a person knowingly exposes . . . is not a subject of Fourth Amendment protection.").

[398] *See supra* Part III.A.

[399] *See supra* Part III.A (explaining that even though a letter is voluntarily disclosed to a postal official, only the information printed on the face of the envelope loses protection).

[400] *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("[E]-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers.").

[401] My analysis thus does not conflict with *Smith v. Maryland*, which finds that metadata are not protected under the Fourth Amendment. Smith v. Maryland, 442 U.S. 735, 741 (1979) ("[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.").

[402] *See* Greenwald, *supra* note 150 ("[T]he numbers of both parties on a call are handed over, as is location data, call duration, unique identifiers, and the time and duration of all calls. The contents of the conversation itself are not covered.").

protection of intimate associations from government intrusion is isolated to social networking communications. Public movements—because they are voluntarily disclosed to the public at large—continue to lack any Fourth Amendment protection. A person's ability to develop and enter into intimate relationships is not adversely impacted knowing that the government may be conducting surveillance on individuals for various periods of time. While this activity could deter expressive associations (as described earlier), it does not seem to directly impact the ability to develop relationships with individuals.[403] As Solove explains, "Even where government information gathering implicates First Amendment values, First Amendment procedural protections should only apply if there is a discernible 'chilling effect.'"[404] Public surveillance does not appear to discernibly chill this type of relationship formation.[405] This is particularly true when one takes into account that intimate relationships—or more specifically the communications constituent of these relationships—occur in person, over the phone, or as this Article argues, over the Internet.

3. Practical Feasibility

The first and most obvious practical hurdle would be the rules that should govern the contours of a protected intimate relationship, both the type of relationship and the number of individuals involved. As to the first, we would need to separate business relationships from those that are personal. Would this include a distant cousin or a childhood friend or a business associate with whom one shares personal matters? Similarly, how many individuals are too many for an intimate association? Obviously, a Facebook post to a user's entire friend network would not be intimate enough, whereas a communication to a single person would certainly qualify. Where do we draw the line between these two extremes?

The first place to start is to recognize the nature of social networking sites like Facebook. These types of sites are primarily designed to develop and maintain social and personal bonds.[406] Business "relationships" are more likely to be conducted over e-mails systems like Yahoo or Gmail than over social networking sites like Facebook.[407] This difference bolsters my earlier point that

[403] *See supra* Part III.A (focusing on Fourth Amendment protection of associational and expression freedoms rather than freedom to form intimate relationships).

[404] *See* Solove, *supra* note 277, at 154.

[405] *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (discussing the threat of government surveillance to associational and expressive freedoms, but making no reference to freedom to form intimate relationships).

[406] *See supra* Part III.B (detailing how social networking sites have revolutionized how people communicate over the internet in the interest of creating and maintaining relationships).

[407] *See* Crocker, *supra* note 42, at 22-32, 66-67; Grimmelmann, *supra* note 48, at 1154 ("Social network sites work for relationship building because they also provide semi-public, explicit ways to enact relationships.").

the theory is specifically geared toward social networking. This may obviate the need to parse out the varying types of relationships. Any social networking "friend" would qualify as a potential personal relationship. Admittedly, this characterization is overbroad. For instance, people may have a number of Facebook friends with whom they do not share an intimate or otherwise personal bond (e.g., colleagues, acquaintances, business associates). It is not problematic to nevertheless cover these friends under my theory. In employing the Fourth Amendment in other contexts, the Court has not shied away from using a bright-line rule to a particular set of facts, even if the rule's underlying rationale is not applicable to the situation at issue.[408] The Court's application helps ensure that police can efficiently apply the relevant Fourth Amendment doctrine without worrying about after-the-fact trial court determinations.[409] The same reasoning applies here. For ease of administration, it makes sense to endorse a bright-line rule that all of a user's friends on a social networking site could potentially constitute intimate associations, even if a specific friend may not fall into this category. The alternative would create problems for the police and courts in deciphering which "friends" qualify as intimate associations. This conclusion is further bolstered by the chilling effect discussed earlier.[410] If there is no blanket protection, users may be afraid to become "friends" with new individuals on social networking sites for fear that the individual may not qualify as a potential intimate association.

The question of what to do with group communications amongst multiple friends over a social networking site remains. Limiting the number of individuals is certainly necessary, lest intimate associations lose any of their value.[411] For instance, imagine a user who creates a Facebook group that includes all of her law school graduating class. Communications amongst this group would obviously not be the kind of intimate associational bonds contemplated by *Jaycees*.[412] This type of line drawing would be similar to

[408] *See* United States v. Robinson, 414 U.S. 218, 235 (1973) (employing a bright-line rule that warrantless search of a cigarette container found on the suspect was proper under search incident to arrest doctrine even if rationale of destruction of evidence or safety of officer was not applicable in the particular factual situation).

[409] *Id.* ("The authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect.").

[410] *See supra* Part III.C.1 (explaining that protecting only actualized relationships could deter users from forming relationships in fear that their relationship was not sufficiently developed to pass the reasonable expectation of privacy test).

[411] *See* Roberts v. U.S. Jaycees, 468 U.S. 609, 620 (1984) ("Among other things, therefore, [intimate relationships] are distinguished by such attributes as relative smallness, a high degree of selectivity in decisions to begin and maintain the affiliation, and seclusion from others in critical aspects of the relationship.").

[412] *See id.* (establishing small size and high selectivity as the most pertinent factors entitling a group to Fourth Amendment protection).

