Boston College Law Review

Volume 54 | Issue 1 Article 2

1-30-2013

Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply

Monu Bedi

DePaul University College of Law, mbedi@depaul.edu

FACEBOOK AND INTERPERSONAL PRIVACY: WHY THE THIRD PARTY DOCTRINE SHOULD NOT APPLY

Monu Bedi*

Abstract: Do communications over social networking sites such as Facebook merit Fourth Amendment protection? The Supreme Court has not directly answered this question and lower courts are not in agreement. The hurdle is the Third Party Doctrine, which states that a person does not have a reasonable expectation of privacy in any communication voluntarily disclosed to a person or entity. All Internet communications are stored on third party servers or Internet service providers, and thus would seemingly lose Fourth Amendment protection. Numerous scholars have weighed in on the issue—analyzing the nature of the communication or the entity to which the information is disclosed—in an effort to show that these communications continue to merit Fourth Amendment protection. These scholars, however, have largely ignored the overall effect of communications over social networking sites such as Facebook. This Article steps outside traditional Fourth Amendment scholarship and relies on the concept of interpersonal privacy rights as a way to protect communications over social networking platforms. Because social scientists have recognized that these relationships share the same qualitative structure and can be just as "real" as their face-to-face counterparts, this Article makes the argument that the concept of interpersonal privacy should apply to social networking relationships over the Internet. This analysis provides a new way to apply the reasonable expectation of privacy test under the Fourth Amendment—one that avoids the common pitfalls associated with the Third Party Doctrine.

Introduction

Fourth Amendment protection has proven difficult to apply in the Internet context. The Fourth Amendment of the U.S. Constitution

 I would like to thank the participants of the DePaul Law Junior Faculty Workshop and DePaul Law Faculty Seminar series for their feedback. I would like to specifically thank Susan Bandes, Joshua Dressler, Jamie Fox, Orin Kerr, Joshua Sarnoff, Katherine Strandburg, Deborah Turkeimer, and Lou Virelli for their comments on earlier drafts. Finally, I would like to thank the editors of the Boston College Law Review, and in particular Claire Specht, for their excellent editing.

protects "against unreasonable searches and seizures."[1] The basic problem stems from the fact that almost all communications over the Internet—including messages over such sites as Facebook, Gmail, and Hotmail—are stored for various lengths of time on third party servers or Internet service providers ("ISPs").[2] These are proprietary systems owned by the respective provider (e.g., Facebook, Gmail) that house the information so that it can be delivered to its destination.[3] The question for scholars has been whether these communications continue to merit privacy protection, despite this disclosure to a third party.[4] This Article relies on the concept of interpersonal privacy to show that these communications continue to merit Fourth Amendment protection despite their disclosure.

The connection between disclosure and privacy has its roots in U.S. Supreme Court precedent from the middle of the twentieth century, well before the arrival of the Internet.[5] The basic premise has not changed. Dubbed the Third Party Doctrine, it states that a person loses Fourth Amendment protection—i.e., does not have a reasonable expectation of privacy—to any communications that the person voluntary discloses to another.[6] This information can be obtained without a warrant supported by probable cause and can be used against the individual at trial.[7] The paradigmatic case—and where the doctrine was initially applied—deals with government agents.[8] A person loses protection to any communication disclosed to an agent, even if the agent was undercover and the agent's intentions were unknown to the individual.[9] It is only relevant that the individual willingly made the communication to the informant.[10]

In 1979, in *Smith v. Maryland*, the Supreme Court extended this doctrine to include information voluntarily disclosed to automated ma-

---

[1] U.S. Const. amend. IV.

[2] *See infra* notes 114–129 and accompanying text.

[3] *See infra* notes 114–129 and accompanying text.

[4] *See infra* notes 130–209 and accompanying text.

[5] *See* Hoffa v. United States, 385 U.S. 293, 302–03 (1966); Lewis v. United States, 385 U.S. 206, 210–12 (1966); Lopez v. United States, 373 U.S. 427, 438–39 (1963); On Lee v. United States, 343 U.S. 747, 753–54 (1952).

[6] United States v. Miller, 425 U.S. 435, 443 (1976) (stating that an individual does not have a Fourth Amendment privacy interest in information that is conveyed to a third party and later conveyed by that third party to the government); United States v. White, 401 U.S. 745, 750–52 (1971).

[7] *Miller*, 425 U.S. at 443; *see infra* note 53.

[8] *See infra* notes 76–89 and accompanying text.

[9] *See Miller*, 425 U.S. at 443; *White*, 401 U.S. at 750–52; *Hoffa*, 385 U.S. at 300–03.

[10] *See Miller*, 425 U.S. at 443; *infra* notes 76–89 and accompanying text.

chines.[11] A thirty-year old opinion, *Smith* remains the reigning precedent to explain communications transmitted over the Internet.[12] Because Internet communications are also voluntarily disclosed to machines in the form of ISPs, arguably under *Smith* users appear to lose any Fourth Amendment protection in these communications.[13] The government would therefore be constitutionally free to acquire these communications from the third-party service provider without first obtaining a warrant, and to use the information against a person at trial.[14]

Despite *Smith*'s implication that the Third Party Doctrine extends to Internet communications, the Supreme Court has not directly ruled on this issue and lower courts have disagreed on how to interpret the Third Party Doctrine in the Internet context.[15] In 2012, the Court issued its most recent decision on technology and the Fourth Amendment, *United States v. Jones*, in which it held that placing a Global Positioning Satellite ("GPS") tracker on a defendant's car without a warrant violated the Fourth Amendment.[16] Yet this decision did not settle the issue. The justices concurring in *Jones* raised meaningful concerns about the viability of the Third Party Doctrine in today's technology-dominated world.[17]

This issue is particularly important because so many individuals across the world now use social networking sites, including Myspace,

---

[11] Smith v. Maryland, 442 U.S. 735, 744–46 (1979); *see infra* notes 90–106 and accompanying text.

[12] *See Smith*, 442 U.S. at 741–46.

[13] *See infra* notes 114–129 and accompanying text.

[14] The third party server may have its own rules (as Facebook does) that could curtail the government from freely acquiring the information, or Congress could pass legislation protecting these communications, though these barriers would not be constitutionally mandated. *See infra* notes 210–262 and accompanying text.

[15] *See, e.g.*, *Smith*, 442 U.S. at 745–46; United States v. Warshak, 631 F.3d 266, 287–88 (6th Cir. 2010) (holding that under certain circumstances, an ISP's control over and access to e-mails will not be sufficient to overcome a user's expectation of privacy in those e-mails); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904–06 (9th Cir. 2008) (holding that users of text messaging services have a reasonable expectation of privacy in those text messages), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010); United States v. Forrester, 512 F.3d 500, 509–11 (9th Cir. 2008) (holding that computer surveillance that captured the "to" and "from" addresses of e-mails, the IP addresses of websites an individual visited, and the total amount of data that was transmitted to and from that account did not constitute a Fourth Amendment search); United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000) (holding that a person does not have a privacy interest in the account information conveyed to an ISP); *infra* notes 130–209 and accompanying text.

[16] *See* United States v. Jones, 132 S. Ct. 945, 949–54 (2012).

[17] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); *id.* at 962–63 (Alito, J., concurring); *infra* notes 263–283 and accompanying text.

Facebook, and Google+.[18] These types of platforms have revolutionized how people communicate and develop relationships.[19] Users on such sites have the ability to send messages, post status updates, post pictures, and video conference, among other things.[20] Although many social networking users believe that their communications will remain privately held by the ISP and free from government intrusion, under the Third Party Doctrine, all of these communications seem to lose Fourth Amendment protection because users voluntarily disclose this information to ISPs.[21]

Scholars have taken wide and varied approaches to this disclosure problem in the Internet context.[22] Some have focused on the nature of the Internet entity to whom the disclosure is made,[23] whereas others have focused on distinguishing the type of information disclosed.[24] Still others have argued that disclosure to ISPs is qualitatively different from disclosure to government agents.[25] The common thread among most of these theories is that they confine themselves to analyzing the discrete transmission itself in an attempt to extend Fourth Amendment protection.[26]

Few scholars, however, have introduced interpersonal privacy into a discussion of the Fourth Amendment.[27] These discussions have typi-

---

[18] *See, e.g.*, Vic Gundotra, *Welcome Nik Software!*, Google+ (Sept. 17, 2012, 11:34 AM), https://plus.google.com/+VicGundotra/posts/2YWhK1K3FA5 (noting that Google+ has over four billion users and one million active monthly users); *Key Facts*, Facebook, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (last visited Dec. 22, 2012) (noting that Facebook had one billion monthly users as of October 2012).

[19] *See infra* notes 382–423 and accompanying text.

[20] *See infra* notes 382–423 and accompanying text.

[21] *See infra* notes 114–129 and accompanying text.

[22] *See infra* notes 130–209 and accompanying text.

[23] *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581, 611–19 (2011) (arguing that Internet communications that are not viewed by a human observer remain private for purposes of the Fourth Amendment).

[24] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1017–31 (2010) (arguing that the content/non-content distinction should be applied to Internet communications); Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105, 2162–63 (2009) (arguing that courts could limit the Third Party Doctrine reasoning in *Smith* by applying it only to non-content information); *see also infra* notes 165–181 and accompanying text (discussing the content/non-content distinction).

[25] *See* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 Md. L. Rev. 614, 654–64 (2011) (arguing that social networking sites have become akin to an extension of the home and, therefore, that the Third Party Doctrine should not be applied as strictly in this context).

[26] *See* Kerr, *supra* note 24, at 1017–31; Strandburg, *supra* note 25, at 654–64; Tokson, *supra* note 23, at 611–19; Tokson, *supra* note 24, at 2162–63.

[27] *See infra* notes 337–375 and accompanying text.

cally been confined to general arguments about the inherent tension between this type of privacy and Fourth Amendment rights.[28] No scholar appears to have specifically linked interpersonal privacy to social networking communications over sites like Facebook.

Given Facebook's popularity, this Article will focus on Facebook and its related functions and policies as the exemplar of this type of social networking. But no one can predict the future, and there could be other social networking platforms that further change how people interact on the Internet. The arguments in this Article regarding Fourth Amendment protection for Internet communications would apply with equal force not only to current social networking platforms but also to any future ones.[29] At its core, this Article grapples with general issues of relationship formation on the Internet and related privacy protection.

This Article uses the concept of interpersonal privacy to examine how to extend Fourth Amendment protection to Facebook communications.[30] The term "interpersonal privacy" is used broadly and encompasses the Court's protection of relationships and the expressive autonomy associated with them. Interpersonal privacy has a history separate and apart from the privacy associated with the Fourth Amendment.[31] It focuses on interpersonal relationships and the accompanying issues of identity and autonomy, and is grounded in the Due Process, Equal Protection, and First Amendment Clauses of the Constitution.[32]

---

[28] Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. Rev. 1, 9 (2010) (stating that the conceptions of "privacy" under interpersonal privacy and under the Fourth Amendment are not always the same); Jonathan W. Penney, *Privacy and New Virtualism*, 10 Yale J.L. & Tech. 194, 240 (2008) (noting that there is a distinction between personal privacy and informational privacy).

[29] In fact, as social networking on the Internet becomes more prevalent and the platforms used more multifaceted, the theory proposed in this Article will apply with even greater force.

[30] *See infra* notes 376–488 and accompanying text.

[31] *See* Crocker, *supra* note 28, at 9. *Compare* Lawrence v. Texas, 539 U.S. 558, 578–79 (2003) (invalidating a state's sodomy law as a violation of privacy under the Due Process Clause of the Fourteenth Amendment), *and* Griswold v. Connecticut, 381 U.S. 479, 481, 485–86 (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), *with* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (articulating the two-part reasonable expectation of privacy test to determine whether the Fourth Amendment has been violated), *and On Lee*, 343 U.S. at 753–54 (holding that the defendant's communications with another at trial that were overheard by an undercover agent did not violate the Fourth Amendment).

[32] Scholars have used the terms "decisional interference" or "right of autonomy" to discuss the due process/equal protection line of cases. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 557–59 (2006); *infra* notes 288–303 and accompanying text. The term "interpersonal privacy" as used in this Article encompasses this type of autonomy

The Supreme Court's 2003 decision in *Lawrence v. Texas* stands as one of the seminal expressions of this privacy right.[33] In *Lawrence*, the Court overturned a government prohibition against sodomy, reasoning that this government intrusion endemically interfered with an individual's right to define his or her relationships.[34] Other interpersonal privacy cases invoking First Amendment and equal protection principles further entrenched this right as one protecting essential qualities of relationships.[35]

This Article interprets these cases, collectively and broadly, and argues that interpersonal privacy applies to Facebook relationships and their constituent communications. Social scientists and psychologists alike have recognized that Facebook relationships can have the same qualitative structure as traditional face-to-face relationships.[36] Both types of relationships can share similar depth, breadth, and quality.[37] If the Court values the interpersonal bonds that arise from traditional relationships and seeks to protect how individuals can define such relationships, it stands to reason that relationships formed through social networking sites such as Facebook should also be valued when applying the Fourth Amendment.[38]

The argument makes two key moves. First, relying on the concept of interpersonal privacy, this Article argues that communications that are constituent of Facebook relationships are deserving of some special consideration when applying the Fourth Amendment reasonable expectation test.[39] Second, disclosure to the ISP—which is absent from traditional face-to-face relationships—should not vitiate privacy protec-

---

but also includes the rights of expressive associations grounded in First Amendment principles. *See infra* notes 289–336 and accompanying text.

[33] *See Lawrence*, 539 U.S. at 578–79.

[34] *See id.*

[35] *See* Boy Scouts of Am. v. Dale, 530 U.S. 640, 659 (2000); Roberts v. U.S. Jaycees, 468 U.S. 609, 617–29 (1984); *infra* notes 305–336 and accompanying text.

[36] *See infra* notes 382–423 and accompanying text.

[37] *See* John A. Bargh & Katelyn Y.A. McKenna, *The Internet and Social Life*, 55 Ann. Rev. Psychol. 573, 586–87 (2004).

[38] *See infra* notes 376–488 and accompanying text. This Article does not argue that Facebook relationships actually merit substantive due process or First Amendment protection. This would mute any discussion of Fourth Amendment protection because another constitutional principle—such as substantive due process—could be invoked to protect these communications from government intrusion. The arguments in this Article could be applied toward such a conclusion, but this is not my aim. Here, the invocation of interpersonal privacy is more appropriately described as a conceptual and instructive tool that supports Fourth Amendment protection under the reasonable expectation of privacy test.

[39] *See infra* notes 376–488 and accompanying text.

tion because this entity serves no part in the relationship.[40] The aim of the proposal is not to elevate Facebook relationships over their traditional face-to-face counterparts. Quite the contrary, the point is only to put Facebook relationships on equal footing with face-to-face relationships in terms of privacy protection. Facebook relationships should bear the same risks and burdens as traditional relationships when it comes to government intrusion.

To be clear, relationships on social networking sites like Facebook cannot fully be analogized to the traditional, private face-to-face relationships found in cases such as *Lawrence*. There are material differences. For instance, relationships on Facebook can involve a large group of individuals who may all have access to significant amounts of personal information. The relationships also do not take place in a private physical space, such as an individual's home. But privacy cases like *Lawrence*—similar to Fourth Amendment cases like *Smith*—never envisioned the sociological implications of Internet networking sites such as Facebook. These interpersonal privacy concepts—at least in the context of applying the Fourth Amendment—are thus ripe for updating in light of today's technology-based world.

In modern times, communications on social networking sites, taken together, are more than the sum of their parts. Unlike traditional communications (e.g., phone, letter), these transmissions do not merely facilitate a face-to-face relationship but rather are constituent of the relationship. Indeed, for many users—particularly younger individuals—Facebook has replaced the need for physical interactions as a means to develop and sustain relationships.[41] Invoking the concept of interpersonal privacy when discussing online relationships ultimately provides a new way to apply Fourth Amendment protection and the reasonable expectation of privacy test—one that protects Facebook relationships to the same degree as traditional relationships.

The Article consists of four parts. Part I traces the history of the Third Party Doctrine and its basic application to Fourth Amendment protection.[42] Part II discusses how this doctrine applies in the Internet context, and particularly to social networking sites like Facebook.[43] In addition, this Part examines the legislative reactions to Internet privacy as well as scholarly arguments on how best to apply the Fourth Amend-

---

[40] *See infra* notes 452–462 and accompanying text.
[41] *See infra* notes 382–423 and accompanying text.
[42] *See infra* notes 49–106 and accompanying text.
[43] *See infra* notes 107–283 and accompanying text.

ment to Internet communications.[44] It also discusses *United States v. Jones*, the Court's most recent case on technology and privacy.[45] Part III summarizes the history of the Supreme Court's interpersonal privacy doctrine and how courts and scholars have understood this doctrine as one that protects interpersonal relationships more broadly.[46] Finally, Part IV explains why this concept of privacy should apply to Facebook (and similar) communications and what sets these communications apart from other Internet transmissions.[47] It goes on to reevaluate the Fourth Amendment's reasonable expectation of privacy using the concept of interpersonal privacy, and concludes by providing a real-world application of the theory.[48]

I. Fourth Amendment and the Third Party Doctrine

This Part examines the history of the Third Party Doctrine and how it applies to Fourth Amendment protection.[49] Section A discusses the change in Fourth Amendment protection from spatial privacy to the reasonable expectation of privacy test and the emergence of the Third Party Doctrine.[50] Section B examines how the Supreme Court has applied the Third Party Doctrine to conversations and personal documents and records.[51] Finally, Section C summarizes the Supreme Court's decision in *Smith v. Maryland* in which the Court extended the Third Party Doctrine to disclosures made to third party machines.[52]

A. *Spatial Privacy and* Katz v. United States

Historically, the Fourth Amendment only protected private citizens from unwarranted government intrusion into their physical property.[53] Any such intrusion necessitated a warrant based on probable cause, issued by a magistrate.[54] Scholars have dubbed this type of privacy "spa-

---

[44] *See infra* notes 130–209, 230–262 and accompanying text.
[45] *See infra* notes 263–283 and accompanying text.
[46] *See infra* notes 284–375 and accompanying text.
[47] *See infra* notes 382–470 and accompanying text.
[48] *See infra* notes 471–488 and accompanying text.
[49] *See infra* notes 53–106 and accompanying text.
[50] *See infra* notes 53–75 and accompanying text.
[51] *See infra* notes 76–89 and accompanying text.
[52] *See infra* notes 90–106 and accompanying text.
[53] *See* Olmstead v. United States, 277 U.S. 438, 465–66 (1928).
[54] U.S. Const. amend. IV; United States v. Ventresca, 380 U.S. 102, 105–07 (1965). The Fourth Amendment of the U.S. Constitution provides that "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, sup-

tial privacy."[55] This conception of privacy was principally articulated in 1928 in *Olmstead v. United States*, in which the Supreme Court held that Fourth Amendment protection applied only to a person's property.[56] In this case, the government, without a warrant, tapped Olmstead's phone lines by making physical intrusions into sections of the phone lines that were not on Olmstead's property.[57] The Court held that the government was free to intercept and record these conversations without first seeking a warrant because it did not trespass on Olmstead's property.[58]

Olmstead led the way for other decisions relating to face-to-face conversations with government agents.[59] Under those decisions, as long as agents did not trespass on a person's property, individuals did not have Fourth Amendment protection in what they disclosed to an undercover informant, irrespective of the individual's belief that the informant would not disclose the information.[60] Any such information could be gathered without a warrant and subsequently used against the person at trial.[61] As the Court articulated, "a wrongdoer's misplaced belief that a person to whom he voluntary confides his wrongdoing will

---

ported 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 (e.g., automobile exception, exigency), but invocation of any such exception assumes that Fourth Amendment protection would otherwise apply. *See Ventresca*, 380 U.S. at 106–07. 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); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 507–08 (2007).

[55] *See* Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 284–87 (2003); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1022 (1998). Implicit in this notion of privacy would be the protection of personal "papers" that may contain private information. *See* DeVries, *supra*, at 288; *infra* notes 76–89 and accompanying text. The idea of personal information as physically separable from "the information's subject" is a slightly different concept and took longer to develop. DeVries, *supra*, at 288. This type of "informational privacy" is not the subject of this Article and is more appropriately governed by federal statutes, such as the Privacy Act of 1974. *See* 5 U.S.C.A. § 552a (2012).

[56] *Olmstead*, 277 U.S. at 464–65.

[57] *Id.* at 456–57.

[58] *Id.* at 464–66.

[59] *See Hoffa*, 385 U.S. at 302–03; *Lewis*, 385 U.S. at 210–11; *Lopez*, 373 U.S. at 438–39; *On Lee*, 343 U.S. at 751–55.

[60] *See, e.g.*, *Hoffa*, 385 U.S. at 302–03; *Lewis*, 385 U.S. at 210–11. Using deceit to enter a defendant's property does not constitute a trespass and therefore any information disclosed to the government agent upon entry would not violate the Fourth Amendment. *E.g.*, *Lewis*, 385 U.S. at 209–10; *On Lee*, 343 U.S. at 752–53.

[61] *Lopez*, 373 U.S. at 438–40.

not reveal it" receives no protection under the Fourth Amendment.[62] This became known as the "Third Party Doctrine," which states that the Fourth Amendment does not protect information a person voluntarily discloses to a third party, even if the government later acquires the information from the third party.[63]

In 1967, the Supreme Court dramatically reconceptualized Fourth Amendment analysis in *Katz v. United States*.[64] The Court no longer restricted Fourth Amendment protection to a person's property or physical space; rather, the Court applied Fourth Amendment protection more broadly to any situation in which an individual had a reasonable expectation of privacy.[65] As the Court famously observed, the Fourth Amendment "protects people, not places."[66]

In *Katz*, the defendant was making illegal gambling bets from a phone booth that, unbeknownst to him, the government was monitoring, without a warrant, using a device attached to the outside of the booth.[67] The Court held that such recordings violated the defendant's Fourth Amendment right to privacy.[68] In a concurrence supporting this holding, Justice John Marshall Harlan II articulated the now well-known two-part test for when Fourth Amendment protection applies: a person must have a subjective expectation of privacy in the communication and the expectation must be objectively reasonable.[69] Even though the government agents did not trespass on the defendant's property, the context in which the communication was made and the defendant's actions suggested that Fourth Amendment protection was appropriate.[70] The defendant "occupie[d] [the telephone booth], shut the door behind him, and pa[id] the toll that permits him to place a call."[71] Therefore, the Court reasoned, the defendant subjectively believed that his conver-

---

[62] *Hoffa*, 385 U.S. at 414; *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, 330–32 (2011) (discussing the misplaced trust doctrine and how that does not curtail application of the Third Party Doctrine).

[63] *White*, 401 U.S. at 749; Tokson, *supra* note 23, at 583–85 (discussing the history of the Third Party Doctrine).

[64] *See Katz*, 389 U.S. at 353.

[65] *See id.* at 353; *see also id.* at 361 (Harlan, J., concurring) (articulating the two-part expectation of privacy test).

[66] *Id.* at 351 (majority opinion).

[67] *See id.* at 348, 352–53, 354 n.14, 356.

[68] *See id.* at 359.

[69] *Id.* at 361 (Harlan, J., concurring).

[70] *See Katz*, 398 U.S. at 352.

[71] *Id.* at 352.

sation was private and this belief was objectively reasonable.[72] Accordingly, the government was required to obtain a warrant before intercepting the call.[73]

Although *Katz* expanded the conception of Fourth Amendment protection, it did not raise the Third Party Doctrine.[74] The Court did not address its applicability because the defendant did not knowingly make his call in the presence of government agents.[75]

B. *Early Development of the Third Party Doctrine*

Shortly after *Katz*, in 1971, in *United States v. White*, the Supreme Court explicitly made clear that the Third Party Doctrine survived the new expectation of privacy test.[76] In *White*, a government informant used a radio transmitter to surreptitiously transmit conversations with the defendant at various locations, including the defendant's home.[77] The Court found no Fourth Amendment violation in using these conversations at trial because the defendant voluntarily disclosed the information to a third party, which vitiated any reasonable expectation of privacy.[78]

In 1976, in *United States v. Miller*, the Court extended the Third Party Doctrine beyond conversations to include personal documents and records conveyed to third parties.[79] In *Miller*, by voluntarily disclosing records to a bank, the defendant lost any claim of Fourth Amendment protection as to those documents.[80] The Court stated that it did not matter that the defendant disclosed these records to the bank for a limited purpose, such as financial security.[81] His misplaced *subjective* belief or trust did not change the fact that once he conveyed the information, he took the risk that the government may obtain it from the

---

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

[73] *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).

[74] *See generally Katz*, 398 U.S. 347 (failing to discuss the Third Party Doctrine).

[75] *See id.* at 352.

[76] *White*, 401 U.S. at 750.

[77] *Id.* at 746–47.

[78] *Id.* at 751–52.

[79] *See Miller*, 425 U.S. at 442–43.

[80] *Id.*

[81] *See id.* at 443. It does not matter if the individual revealed the information "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." *Id.*

bank.[82] Thus, the Court held that the defendant could not object to the government's warrantless seizure of these documents.[83]

Given the Court's opinion in *Miller*, some scholars have treated the Third Party Doctrine as a doctrine of consent or waiver.[84] Understood in this way, a person "consents" or "waives" his or her right to Fourth Amendment protection over the communication when he or she discloses it to a third party.[85] It is not relevant that the individual releases the information for a limited purpose or with limited knowledge—the voluntary nature of the disclosure vitiates all privacy protection for the communication.[86]

This loss of protection also applies to information exposed to the public at large.[87] The Court, for instance, has ruled that a driver does not have a reasonable expectation of privacy in his or her movements through public streets.[88] The voluntary act of driving in public suggests the driver has consented to his or her subsequent movements being monitored without any Fourth Amendment protection.[89]

C. *The Third Party Doctrine and Technology: The Automation Rationale*

The 1979 Supreme Court decision, *Smith v. Maryland*, applied the Third Party Doctrine to technological advancements.[90] In *Smith*, the government requested that the phone company set up a "pen register," a device intended to record all outgoing phone numbers dialed by the defendant from his home.[91] The device was installed at the phone

---

[82] *Id.*

[83] *Id.* at 440–43.

[84] *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 588–90 (2009); Sonia K. McNeil, *Privacy and the Modern Grid*, 25 Harv. J.L. & Tech. 199, 216–18 (2011).

[85] *See, e.g.*, Kerr, *supra* note 84, 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 84, at 216–18 (discussing and ultimately disagreeing with the argument that the Third Party Doctrine should be interpreted as a doctrine of consent).

[86] *See* Kerr, *supra* note 84, 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).

[87] *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281–82 (1983); United States v. Cowan, 674 F.3d 974, 955–56 (8th Cir. 2012).

[88] *Knotts*, 460 U.S. at 281–82; *see infra* notes 263–283 and accompanying text.

[89] *See Knotts*, 460 U.S. at 281–82.

[90] 442 U.S. at 744–46.

[91] *Id.* at 737. This device records the numbers dialed by monitoring the impulses caused when the dial on the telephone is released. *Id.* at 736 n.1. The device does not record the conversations that take place after a call has been made. *Id.*

company's offices; at no point did the government enter the defendant's property.[92]

The Court upheld the warrantless use of the pen register, stating that the Fourth Amendment did not protect the numbers dialed by the telephone user.[93] Applying the two-part *Katz* test, the Court held that the defendant did not have a subjective expectation of privacy in the dialed numbers, nor would any such expectation be reasonable.[94] Telephone users realize that they must convey the number to the telephone company in order to make a call and that the company has facilities for making permanent records of the numbers dialed.[95]

Further, and more importantly, the Court held that any subjective expectation of privacy (assuming one existed) was not something society would find reasonable.[96] Citing *Miller*, the Court concluded that the defendant did not satisfy the second element of the *Katz* test because he did not have a reasonable expectation of privacy in the dialed numbers.[97] 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."[98] Accordingly, the defendant waived any right to privacy protection.[99]

Because the individual voluntarily disclosed the information to a third person, the information was no longer secret, and the government could obtain the information without violating the Fourth Amendment.[100] The fact that the number was disclosed to an automated machine instead of a human being was of no consequence:

> 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 re-

---

[92] *Id.* at 741.
[93] *Id.* at 745–46.
[94] *Id.* at 741–46.
[95] *Id.* at 742.
[96] *Smith*, 442 U.S. at 743.
[97] *Id.* at 743–44.
[98] *Id.* at 744.
[99] *See id.*
[100] *Id.* at 743–46; Tokson, *supra* note 23, at 609.

> sult is required because the telephone company has decided to automate.[101]

This point is critical to the holding in *Smith*.[102] The Court did not address whether a human being actually observed the number being dialed.[103] This apparently was not relevant.[104] All that mattered was that the defendant voluntarily exposed the number to a third party's machine—in this case, the telephone company's switching equipment.[105] The implication here is that an individual will likely lose Fourth Amendment protection as to any information he or she exposes to a third party's machine in the normal course of business, regardless of whether a human actually observes the information.[106]

II. Facebook and the Third Party Doctrine

How courts should apply the Third Party Doctrine in the Internet context has proven difficult to determine.[107] This Part examines the applicability of the Third Party Doctrine to the Internet context, using Facebook as an example.[108] Section A examines the strict application of the Third Party Doctrine to social networking communications.[109] Section B then discusses the various approaches taken by lower courts and scholars in applying the Third Party Doctrine to Internet communications and information.[110] Section C summarizes Facebook's privacy policies and evaluates how such policies would intersect with the Third Party Doctrine.[111] Section D then examines how certain provisions of the Electronic Communications Privacy Act would apply to social networking communications.[112] Last, Section E analyzes the U.S. Supreme Court's 2012 decision, *United States v. Jones*, which held that installing a GPS tracking device in an individual's car without a warrant violated the Fourth Amendment.[113]

---

[101] *Smith*, 442 U.S. 744–45 (citation omitted).
[102] *See id.*
[103] *See id.*
[104] *See id.*; Tokson, *supra* note 23, at 600.
[105] *See Smith*, 442 U.S. at 744–45; Tokson, *supra* note 23, at 600.
[106] Tokson, *supra* note 23, at 600; *see Smith*, 442 U.S. at 744–45.
[107] *See infra* notes 114–283 and accompanying text.
[108] *See infra* notes 114–283 and accompanying text.
[109] *See infra* notes 114–127 and accompanying text.
[110] *See infra* notes 130–209 and accompanying text.
[111] *See infra* notes 210–229 and accompanying text.
[112] *See infra* notes 230–262 and accompanying text.
[113] *See infra* notes 263–283 and accompanying text.

A. *Storage on the Internet and Third Party Disclosure*

The Third Party Doctrine has proven difficult to apply in the Internet context.[114] Nearly all online data is stored somewhere in third-party servers or ISPs.[115] These servers and ISPs consist of proprietary systems where information is stored so that it can be delivered to its desired location.[116] Commonly used e-mail systems like Gmail, Hotmail, and Yahoo utilize these third-party servers and ISPs.[117]

Facebook and other social networking sites work in the same way.[118] Facebook provides a social networking space that allows users to create individual profiles with pictures and other personal information and to communicate with other users using a host of various interactive tools, including posting status updates or photographs, sending and receiving e-mails or instant messages, and video-conferencing.[119] Almost all of this information is stored (for various lengths of time) in private facilities or ISPs owned by Facebook.[120] Under a strict applica-

---

[114] *See* Tokson, *supra* note 23, at 584; *infra* notes 130–209 and accompanying text.

[115] Tokson, *supra* note 23, at 585, 602–03; *see* Preston Gralla, How the Internet Works 88–99 (8th ed. 2004) (describing how e-mails are transmitted and stored).

[116] Gralla, *supra* note 115, at 88–99; Tokson, *supra* note 23, at 602–03.

[117] *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) (describing how e-mails are routed by equipment owned by the ISP that processes their data); Tokson, *supra* note 23, at 602–03 (describing how e-mail service providers, such as Gmail and Hotmail, store e-mail data); *Privacy Policy*, Google, http://www.google.com/intl/en/policies/privacy/ (last updated July 27, 2012) (explaining that Gmail scans text of e-mails in order to file spam and detect viruses). Even deleted e-mail is 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 (PLI Intellectual Prop., Course Handbook Ser. No. G-865, 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."); Deirdre K. Mulligan et al., *Risks of Online Storage*, Comm. ACM, Aug. 2006, at 112, 112 ("Often, 'deleted' email will remain on backup storage unbeknownst to users.").

[118] *See infra* notes 119–120 and accompanying text.

[119] *See* Jonathan Strickland, *How Facebook Works*, How Stuff Works, http://computer.howstuffworks.com/internet/social-networking/networks/facebook1.htm (last visited Dec. 22, 2012) (describing the features of Facebook and various tools available to users); *Pages Basics*, Facebook, https://www.facebook.com/help/387958507939236/ (last visited Dec. 22, 2012); *Video Calling: Basics & Privacy*, Facebook, https://www.facebook.com/help/439078162792430/ (last visited Dec. 22, 2012). Google's networking platform (Google+) allows for similar types of communications. *See New Ways of Sharing, Across All of Google*, Google+, http://www.google.com/+/learnmore/ (last visited Dec. 22, 2012); *see also infra* notes 382–423 and accompanying text (discussing these features of Facebook and how they foster relationships).

[120] *See* 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 internet

tion of the Third Party Doctrine under *Smith*, a Facebook user would lose Fourth Amendment protection for *any* communication or information transmitted or posted through the social networking site because the user has knowingly disclosed it to a third party's storage system.[121]

Under a waiver theory, a Facebook user consents to revealing this information to the ISP and thus seemingly forfeits any protection over

---

service providers (ISP), 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. *See* 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/ [hereinafter Miller, *Facebook Makes Big Investment*]; Rich Miller, *$20 Million a Year on Data Centers*, Data Center Knowledge (May 18, 2009), http://www.datacenterknowledge.com/archives/2009/05/18/facebook-20-million-a-year-on-data-centers/; Adam Ostrow, *How Facebook Serves Up Its 15 Billion Photos*, Mashable Social Media (Apr. 30, 2009), http://mashable.com/2009/04/30/facebook-photo-sharing (discussing how Facebook stores uploaded photographs). Indeed, Facebook acknowledges that it may share information in response to a legal request if the site has a good faith basis to believe that the law requires it. *Data Use Policy: Some Other Things You Need to Know*, Facebook, https://www.facebook.com/full_data_use_policy (last revised Dec. 11, 2012); *see infra* notes 210–229 and accompanying text (discussing Facebook's privacy policies in further detail). Even deleted Facebook accounts may remain on servers for up to ninety days after a user deletes the account. *See Data Use Policy: Deleting and Deactivating Your Account*, *supra*; *Statement of Rights and Responsibilities: Sharing Your Content and Information*, Facebook, https://www.facebook.com/legal/terms (last revised Dec. 11, 2012). Yet, it appears that the video chatting content is not stored in any way. *Video Calling: Basics & Privacy*, *supra* note 119 (noting that the calls themselves are not stored).

[121] *See* Semitsu, *supra* note 62, at 329 (arguing that a Facebook user does not have Fourth Amendment protection over the majority, if not all, of the content posted on Facebook "since it is information that a Facebook user voluntarily agrees to have held in third party storage"); Strandburg, *supra* note 25, 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"). It is important to note that all Facebook users agree to terms stating that the company will hold their information. *Statement of Rights and Responsibilities*, *supra* note 120 ("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."); *see infra* notes 210–229 and accompanying text. 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 v. Maryland, 442 U.S. 735, 744 (1979) (noting only that the information was voluntarily disclosed, not the length of time that the information had been disclosed); United States v. Miller, 425 U.S. 435, 443 (1976) (same). This loss of Fourth Amendment protection is conceptually different from the situation where a Facebook user makes his or her profile publicly viewable. Semitsu, *supra* note 62, at 342–44. Here, there is no reasonable expectation of privacy because the evidence is in "plain view." *Id.*

the transmission.[122] The user made a voluntary choice to sign an agreement before opening an account, acknowledging that Facebook will hold the user's communications.[123] Thus, there would be no constitutional barrier to the government acquiring this information from the ISP without a warrant.[124] It would not matter if the individual user *subjectively* expected the communication to remain privately held, and not reviewed by the ISP or otherwise disclosed to the government.[125] 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 oneself at trial.[126] It is not relevant that the person may not have all the facts before making this disclosure or does not otherwise recognize the true identity of the informant.[127] What matters is that the person willingly disclosed the information.[128] This act, on its own, vitiates any Fourth Amendment privacy protection. The same reasoning applies to information relayed to an ISP. Under *Katz v. United States* and its progeny, even though subjective expectations may be relevant, a normative judgment as to whether the expectation is "objectively reasonable" remains the dispositive factor.[129]

B. *Responses to the Third Party Doctrine and Internet Privacy*

The Supreme Court has yet to decide how the Third Party Doctrine will impact communications on the Internet, specifically those transmit-

---

[122] *See* Kerr, *supra* note 84, at 588–90; *Statement of Rights and Responsibilities*, *supra* note 120 (describing Facebook's terms of usage and incorporating the Data Use Policy); *see also supra* notes 84–86 and accompanying text (discussing the waiver theory of the Third Party Doctrine).