Slobogin's line drawing in the surveillance context.[413] The point here is to present a workable number even though reasonable people may disagree on the exact number. Perhaps, five to ten friends may be a reasonable limitation. Again, the aim here is not to persuade the reader as to the exact number but instead to recognize that a limitation must be imposed.

The more interesting issue is how the government should handle acquiring information from the ISP with this mosaic in place. While much of a social networking site would be constitutionally protected under my mosaic theory—specifically, communications with a single friend—much of it would not; specifically, a user's public posts or communications amongst a large group of social networking friends. Practically speaking, how would the government go about collecting the latter, which would require no warrant or probable cause, without interfering with the former?

One solution would be for the ISP to provide the government with the basics of an individual's account, including the bulk of what would not be protected. In the Facebook context, this information could include the names of the all user's Facebook friends, the user's various Facebook friend groups (and the names of individuals in the group), all public posts,[414] and all group communications to more than ten Facebook friends.[415] The public posts and the group communications to more than ten friends would have no protection because—given the number of recipients—these communications cannot be part of an intimate association.

As far as the names of a user's Facebook friends and the individuals in any created group, these pieces of information can be likened to the non-content portion of an e-mail (e.g., the recipient's name or e-mail address) or the metadata of a phone call (e.g., the number dialed and the person called), none of which is constitutionally protected either under current precedent (*Smith v. Maryland*) or my theory.[416] As previously mentioned, this information does not constitute the substantive part of the relationship.[417] After receiving the above-mentioned information, the government would be free to review the material and decide if wants to acquire any additional constitutionally protected information. For instance, if the government wished to acquire communications from a particular Facebook friend or from a group that was

[413] Slobogin, *Making the Most*, *supra* note 202, at 16-32 (discussing his proposed statute and suggesting that "[r]ules based on duration are easier to understand and abide by").

[414] This could also include any "likes," or other non-targeted information.

[415] Again, reasonable persons may disagree on the exact number here.

[416] *See* Kerr, *Applying*, *supra* note 322, at 1023 ("[T]he outside of packages is not protected by the Fourth Amendment: in the modern lingo, people do not retain a reasonable expectation of privacy in the outside of their packages."); *see also* Smith v. Maryland, 442 U.S. 735, 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business.").

[417] *See supra* Part III.A (distinguishing between the content and non-content portions of communication).

below the threshold, it would have to first get a warrant based on probable cause.[418] This compromise appropriately balances the competing interests of protecting an individual's ability to develop intimate relationships online and the government's ability to conduct investigations.

The warrant and probable cause standard would also not be difficult to administer. The same standard would apply as with searches in physical locations.[419] Consider probable cause, which requires a fair probability that evidence will be found in a specific location.[420] Here, the government, before acquiring communications between the suspect and a social networking friend or group of friends, would have to find that this set of communications (e.g., posts, photographs, or e-mails) likely contains incriminating information. Because the search does not entail surveillance over many locations, there is not any confusion as to where the evidence will be found. The warrant requirement also would be easy to administer. Again, it requires that the police spell out with particularity the place to be searched and the things to be seized.[421] In this context, the government would simply specify what communications they were interested in (naming the individual or group of individuals and the relevant time frame of the communication) and what potentially incriminating communication they would likely find by gathering this information. This could be an incriminating statement or possibly an incriminating photograph. The point here is that, unlike in the surveillance context, there is a specific "place" to search and particular evidence to be identified.

The instant discussion is not intended to be the final say on how to implement my mosaic theory, but it is a good start. The focus here was not on providing a comprehensive plan, but instead on sketching out the basic parameters.[422] The key takeaway should be that courts could establish rules

---

[418] Again, this assumes that probable cause and warrant would be the appropriate requirements under the Fourth Amendment. *See supra* Part II.B.3 (outlining probable cause and warrant requirements necessary before police can conduct surveillance).

[419] *See supra* Part II.B.1-2 (requiring both probable cause, defined as "an articulable belief that a search will more likely than not . . . produce significant evidence of wrongdoing," and a warrant, which "must describe with particularity the person or place targeted . . .").

[420] *See* Illinois v. Gates, 462 U.S. 213, 273 (1983); Warden v. Hayden, 387 U.S. 294, 307 (1967) ("There must, of course, be a nexus . . . between the item to be seized and criminal behavior. Thus in the case of 'mere evidence,' probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction.").

[421] U.S. CONST. amend. IV ("The right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated . . . but upon probable cause . . . particularly describing the place to be searched . . ."); *see supra* Part II.B.3 (establishing that probable cause to search a location requires that police believe that evidence pertaining to the crime will be found in the stated location).

[422] The aim here was using Facebook as the exemplar. I recognize that social networking

that make my mosaic application a viable constraint on law enforcement's ability to acquire information over social networking communications, without discarding or fundamentally changing the current state of the Doctrines.

CONCLUSION

The mosaic theory has perhaps been overdeveloped in the area of government surveillance of public movements. This is not surprising since the factual scenario in *Jones* involved GPS tracking. But it turns out that this theory has a real role to play in protecting social networking communications over the Internet. The Internet is no longer simply a place to transmit information quickly and efficiently. The more it becomes a space for developing and maintaining intimate relationships, the more flexible Fourth Amendment jurisprudence must become. The application of the mosaic theory in this narrow context properly recognizes the value of social networking communications while simultaneously preserving the government's ability to investigate crime.

platforms work slightly differently, but I do not think it would be difficult to come up with overarching principles that would guide what information on the site would be protected and what would not. Based on what I've argued, we could use a combination of specific non-content information (e.g., names) and number of individuals being contacted—common elements in all social networking platforms—in crafting this line.