[123] *See supra* note 121 and accompanying text; *infra* notes 210–229 and accompanying text.

[124] *See Miller*, 425 U.S. at 443.

[125] *See id.* at 443; United States v. White, 401 U.S. 745, 751–52 (1971). 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 23, at 622–26.

[126] *See Miller*, 425 U.S. at 443; *White*, 401 U.S. at 751–52.

[127] *See Miller*, 425 U.S. at 443; *White*, 401 U.S. at 751–52; Kerr, *supra* note 84, at 588–89.

[128] *See Miller*, 425 U.S. at 443; Kerr, *supra* note 84, at 588–89.

[129] *Smith*, 442 U.S. at 740 & n.5, 743–44 (discussing the two-part test under *Katz* and noting that even if the defendant had a subjective expectation of privacy, it was not objectively reasonable); Tokson, *supra* note 24, at 2162 ("The Court has stated in several cases that a normative judgment under the 'objectively reasonable' prong of *Katz* is generally the most important determinant of Fourth Amendment protection, and trumps any contrary conclusion based on subjective expectations of privacy.").

ted through social networking sites.[130] Scholars and lower courts are not in agreement as to how this doctrine should apply in today's technological context, or whether it should apply at all.[131] Some appellate courts have adopted the Third Party Doctrine when applying the Fourth Amendment to Internet communications,[132] whereas others have focused on distinguishing between types of information contained in the communication.[133]

The Third Party Doctrine has also generated significant, and sometimes strident, reactions by Fourth Amendment scholars as to its application to the Internet.[134] These individuals have suggested a variety of solutions, including greater positive laws protecting Internet communications, complete reconceptualizations of how the Fourth Amendment should work in the Internet context,[135] and outright elimination of the doctrine.[136]

This Article does not seek to provide a comprehensive analysis of Fourth Amendment doctrine as applied to the Internet. Indeed, this type of undertaking would require significant discussion of the preceding scholarship, much of which is not pertinent here. The important

---

[130] Some scholars argue that the doctrine is unlikely to be overturned. *See, e.g.*, Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 Harv. C.R.-C.L. L. Rev. 435, 460 (2008); Tokson, *supra* note 23, at 586.

[131] *See infra* notes 139–209 and accompanying text.

[132] *See infra* notes 139–164 and accompanying text.

[133] *See infra* notes 165–181 and accompanying text.

[134] DeVries, *supra* note 55, at 309–10 (noting that there is agreement among privacy scholars that privacy law must change in the digital age, but that various approaches have been proposed).

[135] *See, e.g.*, Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 151–64 (2007) (discussing subpoenas to third parties and the rationale for requiring those entities to disclose to the government); Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 20–21 (2008) (arguing that legislative action should be taken); Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1426–27 (2004) (arguing for stronger legislation to protect information in the Internet context); Kerr, *supra* note 24, at 1019–22 (arguing for application of a content/non-content distinction); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1151–67 (2002) (articulating a framework under which the Third Party Doctrine should operate given the sheer volume of information that is accessible under this doctrine); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 Fordham L. Rev. 747, 761–77 (2005) (arguing that legislation may be ill-equipped to protect information in the Internet context).

[136] *See, e.g.*, Strandburg, *supra* note 25, at 654–64 (arguing that the Third Party Doctrine should not be applied to certain Internet communications); 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").

takeaway for this analysis is that by and large these theories focus on communications as communications when trying to explain why these discrete transmissions merit privacy protection.[137]

The Article moves away from this traditional approach in an effort to offer a new way of thinking about the reasonable expectation of privacy test. Although this Article seeks to identify the common problems associated with the Third Party Doctrine and its application to Internet communications (a frequently discussed theme within this scholarship), its ultimate aim is to posit a solution that focuses on the relationships created by Internet communications over social networking sites rather than on the individual transmission standing alone. Accordingly, this Article will briefly focus on three representative theories—within the conventional Fourth Amendment jurisprudence—that seek to explain how the doctrine should be applied in the Internet context.[138]

1. Automation Versus Human Observer

One scholar challenges the premise that merely disclosing data to electronic storage facilities vitiates Fourth Amendment protection.[139] That scholar proposes a human observer theory, which argues that proper application of the Third Party Doctrine contemplates that the disclosure will eventually be exposed to human observation.[140] It is this ultimate human observation that vitiates an individual's expectation of privacy, not the mere exposure to an automated machine.[141]

Online users transmit voluminous amounts of data over the Internet.[142] But this mass of data is stored on third party servers and has a low chance of being directly observed by a human being.[143] According

---

[137] One scholar's account seems to recognize the value of these communications as more than just the discrete communication. *See* Strandburg, *supra* note 25, at 654–64. But this account focuses on the general connection between cyberspace and the real world, whereas this Article's analysis focuses more on the actual relationship formed in cyberspace. *Compare infra* notes 182–209 and accompanying text (discussing the technosocial theory), *with infra* notes 382–423 and accompanying text (discussing the role of social networking communications in human life).

[138] *See, e.g.*, Kerr, *supra* note 24, at 1017–29 (arguing for the application of the content/non-content distinction); Strandburg, *supra* note 25, at 654–64 (arguing that the Third Party Doctrine should not be applied to certain Internet communications); Tokson, *supra* note 23, at 601–19 (arguing that the Third Party Doctrine should apply only to communications that are exposed to a human observer).

[139] Tokson, *supra* note 23, at 616–17.

[140] *Id.*

[141] *Id.*

[142] *See id.* at 604–05.

[143] *See id.* at 604–09.

to the human observer theory, the machine cannot truly violate one's privacy.[144] These automated systems "cannot see us, think about us, judge us, ridicule us, or be curious about us—they cannot perceive us at all."[145] It does not make sense then to say that we lose our right to privacy when information is simply stored in these machines.[146]

The human observer theory finds support in related Supreme Court cases involving technology and surveillance, in which the Court has held that a search only occurs after the information was exposed to human observation.[147] In 1984 in *United States v. Karo*, for instance, the Supreme Court held that merely placing a homing beacon in a container that ultimately found its way into the defendant's possession did not violate the defendant's Fourth Amendment rights because no government official was monitoring the transmission.[148] Only after the police began to monitor the device in the defendant's home did they violate the defendant's reasonable expectation of privacy.[149] Similarly, in 2001 in *Kyllo v. United States*, the Court concluded that the defendant had no expectation of privacy in the infrared heat wave emanating from the defendant's house.[150] The police only violated the defendant's Fourth Amendment rights when they used a thermal scanner outside the defendant's house to detect activity inside the home.[151] Without this human observation, the mere collection of this information by a machine would not violate the Fourth Amendment.[152]

---

[144] *Id.* at 616–17.

[145] Tokson, *supra* note 23, at 617.

[146] *Id.* at 616–17.

[147] *Id.* at 615–16.

[148] *See* United States v. Karo, 468 U.S. 705, 712–13 (1984). Specifically, the Court has stated:

> The mere transfer to [defendant] of a can containing an unmonitored beeper infringed no privacy interest. It conveyed no information that [defendant] wished to keep private, for it conveyed no information at all. To be sure, it created a *potential* for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment.

Id. at 712. Further, the government did not trespass on property or person because the beeper was placed in a container prior to the defendant taking possession of the container. *Id.* at 708; *see* Tokson, *supra* note 23, at 615.

[149] *Karo*, 468 U.S. at 714–15.

[150] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001); Tokson, *supra* note 23, at 615.

[151] *Kyllo*, 533 U.S. at 34–35; Tokson, *supra* note 23, at 615.

[152] Tokson, *supra* note 23, at 615–16.

Appellate courts have yet to adopt this distinction.[153] By and large, they have simply accepted the automation rationale under *Smith v. Maryland* without a discussion of the relevance of human observation.[154] The U.S. Court of Appeals for the Ninth Circuit, for instance, held that certain information in an e-mail—the "to" and "from" lines—was not protected by the Fourth Amendment simply because the user voluntary conveyed it to third party equipment.[155] The U.S. Court of Appeals for the Fourth Circuit similarly concluded that a person loses any expectation of privacy to an e-mail because of its disclosure to third party equipment, without determining whether a human employee observed the information.[156]

It is also not clear how the human observer theory impacts Fourth Amendment protection when it comes to Facebook communications. Facebook privacy policies explicitly state that the company can use a person's information "as part of [its] efforts to keep Facebook . . . safe and secure"[157] as well as "share [a user's] information in response to a legal request . . . if [it] ha[s] a good faith belief that the law requires [it] to do so."[158] This language suggests that actual employees may at any point review the stored data to prevent fraud or to otherwise comply with government requests.[159] Does the potential of human observation change the foregoing analyses?[160] Would it matter if employees

---

[153] *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510–11 (9th Cir. 2008); United States v. Hambrick, No. 99–4793, 2000 WL 1062039, at *3–4 (4th Cir. Aug. 3, 2000).

[154] *See, e.g.*, *Forrester*, 512 F.3d at 510–11; *Hambrick*, 2000 WL 1062039, at *3–4; *see also* Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 182–83 (D. Conn. 2005) (holding that the defendant did not have a reasonable expectation of privacy in his AOL subscriber information because his contract with AOL permitted AOL to release the information to third parties).

[155] *See Forrester*, 512 F.3d at 510–11.

[156] *See Hambrick*, 2000 WL 1062039, at *3–4. The case only involved non-content parts of an e-mail. *See id.* at *3; *infra* notes 165–181 and accompanying text.

[157] *Data Use Policy: How We Use the Information We Receive*, *supra* note 120.

[158] *Data Use Policy: Some Other Things You Need to Know*, *supra* note 120.

[159] *See* Semitsu, *supra* note 62, at 296, 306 (discussing the potential for Facebook employees to review data as necessary to comply with the law); *Data Use Policy: Some Other Things You Need to Know*, *supra* note 120.

[160] As one scholar argues,

> If Tokson is correct that we retain privacy when we give information to third parties *because* computers do not—indeed, cannot—invade privacy, then it would seem the government could run machine searches of data without justification. Perhaps there would be an ultimate human reader, but it would occur only after the necessary justification, or perhaps in a future system the computer would inform officers to focus on a certain threat . . . without revealing any of the searched data.

regularly reviewed a specific random sampling content for compliance with Facebook policies?

Scholars arguing for the need of human observation would surely focus on actual observation as the critical element for vitiating Fourth Amendment protection, presumably relying on *Karo* and *Kyllo*.[161] For even in *Smith*, there was the potential that an operator could review the dialed numbers.[162] 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?* If the doctrine is best understood as a waiver principle, the situations are identical—the individual voluntarily disclosed the information to somebody or something else.[163] Thus, accepting the human observation proposal would also seem to overrule *Smith*, which did not distinguish between disclosure to a machine and human.[164]

2. Content/Non Content Distinction

Another scholar provides another prominent response that focuses on the old distinction between content and non-content information, originally created to protect mail delivered by the U.S. Postal Service.[165] Under long-standing Supreme Court precedent, an individual has a reasonable expectation of privacy in the contents of the mail being sent but not in what is printed on the face of the envelope, including the recipient and mailing address.[166] The rationale is that citizens should be free to take advantage of the mail system without foregoing privacy protections of sealed envelopes.[167]

Henderson, *supra* note 136, at 48.

[161] *See Kyllo*, 533 U.S. at 34–35; *Karo*, 468 U.S. at 712–14.

[162] *See Smith*, 442 U.S. at 744.

[163] *See supra* notes 84–86 and accompanying text.

[164] *See Smith*, 442 U.S. at 744–45. The human observation theory argues that *Smith* should be treated as sui generis based on the unique facts, namely human operators formerly served in the role that is now performed by machines. Tokson, *supra* note 23, at 634–36. It is not clear, however, why this theory dismisses the Court's broad language as irrelevant to the Internet context when it would squarely include ISPs. *See Smith*, 442 U.S. at 744–46. Whether desirable or not, *Smith* remains precedent for today's technological world, and it must be accounted for accordingly. *See id.* at 741–46.

My argument seeks to retain the basic holding in *Smith* but provides a justification for why communications constituent of social networking relationships deserve special attention, even though the transmission is disclosed to a machine or an ISP.

[165] Kerr, *supra* note 24, at 1020–31.

[166] *See id.* at 1022–23; *see also Ex Parte* Jackson, 96 U.S. 727, 733 (1877) (holding that letters and sealed packages cannot be opened unless the government obtains a warrant).

[167] *See* United States v. Van Leeuwen, 397 U.S. 249, 251–52 (1970).

To be clear, the content/non-content theory seeks to provide a general framework for applying the Fourth Amendment in the Internet context; it focuses on applying the traditional conceptions of spatial privacy.[168] Using this theory, one can analogize the recipient and mailing address on a postal letter to the "to" and "from" address fields in an e-mail, both constituting non-content information.[169] The content part of a mailed letter is analogized to the subject line and body of the e-mail, both deserving Fourth Amendment protection.[170]

This theory does not necessarily interfere with the proper application of the Third Party Doctrine because the crux of the principle remains. An individual still loses her expectation of privacy with certain information after handing it to a postal employee or sending it over the Internet.[171] But, this disclosure is simply restricted to non-content information and does not apply to the sealed information of a postal letter or the subject line or body of an e-mail.[172] It is also of no consequence whether the communication would be disclosed to a machine or human being.[173] This theory provides a distinction grounded solely on the normative principles of content versus non-content.[174] In this way—and unlike the aforementioned human observation doctrine—this theory avoids reliance on empirical determinations associated with whether the communication is or will be observed by a human.[175]

Some appellate courts have adopted this approach to explain how the Fourth Amendment should apply to communications over the

---

[168] *See* Kerr, *supra* note 24, at 1017–22. The proponent of the content/non-content theory for Internet communications analogizes the foundational Fourth Amendment distinction of inside versus outside (i.e., the doctrine of spatial privacy) to the content versus non-content distinction described above. Kerr, *supra* note 24, at 1017–22.

[169] *Id.* at 1023; *see also* United States v. Maxwell, 45 M.J. 406, 417–19 (C.A.A.F. 1996) (analogizing America Online e-mails to letters).

[170] Kerr, *supra* note 24, at 1023; *see also* Semitsu, *supra* note 62, at 334 (analogizing the law on wiretap searches to the law on mail searches).

[171] *See* Kerr, *supra* note 24, at 1023 (noting that information like the e-mail header would still not be entitled to Fourth Amendment protection).

[172] Kerr, *supra* note 24, at 1022–23. This doctrine is also consistent with the holding in *Smith*, because the pen register recorded only the phone number or the non-content information of the call, not the substance of the conversation or the content of the communication. *See Smith*, 442 U.S. at 744–45.

[173] *See* Kerr, *supra* note 24, at 1017–22.

[174] *Id.* at 1020.

[175] *See id.* at 1020–21; Tokson, *supra* note 23, at 601–19. The proponent of the human observation rationale raises this as a potential objection to his theory. Tokson, *supra* note 23, at 636–38. Yet this scholar argues that although this theory rests on a purely factual assertion (whether or not the information was observed by a human), a court is free to apply a normative principle after this initial determination has been made. *Id.* at 637–38.

Internet.[176] The U.S. Court of Appeals for the Sixth Circuit, for instance, held that an individual has a reasonable expectation of privacy in the content of an e-mail, even if the message is stored in a third party server.[177] But, other courts seem to favor a straightforward application of the Third Party Doctrine, in which the content of the e-mail also does not receive Fourth Amendment protection.[178]

At a conceptual level, the content/non-content distinction works well to explain e-mails sent over sites such as Gmail and Yahoo where there is a clear "to" and "from" category distinguished from the body of the e-mail. But not all communications over social networking sites such as Facebook are readily translated into these two categories.[179] How would this theory account for status updates, instant messages, or pictures? It is hard to see how the content/non-content distinction would apply to these types of communications.[180] By analogizing to postal letters, the theory assumes that the communication has both parts—content and non-content—and that one can easily make this distinction.[181] But Internet communications over Facebook do not work so neatly. Status updates do not seem to have these two types of information; neither do instant messages. These types of communications cannot be separated into component parts in the same way postal letters or e-mails can. There would be similar—if not greater—difficulty in categorizing pictures posted on Facebook.

It will not work to say simply that the entire communication contains substantive content and thus it should all be protected. This is because the basic thrust of the theory is working from the analogy to postal letters. If the analogy breaks down, so does the rationale for protecting the content part of the communication. The problem is that

---

[176] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904–05 (9th Cir. 2008) (holding that users have an expectation of privacy in the contents of their text messages), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (holding that the search was reasonable and, therefore, did not violate the Fourth Amendment).

[177] *Warshak*, 631 F.3d at 288. An earlier ruling on this issue was vacated on ripeness grounds. 490 F.3d 455 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

[178] *See, e.g.*, Rehberg v. Paulk, 598 F.3d 1268, 1281–82 (11th Cir.), *vacated*, 611 F.3d 828 (11th Cir. 2010); *In re* Search Warrant for Contents of Elec. Mail, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009) (noting 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").

[179] *See* Strandburg, *supra* note 25, at 643 & n.150. The content/non-content theory may adequately explain Facebook messages that are sent between users.

[180] *See id.* (finding that although the content/non-content distinction may work well with e-mails, the analogy breaks down with other types of electronic communications).

[181] *See id.*

communications over the Internet, and particularly over social networking sites such as Facebook, cannot be reduced to electronic versions of postal letters—the range of tools is far more varied and complex. The problem with this theory stems from the focus on the discrete transmission itself and its component parts. Working, instead, from the perspective of the relationship created by these communications—as this Article seeks to do—provides a more robust theory for protecting these communications.

3. Technosocial Continuity

Another scholar takes a stronger position by arguing against the application of the Third Party Doctrine in today's technological age.[182] The scholar's basic thesis is that an aggressive application of this doctrine fails to appreciate the social role of the Internet, something that could not have been appreciated when the doctrine was first articulated in *United States v. Miller* and *Smith*.[183]

This scholar's theory—the technosocial continuity theory—argues that "[c]yberspace has become a space for social life" and in this way "digital and physical social realms are inextricably intertwined."[184] Because of the prevalence of social media in our lives, the technosocial continuity theory finds that cyberspace has become an extension of the home or office, places where the Fourth Amendment historically applies.[185] Accordingly, application of the Third Party Doctrine in the social media context is not appropriate, and it should not aggressively be applied.[186]

The technosocial continuity theory further states that third party Internet service storage systems are the modern equivalent of landlords or other service providers that may share authority over a person's home or other physical space.[187] These servers similarly promote and sustain the ability of users to transmit information over the Internet from one person to another.[188] Thus, even though there is a shared transmission of information, the disclosure to third party servers should not vitiate the sender's reasonable expectation of privacy.[189]

---

[182] *Id.* at 634–39.
[183] *Id.*
[184] *Id.* at 639.
[185] Strandburg, *supra* note 25, at 654–64.
[186] *See id.* at 639, 656–57.
[187] *See id.* at 639–41.
[188] *Id.* at 641.
[189] *See id.*

This technosocial continuity theory finds support in Supreme Court precedent involving individuals who share premises.[190] The scholar cites the Supreme Court's 2006 decision, *Georgia v. Randolph*, where the Court held that the government could not conduct a search of the premises where one occupant consented but the other did not.[191] In addition, other precedent holds that individuals have a reasonable expectation of privacy in a temporary quarter, even if an owner or landlord continues to have a right to enter the property.[192] Shared use thus does not automatically mean loss of privacy protection, particularly when the third party, such as a landlord, provides services that promote and sustain the property.[193]

This scholar makes a valid point.[194] In fact, the ubiquitous nature of making disclosures in today's technology dominated world has led some scholars to question whether the Third Party Doctrine should be understood as a doctrine of waiver or consent.[195] One scholar writes, "[e]ven when a person allows a third party access to information . . . it does not necessarily mean that either the individual or the third party has consented to access by the government. . . . [The doctrine assumes] that there was a choice to disclose information to a third party . . . ."[196] This scholar cites to paying electricity bills and depositing money in a bank as necessary acts that, under a consent theory, would constitute a waiver of all privacy protection for the information.[197] Similar reason-

---

[190] *Id.* at 639–41; *see, e.g.*, Georgia v. Randolph, 547 U.S. 103, 106 (2006) (holding that one co-tenant may not consent to a search over the objection of another present co-tenant); Minnesota v. Olson, 495 U.S. 91, 96–97 (1990) (holding that an overnight guest had a reasonable expectation of privacy in the host's home).

[191] *Randolph*, 547 U.S. at 106; Strandburg, *supra* note 25, at 639–40.

[192] Strandburg, *supra* note 25, at 640 & n.138 (collecting cases).

[193] This technosocial continuity theory relies on another scholar's analysis. *See id.* at 641. In relevant part, that scholar states "entities [digital service providers] are functionally analogous to 'servants' who are also encompassed by this conception of shared privacy; unlike the servants of centuries ago, they do not reside in the home, but they provide services that promote and sustain activities within the home." *Id.* at 641 (citing Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 Miss. L.J. 1, 76 (2005)).

[194] Indeed, one may take this scholar's argument about facilitation a step further and focus on the necessity of Internet storage servers. Put simply, without these servers, there would be no transmission. *See infra* notes 452–462 and accompanying text.

[195] *See supra* notes 84–86 and accompanying text.

[196] McNeil, *supra* note 84, at 216.

[197] *Id.* at 216–17. The scholar notes that in order to put money in a bank account, the banker must disclose some information to the bank, including one's name, social security number, as well as the various deposits and credits into the account. *See id.* All of this information would, therefore, not be protected under the Third Party Doctrine. The alternative to making such disclosures, however, is for one to keep the money in a shoebox

ing can be applied to Internet communications. Because the ISP is a necessary component to the transmission, the Internet user has no real choice in making the disclosure.[198]

The merits of this theory would ultimately turn on how one characterizes the nature of the consent. A strict interpretation of the term would seem to suggest that a Facebook user has in fact consented to disclosing the information.[199] Moreover, even though technology dominates our lives and there are many instances where one might argue people *must* disclose things to other parties to function (e.g., bank records, electricity bills), Facebook does not appear to fall into this category. No one needs to have a Facebook account to survive. Any use of the site would thus suggest a willing disclosure. But regardless of the merits of the theory that necessary disclosures should not be subject to the Third Party Doctrine, as previously discussed, the Court has not adopted such a narrow conception of consent in the Fourth Amendment context.[200] Under the current application of the Third Party Doctrine, individuals assume the risk in making these disclosures, even if these disclosures are an integral part of their lives.[201]

The technosocial theory on its own terms, however, would also not seem to protect fully communications from the government's reach. Nothing would seem to stop the government from compelling service-oriented individuals (e.g., maids, landlords) to divulge incriminating information or prevent these individuals from reporting behavior on their own accord.[202] Similarly, the government would be otherwise free to acquire the information from the ISP,[203] or this entity itself would be free to disclose information to the government.[204] In either case, there is no constitutional check on the government's ability to acquire the information.

---

under one's bed. *Id.* at 216. Although this may be an option, it is not a practical option in today's world. *Id.* at 216–17.

[198] *See* Miller, *Facebook Makes Big Investment*, *supra* note 120 (noting that Facebook has extended the number of servers needed for the data on its site); *cf.* Gralla, *supra* note 115, at 88–99 (describing how e-mails are transmitted and stored).

[199] *See supra* notes 114–129 and accompanying text.

[200] *See supra* notes 76–89 and accompanying text.

[201] *See Smith*, 442 U.S. at 744–45; *Miller*, 425 U.S. at 442–43. Justice Sonia Sotomayor's concurring opinion in *United States v. Jones* raises concerns about the doctrine as it currently stands. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *infra* notes 263–283 and accompanying text.

[202] Strandburg, *supra* note 25, at 641; *see infra* notes 337–375 and accompanying text.

[203] *See infra* notes 230–262 and accompanying text.

[204] *See infra* notes 263–283 and accompanying text.

More to the point, the technosocial theory comes at the cost of jettisoning the Third Party Doctrine, at least in the context of social networking on the Internet.[205] The proposing scholar, for example, finds that although undercover informants may use chat rooms to gather incriminating statements from would-be criminals (e.g., posing as an underage child) because chat rooms are not extensions of the home or office, similar ploys relating to creation of fake Facebook profiles by government agents should not be allowed, presumably because Facebook is an extension of the home or office.[206] It is not clear why these types of disclosures do not stand or fall together, at least from the perspective of voluntary disclosure and waiver to the undercover government informant.

This Article does not make such a bold claim, nor has the Court adopted such a drastic remedy.[207] In fact, this Article's argument preserves most of the doctrine as it stands. It does not seek to thwart government efforts to use fake identities or other deceptive tactics via social networking sites to solicit information from potential criminals.[208] It simply puts Internet relationships on the same footing as their face-to-face counterparts while preserving the basic principles behind the Third Party Doctrine.[209]

---

[205] *See* Strandburg, *supra* note 25, at 634 (noting that "some courts . . . are beginning to move away from a rigid and aggressive third party doctrine and toward an approach consistent with the principle of technosocial continuity"). Another scholar seems to make a similar argument. *See* Semitsu, *supra* note 62, at 369 ("Courts should view Facebook as the twenty-first century equivalent of the phone booth. . . . Today, if Katz's son sets his Facebook content to 'private' and limits his conversations to trusted friends, he has done the equivalent of shutting the phone booth doors."). As to the application of the Third Party Doctrine, like the technosocial continuity theory, this scholar seems to argue that such disclosures should not sacrifice a user's privacy interest. *See id.* at 369–71. But the scholar does not explain why disclosure to an ISP should not vitiate a reasonable expectation of privacy, when a similar disclosure made to a pen registry in *Smith* did. *See id.* If the scholar's point relates to preventing government surveillance and surreptitious monitoring, that argument would also suggest that a person should retain an expectation of privacy in disclosures made to an undercover government agent in a face-to-face setting, a view that the Court has rejected. *White*, 401 U.S. at 748–54; On Lee v. United States, 343 U.S. 747, 750–53 (1952).

[206] Strandburg, *supra* note 25, at 670–79.

[207] *See id.*; *infra* notes 263–283 and accompanying text; *infra* notes 376–488 and accompanying text. But the Supreme Court's most recent decision on privacy and technology, *Jones*, 132 S. Ct. 945, suggests a reevaluation of the Third Party Doctrine in light of the pervasive use of the Internet. *See infra* notes 263–283 and accompanying text.

[208] *See infra* notes 459–462 and accompanying text.

[209] The technosocial continuity theory also tackles the issue of how the plain view doctrine would apply in the Internet context as well as the use of undercover surveillance and informants in social media contexts. Strandburg, *supra* note 25, at 664–79. A full examination of this theory, however, is beyond the scope of this Article. For my purposes, it is

C. *Facebook Privacy Policies*

The Fourth Amendment simply represents the minimum protection afforded to communications over social networking sites.[210] There are other nonconstitutional mechanisms available—such as privacy policies or congressional legislation—that may provide additional protection.[211] Facebook, like most interactive websites, has extensive privacy policies intended to ensure protection of a user's content.[212]

The relevant portion of Facebook's privacy policies states that a user's "privacy is very important" and that the company shares information only in limited circumstances.[213] These circumstances include where the company has received permission from the user, where the user has been given notice (such as in the privacy policies), and where the user's name and personal information have been removed.[214] These circumstances appear relatively restrictive—anonymous disclosures or substantive disclosure only by notice—but by referencing its other privacy policies, Facebook retains significant discretion in releasing information to third parties.[215] The most pertinent part of Facebook's privacy policies relates to sharing information with government authorities. Facebook's policies state that it may:

> access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so.

---

enough to say that there are some scholars who favor wholesale rejection of the Third Party Doctrine as it applies to these sites. *See* Henderson, *supra* note 136, at 39–40; Strandburg, *supra* note 25, at 634–41, 654–64.

[210] *See infra* notes 211–262 and accompanying text.

[211] *See infra* notes 211–262 and accompanying text.

[212] *Data Use Policy*, *supra* note 120 (describing the privacy policies for Facebook); *Statement of Rights and Responsibilities*, *supra* note 120 (describing the terms of use for Facebook); *see Privacy Policy*, GOOGLE, *supra* note 117 (describing the privacy policies for Google); *Privacy Policy*, MYSPACE, http://www.myspace.com/Help/Privacy (last revised Dec. 17, 2012) (describing the privacy policies for Myspace); *see also* Semitsu, *supra* note 62, at 302–18 (discussing the privacy policies of Facebook and other social networking sites).

[213] *Data Use Policy*, *supra* note 120 (outlining the circumstances under which Facebook can reveal users' information); *Statement of Rights and Responsibilities*, *supra* note 120 ("Your privacy is very important to us. 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.").

[214] *Data Use Policy: Information We Receive and How It Is Used*, *supra* note 120. When it comes to advertisers, the policy explicitly states that information is disclosed only after a user's name or any other personally identifying information is removed. *Data Use Policy: How Advertising and Sponsored Stories Work*, *supra* note 120.

[215] *See* Semitsu, *supra* note 62, at 305–06.

> This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.[216]

The language seems overly inclusive and could potentially allow disclosure based on requests short of warrants, including requests from international law enforcement authorities.[217]

But even if this is an unfair characterization, the final paragraph and its catchall language eviscerates any supposed protections offered by the preceding paragraph.[218] The relevant language states that Facebook may also share information when necessary to "prevent fraud or other illegal activity" and may be accessed for "investigations concerning possible violations of our terms or policies."[219] The Statement of Rights and Responsibilities details a wide range of proscriptions, including not posting anything hateful, threatening, pornographic, containing nudity, or gratuitous violence, or using Facebook to do anything misleading, malicious, or discriminatory.[220] Although, as a whole, these prohibitions may certainly benefit users, the sweeping language gives Facebook wide latitude in disclosing a person's information.[221]

These policies, however, only bind Facebook.[222] Facebook remains free—at any point—to modify these policies and to provide even less privacy protection.[223] And because recent studies show that most users are not aware or otherwise do not carefully read these policies, users may not realize that their information is potentially more vulnerable to disclosure based on evolving Facebook privacy policies.[224] Furthermore,

---

[216] *Data Use Policy: Some Other Things You Need to Know*, *supra* note 120.

[217] *See* Semitsu, *supra* note 62, at 306.

[218] *See id.* at 307; *Data Use Policy: Some Other Things You Need to Know*, *supra* note 120.

[219] *Data Use Policy: Some Other Things You Need to Know*, *supra* note 120.

[220] *Statement of Rights and Responsibilities: Safety*, *supra* note 120.

[221] *See supra* notes 213–220 and accompanying text. Other social networking sites have similar privacy policies. Myspace, for example, allows the company to disclose user information to protect or defend the company or its employees, protect the safety and security of users, protect against fraud or for risk management purposes, or to comply with the law or legal process. *See Privacy Policy*, Myspace, *supra* note 212; *see also* Semitsu, *supra* note 62, at 315 (discussing Myspace's privacy policy).

[222] *See* James Grimmelmann, *Saving Facebook*, 94 Iowa L. Rev. 1137, 1183 (2009).

[223] Facebook has changed its privacy policies many times in response to complaints about inadequate protection. Semitsu, *supra* note 62, at 302.

[224] *See* Grimmelmann, *supra* note 222, at 1181–82 (detailing studies that showed that most users never read the privacy policies or did not accurately understand what the policies allowed).

these polices would not legally prevent the government from acquiring the information without a warrant.[225] As at least some courts have held, current law would allow the government to acquire this information short of a warrant, despite efforts by Facebook to block such requests.[226]

Perhaps most important, though, these self-regulated privacy policies—assuming they are considered effective—are not synonymous with constitutional protection. Under the Third Party Doctrine, loss of Fourth Amendment protection occurs as soon as the user exposes the information to a third party, in this case Facebook servers.[227] It would not make a difference, then, if Facebook, without any notice, suddenly changed its policies to the detriment of its users.[228] All that matters—from a constitutional perspective—is that a user knowingly exposed the information to Facebook, even if on the (erroneous) assumption that "it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[229]

D. *Congressional Legislation*

Congressional legislation provides another, perhaps more robust, way to protect communications over social networking sites.[230] The Electronic Communications Privacy Act of 1986 (ECPA) attempts to provide a comprehensive scheme that goes beyond Fourth Amendment protection to restrict unauthorized government surveillance of electronic

---

[225] *See infra* notes 230–262 and accompanying text.

[226] *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113–15 (3d Cir. 2003) (holding that the Wiretap Act and the SCA do not protect e-mail communications stored on servers);United States v. Weaver, 363 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (holding that previously read e-mails do not constitute electronic storage under the Stored Communications Act (SCA)); *see also infra* notes 230–262 and accompanying text.

[227] *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) (holding that a government agent's search following a search by a private carrier did not constitute a search within the meaning of the Fourth Amendment); *supra* notes 114–129 and accompanying text.

[228] There would be no constitutional violation here because a private party, not the government, would be breaching its agreement. *See, e.g.*, NCAA v. Tarkanian, 488 U.S. 179, 191 (1988) ("As a general matter the protections of the Fourteenth Amendment do not extend to 'private conduct abridging individual rights.'" (quoting Burton v. Wilmington Parking Auth., 365 U.S. 715, 722 (1961))).

[229] *Miller*, 425 U.S. at 442; *see also Jacobsen*, 466 U.S. at 117 ("It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information."); *Semitsu*, *supra* note 62, at 349 ("If Facebook or its employees were to voluntarily provide a user's personal information to government investigators, the Fourth Amendment would not clearly prevent or exclude such evidence under the [Third Party Doctrine].").

[230] *See infra* notes 231–262 and accompanying text.

communications.[231] Three relevant parts of the ECPA potentially apply to Facebook communications: (1) the Wiretap Act;[232] (2) the Stored Communications Act (SCA);[233] and (3) the Pen Register Act (PRA).[234]

The Wiretap Act prohibits federal law enforcement from intercepting wire and electronic communications, unless it has probable cause and a warrant signed by a judge.[235] Facebook communications would seem to fall under the Wiretap Act as they constitute electronic communications. Another part of the Wiretap Act, however, defines "intercept" as the contemporaneous "acquisition of the contents of any" electronic transmission.[236] This would mean that most Facebook communications are not protected because the social networking site is designed to be a storage site for communications, rather than a mechanism for simultaneous conversations.[237] Courts facing this issue have concluded that, for this reason, the Wiretap Act does not cover Facebook communications.[238]

The SCA was explicitly designed to address various Internet communications that were not necessarily protected by the Fourth Amendment.[239] The Act seeks to prevent the government from access-

---

[231] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522, 2701–2711, 3117, 3121–3127 (2006)).

[232] 18 U.S.C. §§ 2510–2522.

[233] *Id.* §§ 2701–2711.

[234] *Id.* §§ 1321–1327. The following discussion of the ECPA, its three relevant parts, and its resulting shortcomings primarily summarizes another scholar's more complete analysis. *See* Semitsu, *supra* note 62, at 352–66.

[235] *See* 18 U.S.C. §§ 2510–2522. The statute originally covered only wire and oral communications, but it was subsequently amended to include "electronic communications." *See id.* § 2511(1); Semitsu, *supra* note 62, at 353.

[236] 18 U.S.C. § 2510(4). Even though the section does not explicitly require contemporaneous interception of communication with their transmission, the other relevant statutes, together with the context in which the Wiretap Act was passed (recording two-way conversations), suggests this interpretation. *See* Semitsu, *supra* note 62, at 355; *infra* notes 239–259 and accompanying text.

[237] *See* Semitsu, *supra* note 62, at 355. This would exclude, of course, instant messaging on Facebook.

[238] *Cf. Fraser*, 352 F.3d at 113–14 (holding that the Wiretap Act does not cover e-mail communications stored on servers); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460–62 (5th Cir. 1994) (same); *see also* Semitsu, *supra* note 62, at 355 & n.240 (collecting cases). *But see* United States v. Councilman, 418 F.3d 67, 79–80 (1st Cir. 2005) (suggesting that contemporaneous interception is not required and that e-mail messages can be intercepted after they are stored).

[239] *Quon*, 529 F.3d at 900 ("The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address."); *see* 18 U.S.C. §§ 2701–2711 (2006); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209–13 (2004) (explaining why the SCA exists).

ing electronically stored content, which would include acquiring communications stored on Facebook servers.[240] Yet there are important exceptions, governed by the length of time the information has been stored.[241] Communications in "electronic storage" for 180 days or less have the greatest protection and require a search warrant supported by probable cause.[242] Communications stored for greater than 180 days, however, only require a trial subpoena supported by reasonable suspicion, which would allow the government to compel Facebook for these records.[243] Facebook communications stored for longer periods thus do not have the kind of protection Congress arguably intended when it enacted the SCA.[244]

But communications stored for less than 180 days may also not receive sufficient protection under the SCA.[245] The problem is that "electronic storage" is not clearly defined under the relevant provision and may exclude previously read communications.[246] This is particularly significant because most Facebook communications—including e-mails, photos, or posts—will presumably be read or viewed prior to 180 days. Under this interpretation, then, most Facebook communications will not receive SCA protection. Courts are divided on how to interpret the relevant statutory language.[247] Some interpret "electronic storage"

---

[240] *See* 18 U.S.C. §§ 2701–2711.

[241] *See id.*

[242] *Id.* § 2703(a).

[243] *See id.* § 2703(a), (d). A court may issue an order to the ISP to disclose information as long as:

> the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, . . . are relevant and material to an ongoing criminal investigation. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Id. § 2703(d); *see also* Semitsu, *supra* note 62, at 360 (noting that under § 2703(d) the government must satisfy a "reasonable suspicion" standard, which is lower than the typical "probable cause" requirement, and that § 2703(d) "allows the government to compel Facebook to disclose all content specific to named individuals with a subpoena, without probable cause, and without any meaningful notice"); *cf.* People v. Harris, 945 N.Y.S.2d 505, 512–13 (Crim. Ct. 2012) (applying the reasonable suspicion standard and finding that under the SCA, Twitter must disclose electronic information).

[244] Semitsu, *supra* note 62, at 360–61.

[245] *Id.*

[246] *See* 18 U.S.C. §§ 2510, 2711 (2006).

[247] *Compare* Theofel v. Farey-Jones, 359 F.3d 1066, 1075–77 (9th Cir. 2004) (holding that the SCA does protect e-mails stored on a server), *with Fraser*, 352 F.3d at 114–15 (holding that the SCA does not protect e-mails stored on a server).

narrowly, refusing to extend protection to these Internet communications.[248] Others, however, interpret the term broadly, extending protection to previously read Internet communications.[249]

Perhaps most troubling, the SCA explicitly states that damages are the only remedy available when the government obtains information from the ISP in violation of the statute.[250] This means that even if the government violates the procedures, the statute does not bar the admission of the communication as evidence in a criminal trial.[251]

The last provision of the ECPA that could provide protection to communications such as those on Facebook is the PRA, which requires the government to seek a court order before installing an electronic device to record incoming address information.[252] Its constitutionality stems from *Smith*;[253] however, the statute provides a bit more protection than the Fourth Amendment.[254] As previously discussed, an individual has no expectation of privacy in the phone numbers he or she dials, and the government is free to acquire this information without a warrant.[255] But now, the PRA requires the government to at least certify that the information is likely to be relevant for an ongoing investigation before installing a pen register device.[256] The statute also applies to certain Internet communications, specifically the "to" and "from" fields of

---

[248] *See, e.g.*, *Fraser*, 352 F.3d at 114–15; *Weaver*, 363 F. Supp. 2d at 773; Flagg v. City of Detroit, 252 F.R.D. 346, 359 (E.D. Mich. 2008).

[249] *See, e.g.*, *Theofel*, 359 F.3d at 1075–77; *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 661 (E.D. Va. 2008). Interestingly, Facebook's own policy on law enforcement requests requires a search warrant pursuant to the SCA for any request for stored content, including "messages, photos, wall posts, and videos." *Information for Law Enforcement Authorities*, Facebook, https://www.facebook.com/safety/groups/law/guidelines/ (last visited Dec. 22, 2012).

[250] 18 U.S.C. § 2708; Semitsu, *supra* note 62, at 362 ("Worst of all, the SCA expressly leaves out exclusion as a remedy when the government obtains content in violation of the statute. Section 2708 states that damages 'are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.'" (quoting 18 U.S.C. § 2708)). There would be no constitutional violation because under the Third Party Doctrine, Facebook users have no reasonable expectation of privacy in the information.

[251] *E.g.*, United States v. Clenney, 631 F.3d 658, 667 (4th Cir. 2011); United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008).

[252] 18 U.S.C. §§ 3121–3127 (2006).

[253] *See* Semitsu, *supra* note 62, at 634; *supra* notes 90–106 and accompanying text.

[254] *See* 18 U.S.C. §§ 3121–3127; Semitsu, *supra* note 62, at 634.

[255] *Smith*, 442 U.S. at 744–46.

[256] 18 U.S.C. § 3122(b)(2). This standard is lower than probable cause and perhaps lower than reasonable suspicion because the government does not have to provide any specific facts. Semitsu, *supra* note 62, at 364–65.

an e-mail communication.[257] The PRA, however, does not authorize the collection of the content of an e-mail.[258] This is because the government's ability to access electronically stored content, such as e-mails, is governed by the SCA.[259]

In sum, the ECPA does not appear to provide comprehensive protections for social networking communications, particularly when one considers that most stored communications are read within 180 days.[260] Put in perspective, though, the current drawbacks of the ECPA are not the real issue. To the extent they do not effectively cover all social networking communications, nor provide adequate protection for these communications, Congress is free to amend the relevant provisions. Congress has the power, for example, to pass legislation that creates uniform warrant requirements for all stored information (regardless of the storage time or nature of communication), and to provide exclusionary remedies for any resulting violation.[261]

The bigger issue is the constitutional one. These legislative measures—both present and any future amendments—are not mandated by the Fourth Amendment. As discussed earlier, the Third Party Doctrine vitiates any reasonable expectation of privacy.[262] Facebook users thus are at the mercy of legislatures and their discretion to implement stricter privacy laws that would prevent the government from acquiring information from Facebook without probable cause. To avoid this predicament, one would have to argue that these communications are still somehow deserving of constitutional protection—protection that could mandate remedial legislative action. This Article takes a step in that direction by providing an argument focused on interpersonal privacy that

---

[257] Semitsu, *supra* note 62, at 365; *see In re* Application of the United States, 416 F. Supp. 2d 13, 17 (D.D.C. 2006). The scope of the Act tracks the content/non-content distinction discussed earlier. *See supra* notes 165–181 and accompanying text.

[258] *E.g.*, *In re Application of the United States*, 416 F. Supp. 2d at 17 (noting that Section 3121(c) requires that the devices do not gain access to the content of e-mails). Indeed, courts have found that these devices cannot be used if they collect an e-mail's content. *In re* Application of the United States, 622 F. Supp. 2d 411, 422 (S.D. Tex. 2007); *see In re Application of the United States*, 416 F. Supp. 2d at 17–18.

[259] *See* 18 U.S.C. §§ 2701–2711 (2006).

[260] *See* Tokson, *supra* note 23, at 591–96 (discussing the weaknesses of the statutory protection for Internet communications).

[261] A recent bill has been proposed to fill important gaps in the ECPA. *See* H.R. 2471, 112th Cong. (2012); Cyrus Farivar, *Cops Might Finally Need a Warrant to Read Your Gmail* (Sept. 12, 2012, 7:10 PM), Ars Technica, http://arstechnica.com/tech-policy/2012/09/cops-might-finally-need-a-warrant-to-read-your-gmail/.

[262] *See supra* notes 49–106 and accompanying text.

avoids the aforementioned problems associated with a conventional application of the Fourth Amendment on the Internet.

E. *The Supreme Court's Decision in* United States v. Jones

The Supreme Court's most recent decision on the Fourth Amendment and technology underscores the problems with the Third Party Doctrine and may shed light on its future.[263] In its 2012 decision, *United States v. Jones*, the Court found that the government violated the Fourth Amendment by placing a GPS tracking device on the defendant's car without a warrant.[264] The police thereafter used the device to monitor the vehicle—through public streets—for a four-week period, collecting thousands of pages of data.[265] This information ultimately led to the defendant's conviction.[266]

Writing for the majority, Justice Antonin Scalia concluded that the warrantless installation of this device on the car was essentially a trespass on the defendant's property, constituting a clear violation of the Fourth Amendment.[267] The Court cited to historical precedent of people being secure in their "persons, houses, paper, and effects" from unreasonable searches.[268] The Court went on to note that although *Katz* changed the test for applying Fourth Amendment protection, it in no way repudiated this basic principle.[269] The majority, however, did not address the broader issue of the Third Party Doctrine, and whether the four-week monitoring of the vehicle through public thoroughfares constituted a search under the Fourth Amendment.[270]

Interestingly, Justices Sonia Sotomayor and Samuel Alito, in their respective concurrences, raised doubts about the Third Party Doctrine as applied to this type of electronic surveillance.[271] Justice Sotomayor began by recognizing that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth

---

[263] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[264] *Id.* at 949 (majority opinion). The police had initially obtained a warrant to place the GPS device, but installed the device after the warrant expired. *Id.* at 948.

[265] *Id.* at 948.

[266] *Id.* at 948–49.

[267] *Id.* at 949–50.

[268] *Id.*

[269] *Jones*, 132 S. Ct. at 950–52.

[270] *See id.* at 948–52. The operative facts were different in *Karo*, where the government used a beeper to monitor activities in the defendant's home. *Karo*, 468 U.S. at 715. Here, all the monitoring involved publicly exposed movements on streets. *Jones*, 132 S. Ct. at 948.

[271] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J, concurring); *id.* at 962–63 (Alito, J., concurring).

of detail about her familial, political, professional, religious, and sexual associations."[272] She explained that the attributes of such surveillance should be taken into account when considering whether a person has a reasonable expectation of privacy in the sum of his or her public movements.[273] Justice Alito similarly took issue with the long-term tracking of the defendant and found that these actions did violate the Fourth Amendment.[274]

Currently, of course, individual GPS disclosures, standing alone, do not receive Fourth Amendment protection because the driver voluntarily discloses his or her position to the public.[275] Voluntary disclosure vitiates any reasonable expectation of privacy.[276] As Justice Sotomayor explained, these movements would "attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."[277] She speculated whether the Court should therefore reconsider—in light of today's technological advancements—the viability of the Third Party Doctrine.[278] She stated:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[279]

Justice Sotomayor's point is well-taken. Today's society involves the use of third parties to relay and convey information in an unprecedented manner and frequency. Should we deny Fourth Amendment

---

[272] *Id.* at 955 (Sotomayor, J., concurring). It is important to note here that the GPS device only tracked public movements by the car. *Id.* at 955–56.

[273] *Id.* at 955–56. Justice Sotomayor seemed to raise concerns about both short- and long-term surveillance using a GPS device. *Id.*

[274] *Id.* at 964 (Alito, J., concurring).

[275] *See* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

[276] *See supra* notes 76–106 and accompanying text.

[277] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[278] *See id.*

[279] *Id.*

protection solely on the ground that the information is disclosed to the public or to a third party for a limited purpose?[280]

This concern becomes particularly important when it comes to communications over social networking sites such as Facebook. Users are dependent on the third party servers to facilitate their communications, but this does not mean that users do not consider the information private. The exposure to the server is for the limited purpose of assuring that the information reaches the sender. There is no doubt that users' subjective expectations alone do not mandate Fourth Amendment protection.[281] Still, one must wonder whether technological advances in surveillance and communication necessitate a reconsideration of the Third Party Doctrine as it presently stands.

But any change may have consequences for traditional forms of disclosure as it relates to law enforcement. Should disclosing to a government informant certain information for a limited purpose mean that the information cannot be used at trial? Most would say "no" and current precedent would agree.[282] To be sure, any global change in the Doctrine would have to address these concerns.[283]

III. Interpersonal Privacy Rights

Given the questionable viability of and the difficulty with applying the Third Party Doctrine to Internet communications, including social networking communications, constitutional law dealing with interpersonal privacy provides another avenue for protecting those communi-

---

[280] In 2010, in *United States v. Maynard*, the case appealed to the Court in *United States v. Jones*, the U.S. Court of Appeals for the D.C. Circuit addressed the issue of public disclosure and privacy in the context of GPS surveillance. United States v. Maynard, 615 F.3d 544, 549 (D.C. Cir. 2010). It reasoned that under a "mosaic theory," individual public disclosures that are seemingly minor and trivial may add up to significant revelations of a person's life. *Id.* at 562. The court noted that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation." *Id.* The court's reliance on the mosaic theory in this case raises questions about whether the Fourth Amendment analysis for surveillance on public thoroughfares may change if the observation is continuous and over longer periods of time. *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012) (examining the merits of the mosaic theory).

[281] *See supra* notes 53–75 and accompanying text.

[282] *See Jacobsen*, 466 U.S. at 117; *Miller*, 425 U.S. at 443.

[283] This Article does not argue for abolition of the Third Party Doctrine, and thus such an analysis is beyond its scope. Rather, it seeks to offer a different foundation—one grounded in interpersonal privacy considerations—for the protection of communications over social networking sites like Facebook.

cations.[284] This Part looks at the interpersonal privacy doctrine and how it intersects with Fourth Amendment privacy.[285] Section A summarizes the development of the interpersonal privacy doctrine.[286] Section B then examines the expansion of the interpersonal privacy doctrine.[287] And, Section C discusses the intersections of and tensions between privacy under the Fourth Amendment and privacy under due process and the First Amendment.[288]

A. *Early Development of Interpersonal Privacy*

Unlike the privacy right associated with the Fourth Amendment, interpersonal privacy involves protection of interpersonal relationships and liberty interests and has its origins in the Due Process Clauses of the U.S. Constitution.[289] In cases dating back to the mid-twentieth century, the U.S. Supreme Court relied on the Due Process Clauses to uphold a person's right to conceive and raise children free from government intervention.[290] But it was not until 1965, in *Griswold v. Connecticut*, that the Supreme Court first articulated the contours of a substantive right to privacy that would ultimately stand apart from the privacy associated with the Fourth Amendment.[291]

In *Griswold*, the Court overturned Connecticut's ban on the use of contraception by married couples.[292] The Court found that this law trampled on a "zone of privacy created by several fundamental constitutional guarantees."[293] Although grounded in the Due Process Clause of the Fourteenth Amendment, the Court cited to various guarantees in the Bill of Rights—including the First, Fourth, and Fifth Amendments—

---

[284] *See supra* notes 107–209; *infra* notes 289–375 and accompanying text.

[285] *See infra* notes 289–375 and accompanying text.

[286] *See infra* notes 289–304 and accompanying text.

[287] *See infra* notes 305–336 and accompanying text.

[288] *See infra* notes 337–375 and accompanying text.

[289] *See generally* Ryan C. Williams, *The One and Only Substantive Due Process Clause*, 120 YALE L.J. 408 (2010) (discussing the substantive Due Process Clause). The Due Process Clause of the Fifth Amendment applies to the federal government, whereas the Due Process Clause of the Fourteenth Amendment applies to the states. Bolling v. Sharpe, 347 U.S. 497, 498–99 (1954). At least one scholar also suggests that this due process right to privacy incorporates equal protection principles. *See, e.g.*, Crocker, *supra* note 28, at 10–12.

[290] *See* Stanley v. Illinois, 405 U.S. 645, 649 (1972); Pierce v. Soc'y of Sisters, 268 U.S. 510, 534–35 (1925); Meyer v. Nebraska, 262 U.S. 390, 399, 403 (1923); Crocker, *supra* note 28, at 10.

[291] Griswold v. Connecticut, 381 U.S. 479, 481–86 (1965); Crocker, *supra* note 28, at 11–12.

[292] *Griswold*, 381 U.S. at 485–86.

[293] *Id.* at 485.

and their penumbras or emanations that supported the invalidation of the government's prohibition on contraception.[294] The Fourth and Fifth Amendments, for instance, protect the "'sanctity of a man's home and the privacies of life,'" whereas the First Amendment protects the freedom to associate and privacy in one's associations.[295] Together, these rights—even in the absence of a specific constitutional provision addressing the contraception issue—protect the intimate relations of a married couple from this type of unwarranted government intrusion.[296] To hold otherwise, the Court reasoned, would have a "destructive impact upon that relationship."[297] Through other privacy decisions, the Court broadened this protection from government intrusion to other types of relationships involving unmarried couples using contraception and parental decisions relating to childbearing.[298]

The Court's abortion rights cases further clarified the contours of this right and ensconced interpersonal privacy as a permanent fixture in American jurisprudence.[299] In 1973, in *Roe v. Wade*, the Supreme Court held that this right of privacy was broad enough to cover a women's decision whether or not to terminate her pregnancy.[300] Recognizing that the Constitution does not explicitly mention this right, the Court concluded that its prior precedent still recognized "a right of personal privacy, or a guarantee of certain areas or zones of privacy," with roots in the First and Fifth Amendments.[301]

Similarly, in 1992, in *Planned Parenthood of Southeastern Pennsylvania v. Casey*, the Supreme Court wrote that "[this privacy right] is a promise of the Constitution that there is a realm of personal liberty which the government may not enter."[302] This notion of a person's liberty weighed prominently in the Court's decision upholding a women's right to choose an abortion.[303] The Court defined such choices as in-

---

[294] *Id.* at 483–84.

[295] *Id.* at 484.

[296] *Id.* at 484–86.

[297] *Id.* at 485.

[298] *See* Carey v. Population Servs. Int'l, 431 U.S. 678, 687 (1977) ("Read in light of its progeny, the teaching of *Griswold* is that the Constitution protects individual decisions in matters of childbearing from unjustified intrusion by the State."); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) ("If the right of privacy means anything, it is the right of the *individual*, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.").

[299] Roe v. Wade, 410 U.S. 113, 152–53 (1973).

[300] *Id.*

[301] *Id.* at 152.

[302] Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 847 (1992).

[303] *See id.* at 847–53.

volving "the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy."[304]

B. *The Expansion of Interpersonal Privacy*

The abortion right cases focused on individual autonomy and personal liberty.[305] This makes sense as the issue before the Court was a woman's right to make decisions about her body and life free from government intrusion. In *Lawrence v. Texas*, decided in 2003, the Supreme Court invalidated a Texas law that criminalized certain sexual conduct between two persons of the same sex and expanded interpersonal privacy to include liberty rights associated with interpersonal relationships.[306]

The Court began with a description of the liberty right at stake here.[307] This right, the Court noted, protects us from "unwarranted government intrusions" in our homes and "other spheres of our lives and existence."[308] In reaching beyond spatial bounds, the Court reasoned that this type of "[l]iberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct."[309] Relying on this formulation, the Court found that Texas' sodomy law substantially interfered with, and sought to control, intimate aspects of a couple's life.[310]

It is important that the Court saw this law as not simply a prohibition of a specific sexual act.[311] According to the Court, this law had "far-reaching consequences, touching upon the most private human conduct, sexual behavior, and in the most private places, the home."[312] In other words, the law stood as deleterious to the very existence of the same-sex relationship.[313] Intimate conduct was an essential element in

---

[304] *Id.* at 851.

[305] *Id.* at 847–53; *Roe*, 410 U.S. at 152–53.

[306] *See* Lawrence v. Texas, 539 U.S. 558, 578 (2003). At least one scholar suggests that relying on privacy (as the Court did here) to invalidate such laws is not necessary. *See generally* Sonu Bedi, Rejecting Rights (2009) (arguing that re-conceptualizing ideas of limited government sets limitations on the reasons and rationale on which the polity can act). Analyzing the sodomy statutes in *Lawrence* from a framework that prohibits legislative morality would be sufficient to overturn this type of law. *See generally id.*

[307] *Lawrence*, 539 U.S. at 562.

[308] *Id.*

[309] *Id.*

[310] *Id.* at 567, 578.

[311] *Id.* at 567.

[312] *Id.*

[313] *See Lawrence*, 539 U.S. at 567.

the relationship and was thus within the bounds of personal liberty.[314] As the Court stated, "The [sodomy] statutes . . . seek to control a personal relationship that . . . is within the liberty of persons to choose without being punished . . . ."[315] In this way, *Lawrence* did more than just protect a person's right to enter into a relationship of his or her choosing; it also sought to protect those qualities that are intrinsic to the relationship.[316]

The Court has gone beyond intimate associations and parent-child relationships, and has also affirmed the protection of interpersonal relationships in other contexts.[317] Focusing on First Amendment and equal protection principles, the Court has protected the right of an individual to define the contours of an association free from government intrusion.[318]

In 1984, in *Roberts v. U.S. Jaycees*, for instance, the Supreme Court noted that "individuals draw much of their emotional enrichment from close ties with others" and found 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."[319] In setting the boundaries of this constitutional liberty interest, the Court distinguished between a small group of individuals with close ties and a large business enterprise comprised of strangers.[320] The Court found that liberty was strongest in the former, with whom one shares "not only a special community of thoughts, experiences, and beliefs but also distinctively personal aspects of one's life."[321] This was contrasted with business associations, which do not share the same level of "deep attachment and commitments," nor have the same type of "selectivity" or "seclusion" found in more personal relationships.[322] For this reason, the Court concluded that U.S. Jaycees, a large, nonselective organization composed largely of strangers, could not exclude women from membership because this exclusion did not further any expressive association of the group.[323]

---

[314] *See id.*

[315] *Id.*

[316] *See id.* at 567, 578.

[317] *See, e.g.*, Boy Scouts of Am. v. Dale, 530 U.S. 640, 659 (2000); Roberts v. U.S. Jaycees, 468 U.S. 609, 619–22 (1984).

[318] *Lawrence*, 539 U.S. at 567; *Dale*, 530 U.S. at 659.

[319] *U.S. Jaycees*, 468 U.S. at 619.

[320] *Id.* 619–20.

[321] *Id.* at 620.

[322] *Id.*

[323] *Id.* at 620–22.

Yet, in 2000, in *Boy Scouts of America v. Dale*, the Supreme Court did allow the Boy Scouts—a private organization—to discriminate and exclude homosexuals.[324] Unlike the organization in *U.S. Jaycees*, where exclusion of women would not advance any expressive quality of the organization, here the Court focused on the expressive nature of the organization and found that not allowing the group to exclude homosexuals would adversely impact the group's identity.[325] The Court cited to the Boy Scout Oath and the organization's goal of instilling certain values in its young members.[326] In this case, the Court determined that a heteronormative ideal was part and parcel of the Boy Scout's identity.[327] The organization thus was free to express this element without government intrusion, even if it meant discriminating against a certain group.[328]

To be sure, taken separately and narrowly, *Lawrence*, on the one hand, and *Dale* and *U.S. Jaycees*, on the other, seem to embody different doctrinal constitutional principles—the former specifically protects intimate conduct under due process, whereas the latter protects expressive elements of a relationship under First Amendment and equal protection principles. But, collectively, these cases embody a similar underlying rationale of protecting the essential qualities of relationships and the autonomy to define them free from government intrusion. It is this overarching value of interpersonal relationships, and the expressive quality associated with them, that underscores my analysis.

One scholar makes a compelling argument for this general conclusion.[329] Drawing from these three cases, he argues that the Court is interested in protecting the sanctity of the relationship and the autonomy to define it.[330] These values stand as the basic principles of the interpersonal privacy right.[331] As he argues, "autonomy, intimacy, and dignity

---

[324] *Dale*, 530 U.S. at 644, 659.

[325] *Id.* at 656–59. The dissent recognized that certain associations, including law firms, schools, and labor organizations, could not practice such discrimination. *Id.* at 678–79 (Stevens, J., dissenting). The dissent looked to *U.S. Jaycees* to suggest that such organizations would not have an expressive association that necessitated discrimination. *Id.* at 679–80 (Stevens, J., dissenting) (citing *U.S. Jaycees*, 468 U.S. at 612–13, 615, 623–27). *See generally* Sonu Bedi, *Expressive Exclusion: A Defense*, 7 J. Moral Phil. 427 (2010) (discussing cases in which the Court found a liberty interest based on expressive association under the First Amendment).

[326] *Dale*, 530 U.S. at 649.

[327] *See id.* at 659; Crocker, *supra* note 28, at 20–21.

[328] *Dale*, 530 U.S. at 659.

[329] *See* Crocker, *supra* note 28, at 22–32.

[330] *See id.*

[331] *Id.* at 22.

are all also interpersonal values protected under due process."[332] Autonomy in this context is somewhat self-explanatory: individuals have the ability to choose with whom they associate and what they decide to do in that relationship.[333] These relationships—whether sexual or membership-oriented—also vary in degree of intimacy.[334] Individuals share experiences, emotions, thoughts, and information.[335] Protecting these interpersonal relationships also simultaneously guarantees a person's dignity.[336] Who a person is and what she thinks of herself is inextricably connected with the relationships into which she enters.

C. *The Intersection of Privacy Interests: The Fourth Amendment Versus Due Process and the First Amendment*

The two aforementioned notions of privacy—interpersonal privacy under due process and First Amendment principles and privacy under the Fourth Amendment—seek to protect two different interests.[337] The former protects interpersonal autonomy whereas the latter focuses on a reasonable expectation of privacy.[338] Both can still be seen as protecting against intrusions by the government. Still, only a few scholars have introduced interpersonal privacy into the larger discussion of third party disclosure, a topic typically reserved for Fourth Amendment jurisprudence.[339]

---

[332] *Id.* at 22; *see also* JOHN D. INAZU, LIBERTY'S REFUGE: THE FORGOTTEN FREEDOM OF ASSEMBLY 4 (2012) (discussing the history of the right of assembly and noting that this right protects "a group's autonomy, composition, and existence"); Jamal Greene, *Beyond* Lawrence*: Metaprivacy and Punishment*, 115 YALE L.J. 1862, 1875 (2006) (arguing that the Court in *Lawrence* protects "metaprivacy," that is, "the right to engage in status-definitional conduct free from normalizing governmental interference").

[333] Crocker, *supra* note 28, at 23–25.

[334] *Id.* at 25–27.

[335] *Id.* at 25–26.

[336] *Id.* at 28–32; *see also* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2092 (2001) ("To equate privacy with dignity is to ground privacy in social forms of respect that we owe each other as members of a common community.").

[337] *Compare supra* notes 289–336 and accompanying text (discussing privacy under the Due Process Clauses and the First Amendment), *with supra* notes 49–106 and accompanying text (discussing privacy under the Fourth Amendment).

[338] *See supra* note 337.

[339] Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1118–19 (2006) (noting that interpersonal or expressive privacy considerations may be helpful in working through the disclosure issues with the Third Party Doctrine); *see also* Penney, *supra* note 28, at 236–37, 240–42 (discussing the importance of interpersonal privacy in virtual space as a means of self-expression). Scholars have raised First Amendment and right to association issues in the context of government surveillance on the Internet. *See, e.g.*, Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 794–812 (2008); Peter Swire, *Social Net-*

Thomas Crocker provides a comprehensive analysis of how interpersonal privacy meshes with the Third Party Doctrine.[340] He finds that these two concepts are ultimately at odds with one another.[341] He argues that the narrow conception of privacy as secrecy under the Fourth Amendment fails fully to recognize the value of interpersonal relationships guaranteed under the Due Process Clauses.[342]

Crocker begins by explaining the implications of the Third Party Doctrine and the risks we undertake when we communicate with others:

> Whenever we communicate with others through speech or writing, they may repeat our words, thoughts, and meanings in contexts and to others in ways we may neither intend nor desire. More particularly, we assume the risk that in sharing, other persons will take our words to have legal significance—as evidence of criminal wrongdoing or political dangerousness—and repeat them to an officer of the State.[343]

Whenever people communicate with another person, they assume the risk that this person may reveal the information to the government.[344] Crocker recognizes that it does not matter that a person may limit what he or she wants the other person to do after receiving the communication.[345] That person has no control over what the other person may do with the information or to whom the other person reveals it.[346] In fact, this principle is central to the role of a confidential informant. This is

---

works, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment, 90 N.C. L. Rev. 1371, 1383–96 (2012). These scholars have argued that the First Amendment should apply when considering the permissibility of government surveillance of online communications (e.g., data mining). *See, e.g.*, Strandburg, *supra*, at 794–95; Swire, *supra*, at 1383–96. These scholars also focus on an individual's right of association under the First Amendment, and how government surveillance may adversely impact this right. *See, e.g.*, Strandburg, *supra*, at 801–04; Swire, *supra*, at 1395–96.

My aim is qualitatively different. This Article focuses on relationship formation over the Internet and how the concept of interpersonal privacy (embodied by both First Amendment and due process principles) provides a Fourth Amendment justification for why the Third Party Doctrine should not apply to Facebook relationships and their constituent communications.

[340] Crocker, *supra* note 28, at 32–48.

[341] *Id.* at 46–48.

[342] *See id.*

[343] *Id.* at 33.

[344] *Id.*

[345] *Id.*

[346] Crocker, *supra* note 28, at 33; *see, e.g.*, United States v. Jacobsen, 466 U.S. 109, 117 (1984); United States v. Miller, 425 U.S. 435, 443 (1976).

someone who, by design, gains an individual's trust (perhaps by deception) with the intention of gathering pertinent communication from the target and revealing it to the government.[347] As previously discussed, the Fourth Amendment would provide no protection to the communication that was disclosed to the government informant.[348]

Crocker goes on to argue that this risk of disclosure under the Third Party Doctrine to an undercover agent undermines the principles behind interpersonal privacy rights.[349] How can the government protect a liberty interest as it pertains to interpersonal relationships when communications in these relationships are not guaranteed to be private? In making this point, Crocker focuses on the connection between the individual liberty interest and relationships.[350] He argues:

> [S]ocial practices are more accurately understood as particular ways of obtaining personal fulfillment through shared social life that produce particular conceptions of privacy. Privacy's role in ordinary social practice is fluid and relational. No doubt, privacy sometimes means undisclosed, but not always. If we recognize how our lives are shaped through social practices of sharing, it is odd to equate the fact that "our observable actions and possessions are private at the discretion of those around us" with an actual fact of publicity . . . .[351]

Take again the scenario from *Lawrence*. The rationale for invalidating a sodomy law was the importance of this interpersonal relationship and the autonomy interest associated with it.[352] In short, this was a personal relationship where the government had no business to inter-

---

[347] *See* On Lee v. United States, 343 U.S. 747, 750–53 (1952).

[348] *See supra* notes 49–106 and accompanying text. In *United States v. White*, Justice William O. Douglas provided an impassioned dissent on this issue. 401 U.S. 745, 756–68 (1971) (Douglas, J., dissenting). He found that the monitoring of conversations by an informant "kills free discourse and spontaneous utterances." *Id.* at 762. He recognized that the "individual must keep some facts concerning his thoughts within a small zone of people." *Id.* at 763. Yet, Justice Douglas observed that:

> [a]t the same time he must be free to pour out his woes or inspirations or dreams to others. He remains the sole judge as to what must be said and what must remain unspoken. This is the essence of the idea of privacy implicit in the First and Fifth Amendments as well as in the Fourth.

Id.

[349] Crocker, *supra* note 28, at 47–48.

[350] *Id.*

[351] *Id.* at 47 (citing Georgia v. Randolph, 547 U.S. 103, 133 (2006) (Roberts, C.J., dissenting).

[352] *See Lawrence*, 539 U.S. at 567.

vene.[353] On these facts, it also stands to reason that one individual would not want communications to his or her partner to be disclosed outside the relationship. Indeed, privacy of communications would seem to be part and parcel of the relationship. As Crocker states, "It is evident then that our form of life is constituted through acts of sharing with particular others—intimate partners, family members, friends, or associates—which we do not intend or expect to become acts of sharing with the world at large."[354] Yet, it would not be unconstitutional for a governmental informant to pose as one of these individuals, in an effort to elicit incriminating statements, even if these statements were made in the confines of a relationship.[355]

Here then stands the opposing normative structure of these two constitutional doctrines. One paradigm—embodied through cases like *Lawrence*, *Dale*, and *U.S. Jaycees*—values interpersonal relationships. Interpersonal privacy seeks to protect interpersonal relationships from government intrusion.[356] To be sure, the Court's focus on the value of relationships stands as the very reason why the government cannot prohibit intimate conduct or restrict the use of contraception.[357] The other paradigm—one stemming from the Fourth Amendment—works against this structure.[358] It does not protect communications made by an individual to an undercover government agent with whom there is a shared relationship.[359] By intruding in the relationship, the state curtails a private citizen's ability to develop his or her identity and to form a true interpersonal bond.[360] Indeed, the only way to assure nondisclosure to the government is to avoid making the communication.[361] This means that the Fourth Amendment does not take into account the relational status of the parties in which the communication is made.[362]

---

[353] *See id.*

[354] Crocker, *supra* note 28, at 53.

[355] *See Miller*, 425 U.S. at 443. Crocker seems to recognize that not all disclosures made to a government informant would occur in the context of a relationship where liberty interests are implicated. *See* Crocker, *supra* note 28, at 67 ("When a government informant is placed among a mixture of close business associates and friends, the nature of the relationship becomes less clear. Such informants can become particularly vexing when they invade not only close personal relationships, but also when they implicate protected civic and political associations. In such cases, courts may have to conduct a more fine-grained analysis to determine if liberty interests are implicated . . . .").

[356] Crocker, *supra* note 28, at 21.

[357] *Id.*; *see Lawrence*, 539 U.S. at 567; *Griswold*, 381 U.S. at 485.

[358] Crocker, *supra* note 28, at 47–48.

[359] *See Miller*, 425 U.S. at 443; *On Lee*, 343 U.S. at 750–53.

[360] Crocker, *supra* note 28 at 51–52.

[361] *See Miller*, 425 U.S. at 443.

[362] *See* Crocker, *supra* note 28, at 47–48, 51–52.

Crocker finds that this problem perhaps is most visible in today's technology-oriented world.[363] He mentions the prevalence of cell phones and the government's ability to monitor such devices and to track a person's location.[364] He also references social networking sites, such as Facebook, and the government's ability to monitor these websites using an alias.[365] Presumably, the point here is that although none of these communications is protected by the Fourth Amendment under the Third Party Doctrine, each facilitates the development of interpersonal relationships—the very type of conduct protected by due process and First Amendment principles.

Crocker concludes his argument by discussing ways that interpersonal privacy considerations can be incorporated into the application of Fourth Amendment principles when it comes to this type of government intrusion.[366] He proposes, for instance, that authorities should first gather the consent of all parties or otherwise seek a warrant in order to acquire the relevant communication within a personal relationship.[367]

Crocker's overall point is valid. There does appear to be some tension between interpersonal privacy and the privacy guaranteed under the Fourth Amendment as it pertains to government intrusion. On the one hand, interpersonal privacy seeks to protect and encourage interpersonal bonds. On the other, the Fourth Amendment allows the government to infiltrate these bonds to gather information.

That said, in another important way, these privacy rights protect different things. The Fourth Amendment—as it relates to third party disclosure—primarily regulates communications, whereas interpersonal

---

[363] *Id.* at 53–56.

[364] *Id.* at 54.

[365] *Id.* at 53–54. Crocker seems to have in mind the government's ability to pose as a Facebook friend and thereby to monitor an individual's posts. *See id.* The Fourth Amendment would not protect information disclosed to this "friend." *See* Semitsu, *supra* note 62, 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). The Fourth Amendment would also not protect one Facebook friend forwarding information to a government agent. *Id.* at 344–46. But, because of the Third Party Doctrine, these messages would already not qualify for Fourth Amendment protection given that these messages are stored privately. *See supra* notes 114–129 and accompanying text.

[366] Crocker, *supra* note 28, at 62–68.

[367] *Id.* at 66–68. Crocker makes allowances for exigent circumstances, where a warrant would not be feasible. *See id.* at 67 (noting that under the proposed framework, the government cannot enter into protected interpersonal relationships without a warrant, unless it has consent or satisfies an established exception to the warrant requirement); *supra* note 54 (summarizing the warrant exceptions).

privacy focuses on essential elements of interpersonal relationships.[368] Under interpersonal privacy, the government cannot prohibit a person or small group's ability to define its relationship the way it sees fit because these choices strike at the heart of a relationship.[369] Not protecting communications made to a government informant would certainly seem to deter individuals from forming these relationships for fear that agents may be posing as prospective intimates.[370] But this lack of protection for communications—and any resulting deterrence—does not appear endemic to the relationship. In other words, the government is not interfering with any essential aspect of the relationship. Individuals are free to form relationships with whomever they choose. Invoking interpersonal privacy thus does not alter the Fourth Amendment reasonable expectation calculus.

One might argue that by not protecting communications, the government is effectively restricting a person's ability to trust another person.[371] Although most would agree that trust is an essential part of any relationship, it does not follow that the government is interfering with this element of a relationship when it seizes the communication without probable cause or a warrant. To be sure, a person may betray another's trust, even if they are not working as an informant or otherwise affiliated with the government. Indeed, to restrict a person's ability to do so would interfere with the recipient's autonomy or liberty.[372] A person thus always assumes the risk that the other person may reveal secrets to somebody else.[373] The insertion of the government here does not sub-

---

[368] *Compare supra* notes 76–106 and accompanying text (discussing the Third Party Doctrine), *with supra* notes 289–336 and accompanying text (discussing interpersonal privacy rights). The Fourth Amendment's reasonable expectation of privacy test also protects tangible objects such as papers and effects. *See Miller*, 425 U.S. at 441–43 (holding that there is no legitimate expectation of privacy in checks and deposit slips).

[369] *See Lawrence*, 539 U.S. at 567; *Dale*, 530 U.S. at 656; *Griswold*, 381 U.S. at 485.

[370] For this reason, some scholars have suggested a more relational account of the Fourth Amendment that would protect these statements under the reasonable expectation of privacy test. *E.g.*, Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 Calif. L. Rev. 1593, 1651–58 (1987). The Court, of course, has not adopted such an approach. *See supra* notes 49–106 and accompanying text.

[371] Crocker seems to make this point. *See* Crocker, *supra* note 28, at 52 ("[W]ith interpersonal relations, each person is reciprocally vulnerable to the other. This condition does not exist when the State occupies the position of the other. . . . [There,] the State attempts to control the conditions of an otherwise intimate or associational interaction, with its power to participate as the non-reciprocal other.").

[372] This would most likely run afoul of basic First Amendment principles.

[373] In fact, even if one argued that the Fourth Amendment should prevent undercover agents from gathering and using incriminating communications from potential suspects,

stantially alter this risk calculus—the risk of betrayal is inherent in any relationship.[374] In other words, although individuals may be deterred from entering such relationships for fear that the government is playing the role on the other side of the relationship, the government's ability to pose as the person in the relationship does not prohibit or otherwise restrict an essential part of it.[375]

Still, the concept of interpersonal privacy does have particular relevance to social networking on the Internet and the issue of third party disclosure. A more nuanced argument, though, is necessary—one that focuses on the relationship between Facebook users created by these communications and the role (or lack of it) that ISPs play in this relationship creation.

IV. Facebook Relationships and Interpersonal Privacy Rights

This Part argues that given the nature of relationships created through social networking sites, the interpersonal privacy doctrine provides a mechanism for protecting those communications.[376] This Part uses Facebook as an example of how social networking communications would work under the interpersonal privacy doctrine.[377] Section A discusses how online relationships through Facebook mimic face-to-face relationships.[378] Section B applies interpersonal privacy principles to Facebook communications and considers under what circumstances these communications are most likely to be protected.[379] Section C analyzes whether social networking communications would be covered un-

---

this relational account would still not prevent a citizen unaffiliated with the government from disclosing voluntarily what was learned to government authorities.

[374] *See* Hoffa v. United States, 385 U.S. 293, 302 (1966); Semitsu, *supra* note 62, at 330–31 ("Under [the misplaced trust doctrine], a person who mistakenly places her trust in someone who turns out to be an informant or government agent does not maintain any privacy rights under the Fourth Amendment.").

[375] A similar difficulty befalls those scholars who argue for First Amendment protection and the right of association as a check on government surveillance of Internet communications. *See* Strandburg, *supra* note 339, at 795–812; Swire, *supra* note 339, at 1383–96. The potential chilling effect of undercover government informants would seem to apply to both online and conventional face-to-face relationships. This focus on First Amendment protection would militate in favor of protecting these statements, which the Court has not done. *See supra* notes 49–106 and accompanying text. This Article does not support such a drastic conclusion, and indeed maintains that the Third Party Doctrine remains an important feature of Fourth Amendment jurisprudence and an essential law enforcement tool, both online and offline.

[376] *See infra* notes 382–488 and accompanying text.

[377] *See infra* notes 382–488 and accompanying text.

[378] *See infra* notes 382–423 and accompanying text.

[379] *See infra* notes 424–470 and accompanying text.

der the reasonable expectation of privacy test given their intersection with interpersonal privacy.[380] And, finally, Section D provides a hypothetical to illustrate how (and which) Facebook communications would be protected.[381]

A. *The Nature of Facebook Relationships*

As previously mentioned, Facebook allows users to send e-mails, post photos and status updates, and send instant messages, among other things.[382] Facebook recently added video conferencing to its list of features.[383] All profiles now also follow a timeline-based format, which chronologically details each user's history on the site, including the user's prior posts, photographs, places the user has been, and other content.[384]

A simple accounting of these various features, however, belies the true impact and reach of Facebook. Facebook has revolutionized the way individuals communicate and develop social relationships.[385] It is no surprise that over one billion users across the world are members of the site, requiring a continuous increase in storage facilities to accommodate the massive amounts of information being transmitted over the Internet.[386]

Social scientists and legal scholars alike have recognized this new form of communication and analyzed its social implications.[387] As one

---

[380] *See infra* notes 471–479 and accompanying text.

[381] *See infra* notes 480–488 and accompanying text.

[382] *See supra* notes 118–121 and accompanying text.

[383] *See Video Calling: Basics & Privacy*, *supra* note 119.

[384] *See Get Started: Introducing Timeline*, Facebook, https://www.facebook.com/help/467610326601639/ (last visited Dec. 22, 2012).

[385] *See generally* 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/ (discussing the ways in which Facebook has altered friendship formation).

[386] *See* Miller, *Facebook Makes Big Investment*, *supra* note 120 (discussing the increase of Facebook storage facilities); *Key Facts*, *supra* note 18 ("One billion monthly active users as of October 2012.").

[387] *See, e.g.*, Bargh & McKenna, *supra* note 37; 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 (2007); Charles Steinfeld et al., *Social Capital, Self-Esteem, and Use of Online Social Networking Sites: A Longitudinal Analysis*, 29 J. Applied Developmental Psychol. 434 (2008); Stephanie Tom Tong et al., *Too Much of a Good Thing? The Relationship Between Number of Friends and Interpersonal Impressions on Facebook*, 13 J. Computer-Mediated Comm. 531 (2008); 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 (2002); Mihaela Vorvoreanu, *Perceptions of Corporations on Facebook: An Analysis of Facebook Social Norms*, J. New Comm. Res.,

sociologist writes, "Facebook has created unique and different way[s] for [individuals] to develop and maintain friendships via the internet, no matter the physical distance."[388] The ability to create new relationships and maintain them probably stands as the most significant function of this kind of social networking.[389]

Psychologists have found that for some individuals, most notably college students, Facebook has replaced physical interactions as a means of developing and sustaining relationships.[390] In this way, Facebook has filled an important social need by allowing individuals to express themselves in ways they may not be able to in face-to-face meetings. Facebook provides 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."[391] Indeed, one study found that individuals expressed their true selves more freely over social networking sites than in face-to-face encounters.[392]

The overall effect is interaction with others on a consistent basis without regard to physical presence or distance.[393] Critical to this conclusion is the corollary finding by psychologists that Facebook relationships can be just as "real" as those relationships that take place in face-to-face meetings.[394] These studies show that Internet relationships on Facebook share the same breadth, depth, and quality as those developed in person.[395]

Spring/Summer 2009, at 67; 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; Bareham, *supra* note 385.

[388] Bareham, *supra* note 385, at Introduction ("Today, practically everyone has a Facebook [profile] and interacts daily online forming and creating relationships. It truly has become a new way to make friends and meet people. We are so accustomed to meeting people and having to develop relationships face to face, but with the Internet it has made friendship and social interaction available practically anywhere.").

[389] Ellison et al., *supra* note 387, at 1162–63.

[390] Bargh & McKenna, *supra* note 37, at 580–82; Vitak, *supra* note 387, at 4–5; Bareham, *supra* note 385, at Discussion Section.

[391] *See* Tyler, *supra* note 387, at 200–01 (citing 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)).

[392] Bargh et al., *supra* note 391, at 44–46.

[393] Bareham, *supra* note 385, at Introduction ("This site has become and [sic] important component to these college students[']lives, and has allowed them to create connections and share information with those in close proximity to them in college.").

[394] *See* Bargh et al., *supra* note 391, at 44–46; Bargh & McKenna, *supra* note 37, at 581.

[395] *See, e.g.*, Bargh & McKenna, *supra* note 37, at 581.

At least one scholar, James Grimmelmann, has also recognized the similar qualitative structure of Facebook relationships and their more traditional face-to-face counterparts.[396] Relying on social and psychological studies, he cites to three ways Facebook promotes social dynamics and interpersonal values.[397] Grimmelmann argues that "Facebook provides users with a forum in which they can craft social identities, forge reciprocal relationships, and accumulate social capital."[398]

Social identity—Grimmelmann's first factor—is how one presents oneself to others.[399] The basic desire to "convince others to accept your claims about yourself" is common to all social interactions.[400] According to Grimmelmann, social networking sites like Facebook facilitate this need of identity construction by allowing users to create the identities they want.[401] Users have full control over what pictures to post and what information to include on their profile. These profiles thus are wholly socially constructed—controlled pieces of information for others to see. In technical terms, Facebook allows users to communicate "prestige, differentiation, authenticity, and theatrical persona using a common language."[402]

Grimmelmann's second factor focuses on the aforementioned ability of Facebook to create and maintain relationships.[403] He writes that social networks are "a way for users to meet new people" as well as "help in the transmission of social cues that facilitate offline transactions."[404] Grimmelmann is quick to point out the unique relationship building features of Facebook that set it apart from traditional e-mail

---

[396] *E.g.*, Grimmelmann, *supra* note 222, at 1154–56.

[397] *Id.* at 1151–60.

[398] *Id.* at 1151. Grimmelmann cites to a number of studies in his article. *See, e.g.*, Erving Goffman, The Presentation of Self in Everyday Life (1959); Sherry Turkle, Life on the Screen: Identity in the Age of the Internet (1995); Danah Boyd, *None of This Is Real: Identity and Participation in Friendster*, *in* Structures of Participation in Digital Culture, at 132 (Joe Karaganis ed., 2007); Judith Donath & Danah Boyd, *Public Displays of Connection*, BT Tech. J., Oct. 2004, at 71; Hugo Liu, *Social Network Profiles as Taste Performances*, 12 J. Computer-Mediated Comm. 252 (2007); Tong et al., *supra* note 387; Patti M. Valkenburg et al., *Friend Networking Sites and Their Relationship to Adolescents' Well Being and Social Self-Esteem*, 9 Cyberpschology & Behav. 584 (2006); Clive Thompson, *I'm So Totally, Digitally Close to You*, N.Y. Times, Sept. 5, 2008, (Magazine), at 42; Alex Williams, *Here I Am Taking My Own Picture*, N.Y. Times, Feb. 19, 2006, § 9, at 1 (quoting various experts).

[399] Grimmelmann, *supra* note 222, at 1152.

[400] *Id.*

[401] *Id.* at 1152–53.

[402] *Id.* at 1152 (internal quotation marks omitted).

[403] *Id.* at 1154–56.

[404] *Id.* at 1154.

systems that merely allow back-and-forth messaging.[405] He specifically cites to a user's ability to add someone as a contact—a fundamental act that gives someone access to the user's profile, and thus provides "a form of minor intimacy that signals trust."[406] Grimmelmann goes on to cite other Facebook features that foster the development of relationships, including the ability to "Poke" someone or to write on another user's wall.[407]

This discussion leads to Grimmelmann's final point about reciprocity. What makes Facebook such a powerful relationship-building tool is its ability to encourage users to respond or otherwise engage in a mutual dialogue.[408] This is embodied in two features: the wall-to-wall tool, which displays the back-and-forth between two users; and the status update tool, which prompts a user to ask "What is on your mind?" and also displays recent answers by fellow Facebook friends.[409] These tools promote a person's existing and "deeply wired human impulse to reciprocate" and "activate relational impulses."[410]

The third factor centers on the community building aspect of social networking sites such as Facebook.[411] Grimmelmann makes the initial observation that Facebook use begets Facebook use.[412] Individuals are more likely to sign up for the service if they see their friends signing up for it.[413] Also, there is the "networked space" of Facebook that allows users to recreate a real-life social network in a virtual space.[414] This structure also provides an inducement for users to extend their network by "friending" more individuals.[415]

---

[405] *See* Grimmelmann, *supra* note 222, at 1154–55; *see also supra* notes 118–121 and accompanying text (discussing Facebook's features).

[406] Grimmelmann, *supra* note 222, at 1155.

[407] *Id.* at 1155.

[408] *Id.* at 1155–56.

[409] *Id.*

[410] *Id.* at 1156.

[411] *Id.* at 1157–60.

[412] *See* Grimmelmann, *supra* note 222, at 1157.

[413] *Id.*

[414] *Id.* at 1157–58.

[415] *Id.* at 1158. Grimmelmann discusses the power of adding individuals as Facebook friends:

> This navigational pleasure also provides an inducement to extend your social horizon. . . . If you add Seth as a contact, all of his contacts are now contacts-of-contacts of yours—and all of your contacts are now contacts-of-contacts of his. Adding connections fills out your social map, giving you a richer view of your social context.

Id.

This sense of community is further enhanced because users are allowed to stake out a social position within their network.[416] Users, for instance, can compete for who has the most contacts, which translates into "social currency."[417] More directly, many Facebook applications take the form of competitive games.[418] Users can post their highest scores for all to see and prompt their Facebook friends to compete in an attempt to best their performance. This type of competitive spirit fosters a community-building environment where individuals—much like in the real world—posture for certain positions.[419] One Facebook application even allows users to place price tags on their friendships.[420]

It is important to note that Grimmelmann's point is ultimately one about human desire.[421] These three qualities—identity, relationship, and community—are not unique to social networking sites; they are "basic elements of social interaction, offline and on."[422] Social networking sites, like Facebook, simply provide a structure under which individuals can satisfy these impulses in a virtual setting.[423]

B. *Protecting Facebook Relationships*

Protecting the sanctity of interpersonal relationships from government intrusion stands at the heart of the cases involving interpersonal privacy rights.[424] These rights are aimed at constructing a zone of privacy where individuals have the freedom to enter relationships and, just as importantly, define them the way they see fit. If Facebook relationships have a similar qualitative structure as face-to-face relationships, it stands to reason that they too should merit privacy protection, despite the disclosure to ISPs. The purpose here is simply to put these

---

[416] *Id.* at 1158–59. Social scientists have also recognized how Facebook creates and maintains an individual's social capital. *See* Ellison et al., *supra* note 387, at 1161–64; Steinfeld et al., *supra* note 387, at 443–44.

[417] Grimmelmann, *supra* note 222, at 1158 ("[Adding Facebook friends makes] you yourself more valuable as a contact, since by connecting to you, others can expand their own horizons.").

[418] *Id.*

[419] *See id.* at 1158–59.

[420] *Id.*

[421] *Id.* at 1159.

[422] *Id.*

[423] *See* Grimmelmann, *supra* note 222, at 1159. 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.

[424] *See supra* notes 305–336 and accompanying text.

Internet relationships on the same footing as face-to-face relationships when it comes to Fourth Amendment protection.[425]

1. Applying the Concept of Interpersonal Privacy

Facebook relationships and their underlying communications pass the reasonable expectation of privacy test, despite the disclosure to ISPs.[426] As previously discussed, the reasonable expectation test is objective in nature and requires courts to determine whether the particular communication merits privacy protection from government intrusion.[427] Before invoking interpersonal privacy, however, an analysis as to why, and in what way, the concept of interpersonal privacy applies to Facebook relationships and to their underlying communications is required.

In short, both kinds of relationships—those over the Internet and those that are face-to-face—foster the same principles of autonomy, identity, and community. As one scholar argues, "*Lawrence*, [*U.S. Jaycees*], and *Dale* are all cases protecting different kinds of interpersonal relationships that are both expressive and identity definitional."[428] This description of interpersonal privacy would also squarely include Facebook relationships.

There are, however, key differences. Interpersonal privacy rights typically involve face-to-face relationships that occur in a person's home.[429] The physical presence requirement is almost a nonstarter. It is certainly true that Facebook relationships do not take place in face-to-face settings, like in a person's home. But why should that matter, at least from a normative point of view? Because a Facebook relationship can be entirely online, the communications themselves take on a more important role—they alone make up the relationship. So it does not make sense to focus on essential physical "acts" when talking about the concept of interpersonal privacy in the online context, because relationships in this medium have no physical "acts" in the conventional

---

[425] This Article does not argue that these relationships actually merit substantive due process or First Amendment protection. The fact that I am not arguing for actual constitutional protection based on due process or First Amendment grounds means Facebook relationships do not have to be exactly the same when it comes to the aforementioned qualities. It is enough that these relationships share similar structures with their face-to-face counterparts.

[426] *See infra* notes 427–470 and accompanying text.

[427] *See supra* notes 64–73, 129 and accompanying text.

[428] Crocker, *supra* note 28, at 21.

[429] *E.g.*, Lawrence v. Texas, 539 U.S. 558, 578 (2003); Griswold v. Connecticut, 381 U.S. 479, 481–86 (1965).

sense of the term.[430] Indeed, much like the aforementioned Fourth Amendment scholarship that seeks to update the Third Party Doctrine to the Internet context,[431] the point here is to use the concept of interpersonal privacy to protect communications in this new medium.

Focusing on intimate acts alone also does not necessarily assail this conclusion. In the first instance, the Supreme Court in *Lawrence v. Texas*, in 2003, although it prohibited Texas's sodomy law, invoked the principles of autonomy and interpersonal relationships in reaching its conclusion, and thus it was not simply a case about sex.[432] For instance, a law against same-sex friendships would also run afoul of *Lawrence*, even though there would be no prohibition against sex.[433]

Second and equally important, because this Article defines interpersonal privacy broadly, it does not argue that such a term is simply reserved for relationships involving intimate conduct. Indeed, the Supreme Court, in *Roberts v. U.S. Jaycees* in 1984 and *Boy Scouts of America v. Dale* in 2000, relied on equal protection and First Amendment principles to argue for the general ability of individuals and expressive groups to define their relationships free from government interference.[434] The *Dale* case, for example, involved a group that wanted to self-define its membership the way it saw fit.[435] The Court recognized this right relying on interpersonal privacy considerations, even though the relationship did not involve intimate acts of any kind.[436]

The fact that Facebook relationships occur in "cyberspace" should also not change the analysis. Assuming this is a public space, there is

---

[430] One may argue that because of this fact alone, interpersonal privacy *a fortiori* has no role to play in the online context when discussing Fourth Amendment protection. But this begs the question of why physical acts alone would be worthy of protection. Presumably, the reason is because they alone are essential to the relationship. In the online context, however, communications alone are constituent of the relationship, and thus necessarily are essential to it.

[431] *See supra* notes 130–209 and accompanying text.

[432] *See Lawrence*, 539 U.S. at 573–74; *supra* notes 306–316 and accompanying text.

[433] This Article also does not seek to apply substantive due process to Facebook communications, and thus does not need to confine itself to the narrow holding of *Lawrence*. Furthermore, although Facebook does not allow sexual-based posts or photographs, one can imagine a platform in the future that would allow such interactions, which would make the narrow holding in *Lawrence* more readily applicable. *See Statement of Rights and Responsibilities: Safety*, *supra* note 120 ("You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.").

[434] *See* Boy Scouts of Am. v. Dale, 530 U.S. 640, 648, 656–59 (2000); Roberts v. U.S. Jaycees, 468 U.S. 609, 617–29 (1984); *supra* notes 305–375 and accompanying text.

[435] *Dale*, 530 U.S. at 647–61.

[436] *See id.*

precedent under *Dale* that identity formation in public is protected.[437] But it is not clear that Facebook relationships take place in a public arena.[438] To be sure, the relationship is not face to face. Yet, this fact alone does not automatically mean that the virtual space in which this relationship is taking place automatically becomes a public arena or public space.[439] For one thing, communications over Facebook are private insofar as only the intended recipient or an individual's group of friends will see it.[440] This is very different from a communication made in the open or in a public setting where there would be no such subjective expectation of privacy.[441] Second, there appears to be no conceptual reason why Internet—or at least the virtual space in which communications are transmitted—is not better seen as a private space, perhaps as an extension of a person's home or office.[442] Public or not, Facebook relationships can embody the same essential qualities as traditional relationships, thus justifying the notion of protecting these relationships from government intrusion in the Fourth Amendment context.

There is an additional element to the interpersonal privacy cases that is distinguishable in the Facebook context. In each of the aforementioned interpersonal privacy cases, the Supreme Court struck down the government's ability to interfere with relationships or a person's ability to define them: in *Roe v. Wade*, this meant overturning a govern-

---

[437] *See id.* (holding that requiring the Boy Scouts to employ a homosexual male as a scoutmaster violated the Boy Scouts' First Amendment right of expressive association).

[438] *See* Steven G. Gey, *Reopening the Public Forum—From Sidewalks to Cyberspace*, 58 Ohio St. L.J. 1535, 1611–17 (1998) (discussing the Internet as a potential public forum); Lyrissa Lidsky, *Public Forum 2.0*, 91 B.U. L. Rev. 1975, 1995 (2011) ("It is hardly a stretch to characterize an interactive social media site as a public forum when it is designed explicitly for providing a locus of discussion and debate."). A rigorous analysis of the Internet as a public or private forum is beyond the scope of this Article.

[439] Under a strict application of the Third Party Doctrine, this conclusion may make sense. Because there is no reasonable expectation of privacy in communications over the Internet, this virtual space is better viewed as a public forum.

[440] As previously discussed, however, a subjective expectation of privacy does not dictate whether such communication deserves Fourth Amendment protection. *See supra* notes 107–129 and accompanying text.

[441] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (stating that "conversations in the open would not be protected against being overheard") (citation omitted); Lee Tien, *Cheap Surveillance, Essential Facilities, and Privacy Norms*, 199 Stan. Tech. L. Rev. 10, at *8–9 (1999).

[442] The technosocial continuity theory makes this very point by arguing that the Internet and virtual media can be seen as an extension of the home or office. *See* Strandburg *supra* note 25, at 654–64. This is different from when a person voluntarily makes public his or her Facebook profile and/or other posts.

ment ban on certain types of abortions;[443] in *Lawrence*, this meant overruling a state's ban on sodomy;[444] and in *Dale*, this meant preventing the government from prohibiting private groups from excluding certain individuals.[445] In the Facebook context, however, there is no positive law at issue. Instead, the government simply seeks to acquire the information for law enforcement purposes. Nevertheless, this should not alter how we apply the concept of interpersonal privacy to Facebook relationships. Much like in the face-to-face context, the government's ability to acquire Facebook communications would have similar deleterious effects when it comes to relationship formation over the Internet.[446] Moreover, finding Fourth Amendment protection does not thwart the government's interest because it preserves its ability to collect information. Indeed, unlike the interpersonal privacy cases that foreclosed the government from employing the specific legislation, here, the government remains free to acquire the information as long as they have probable cause and a warrant.[447]

2. Contexts for Protecting Facebook Communications Under Interpersonal Privacy

In order to examine the application of the concept of interpersonal privacy to Facebook relationships and the Fourth Amendment, the context to which that framework is applicable must be addressed. Would this concept apply to all Facebook communications? Does it matter if the communication is directed to one individual (or small group of individuals) or a person's entire Facebook friend network?

First, any such concept of interpersonal privacy should apply only to communications that constitute a "relationship"—one that fosters identity, autonomy, and community.[448] Second, how extensive that relationship is should factor into the analysis. The associations articulated in *U.S. Jaycees* may be instructive (though not dispositive) on whether a particular relationship merits protection.[449] Under that framework, if the communications taken as a whole indicate the type of relationship where a person shares "not only a special community of thoughts, experiences, and beliefs but also distinctively personal aspects of one's

---

[443] 410 U.S. 113, 162–64 (1973).
[444] 539 U.S. at 567, 578.
[445] 530 U.S. at 659.
[446] *See supra* notes 337–375 and accompanying text.
[447] *See* U.S. Const. amend. IV; *supra* notes 289–336 and accompanying text.
[448] *See supra* notes 340–367 and accompanying text.
[449] *See supra* notes 305–336 and accompanying text.

life," this would suggest the type of association that should be protected.[450] Thus, ongoing Facebook communications—including messages, posts, videos, and photographs—to a single person or small group of persons would probably constitute a relationship. By contrast, an isolated Facebook message to a user with whom there has been little prior contact probably would not constitute a relationship.[451] Similarly, business-related messages—no matter how frequently exchanged—would not contain the deep attachment and commitments indicative of a relationship worthy of protection.

3. The Role of Third Party Servers in Facebook Relationships

A key issue remains in this argument. Why do communications over Facebook merit privacy vis-à-vis the concept of interpersonal privacy when their face-to-face counterparts would not receive such protection, in light of similar considerations? Facebook relationships may indeed have the same qualitative structure of face-to-face relationships. But, as discussed earlier, communications made to another person in a face-to-face setting—even in the context of a bona fide "relationship"—do not merit privacy protection, and the other person is free to disclose the information to the government.[452] Although interpersonal privacy focuses on preventing the government from interfering with essential aspects of a relationship, individuals assume the risk when they disclose communications to a third party—regardless of whether the recipient is a government informant.[453]

Facebook relationships work differently. Third party servers are integral to the relationship in a way that they obviously are not with

---

[450] *See Roberts*, 468 U.S. at 620.

[451] *See supra* notes 382–425 and accompanying text. It is important to note here that Facebook recently implemented the ability to control what group or groups of people can view a user's status update or posted photograph. This makes it easy to communicate more regularly or to relay more personal information to a small group of individuals like close friends or family. Of course, many users post updates and photographs for all of their Facebook friends to see. This certainly would complicate any interpersonal privacy analysis. Should every communication to one's entire Facebook friend network constitute part of the relationship or just a select few? This type of close factual analysis is beyond the scope of this Article. Indeed, a full analysis would require further explanation of the contours of a Facebook relationship and exactly when a communication (e.g., post, e-mail, video) that is constituent of this relationship merits privacy protection. That said, the preceding is a compelling start to answering these questions. It is important to understand that the purpose of this Article is to begin the dialogue of applying the concept of interpersonal privacy to the Internet, not to be the last word on the subject.

[452] *See supra* notes 53–106 and accompanying text.

[453] *See supra* notes 114–129, 337–375 and accompanying text.

face-to-face communications. Face-to-face relationships and the underlying communications do not involve any third party server or other intermediary; individuals speak directly with other individuals. The recipient thus occupies dual roles. The recipient is both the potential government intrusion (i.e., a government agent) as well as part of the actual relationship. It makes sense then that there would be no interpersonal privacy consideration when analyzing the privacy of these communications and the government's ability to seize the information. As explained earlier, individuals assume the risk that the other person(s) in the relationship may reveal information to the government.[454] This risk is inherent in the nature of any relationship. Indeed, one may argue that the very qualities of a relationship—autonomy, identity, and community—require the potential risk of disclosure. For only with this possibility of betrayal can any resulting relationship be considered genuine or authentic.

The transmission of Facebook communications—and the corresponding risk involved—is qualitatively different. The relevant government intrusion can be conceptually separated from the Facebook relationship itself. The components of this relationship include three parts: the sender, the recipient (i.e., Facebook friend(s)) and the ISP (i.e., Facebook, the company). No doubt each of these elements is necessary for the relationship, but one can conceptually remove the element of government intrusion from the relationship itself.

The potential intrusion comes into play with the server from which the government can acquire the information free from constitutional restraint.[455] The reason of course centers on the Third Party Doctrine and the fact that these communications lose any expectation of privacy as a result of this disclosure.[456] Yet, the storage server or ISP is simply an intermediary who shares no part of the actual relationship. The server does not choose the communications or otherwise actively

---

[454] *See supra* notes 337–375 and accompanying text. One scholar seems to think that where the other person in a relationship is a government informant, the government has gone too far and violated a person's interpersonal privacy right. *See* Crocker, *supra* note 28, at 66–67. Yet, this scholar would have to acknowledge that if the other person voluntarily and independently (i.e., was not acting on behalf of the government) decided, after the fact, to reveal the communication to the government, there would be no protection. My point is that these two situations are identical, at least in terms of risk, and must stand or fall together. I take the position that such a risk is always present in a relationship, and thus any government intrusion does not change this basic calculus. Hence, interpersonal privacy considerations would not displace application of the Third Party Doctrine in either case.

[455] *See supra* notes 114–129 and accompanying text.

[456] *See supra* notes 114–129 and accompanying text.

participate in the relationship. It simply provides the "space" in which users can interact and develop relationships. In this way, the risk of government intrusion originates from something separate than the relationship. Why then should an individual user bear the burden of this additional risk, when the server—the source of risk—makes no substantive contribution to the relationship? The user should not. If society values the qualities inherent in Facebook relationships (as similar to those qualities in face-to-face relationships), it should protect these communications—as functions of the relationship—from this type of intrusion.

The technosocial theory seems to be on the right track with its argument about ISPs playing the role of middlemen.[457] These service providers facilitate communications between individuals much like landlords or other providers, but there is an important difference. Landlords, maids, and other service individuals play a role—albeit a small one—in the relationship between the two individuals for whom they facilitate communication. They may not have a stake or preferred outcome in the matter. Nevertheless, they are a part of the resulting relationship in that they form a mini-relationship (perhaps not to the same depth or quality) with the sender and/or the recipient. In other words, they are not *merely* conduits that transmit information. This is very different from ISPs, which play no comparable role. The ISP entity is just an intermediary mechanism transmitting the information. The fact that that the server is a computer machine further enhances this point.[458] No human interaction is taking place.[459] In short, there is no relationship between either the sender or the recipient and the third party server.

This analysis, however, does not change the dynamic between the sender and the recipient of the Facebook communication—this interaction mimics that of a face-to-face communication. Individuals on Facebook—like their offline counterparts—assume the risk that one or more of their Facebook friends may betray their trust and reveal their

---

[457] *See supra* notes 182–209 and accompanying text.

[458] *See supra* notes 139–164 and accompanying text.

[459] It would not matter if a Facebook employee "observed" the information for quality control or other related reasons. *See supra* notes 139–164 and accompanying text. Even here, the employee is in no way participating in the relationship or interacting with the sender or the recipient.

My theory can also help explain the postal exception to the Third Party Doctrine. *See supra* notes 165–209 and accompanying text. There, too, the postal worker serves simply as an intermediary between the sender and the recipient of the letter, and has no substantive interaction with the parties.

communication. Interpersonal privacy considerations have no role to play here. This risk is inherent in any relationship, online or offline. We must be wary before communicating confidential information to a Facebook friend in the same way we must be cautious before revealing information to another individual in a face-to-face interaction. There is nothing to stop an undercover informant from becoming a user's Facebook friend and acquiring purportedly confidential information.[460] This should not be surprising or alarming. As previously discussed, interpersonal privacy has no role here when applying the reasonable expectation of privacy test.[461] Unlike with the case of the third party sever, the Facebook "friend"—like the face-to-face counterpart—is part and parcel of the relationship. This risk of disclosure constitutes the necessary cost of engaging in this type of social interaction.[462]

4. Other Internet Communications

The preceding discussion of interpersonal privacy has focused on communications in the context of social networking relationships, such as through Facebook. It intentionally excluded reference to other Internet communications, most notably e-mails transmitted over Gmail or Hotmail.[463] These communications are more difficult to analyze. Because these communications follow the same pattern as Facebook communications—sender, non-participant third party server, and recipient—it might be deceptively easy to conclude that these communications likewise merit Fourth Amendment protection in light of interpersonal privacy considerations.[464] But there is a key difference. Facebook communications are constituent of the resulting relationship, whereas e-mail communications seem to simply facilitate their respective relationships.

---

[460] *See* Semitsu, *supra* note 62, at 322–24, 344–48 (providing a good discussion of the various ways police officers can infiltrate Facebook networks and acquire incriminating evidence, including instances where governmental officials create fake "online identities" to gain access to a user's Facebook communication).

[461] *See supra* notes 305–336 and accompanying text.

[462] A similar risk applies to those Facebook communications that are voluntarily made public to all users. Here, too, users take on the risk that someone may reveal the information to the government. *See* Semitsu, *supra* note 62, at 342–43 (noting that when a user's profile is public, the user has no reasonable expectation of privacy).

[463] This category would also include discrete Facebook communications that would not be considered as part of a Facebook relationship. *See supra* note 451 and accompanying text.

[464] *See supra* notes 114–129, 448–462 and accompanying text.

Put differently, e-mails are similar to telephone conversations or postal letters. People use these methods of communications to maintain preexisting relationships or begin the process of making new ones. But these communications are hardly considered replacements for face-to-face meetings. For instance, exclusively talking on the phone is typically not considered a complete relationship, or at least the type of relationship that fosters qualities such as autonomy, identity, or community. Conversations are better seen as supplementing face-to-face relationships.

The same reasoning applies to e-mails. Like phone conversations, these communications typically facilitate relationships. They only allow individuals to send and receive messages as a way to supplement their existing offline relationships.[465] Most individuals do not rely on this type of communication alone as a means to develop and maintain their relationships.[466] This means that the communication is not, strictly speaking, necessary for the relationship.

If e-mail communications are used exclusively, this probably means that the sender and the recipient function more like business associates or acquaintances.[467] Most would agree that this type of connection does not rise to the level of a relationship, or at least the kind of relationship that fosters the characteristics central to interpersonal privacy—identity, autonomy, and community. Indeed, no one really talks about a "Gmail relationship" or "Hotmail relationship." 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 communication for the online relationship.

This is not to say that the ability instantaneously to send and receive e-mails over great distances was not a qualitative technological leap. It certainly was. But in other ways, this type of communication remains conceptually no different than more traditional forms of communication. Postal letters also allow individuals to send and receive communications over great distances. Although the communication

---

[465] It is not clear that instant messaging via these sites changes the analysis. Even though these communications may occur in real-time, these communications would seem to be more similar to phone conversations than Facebook communications in that the former merely facilitate relationships.

[466] *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).

[467] These types of "relationships" would probably not rise to a level worthy of interpersonal privacy protection. *See* Crocker, *supra* note 28, at 22–32, 66–67.

takes longer to arrive, the basic concept remains the same—individual transmission of discrete messages.

This is what makes social networking sites so unique. For the first time in history, users have access to a wide variety of electronic tools—instant messages, posting of pictures, updates, videos—that can all be used in real-time. It is no wonder that social scientists and legal scholars alike have analyzed the unique social implications of this type of communication. The end result is a relationship that is just as real as a traditional face-to-face one. The myriad number of Facebook communication tools (and their resulting effect) differentiates this type of interface from traditional e-mail systems, which constitute the mere exchange of discrete messages. Facebook communications are necessary for the online relationship. Without these communications, there would be no relationship.

Not all communications over the Internet benefit from such interpersonal privacy considerations. A discrete e-mail sent to a business associate or acquaintance would lose all Fourth Amendment protection once it is disclosed to an ISP. This is an acceptable conclusion. The aim of this Article is to recognize the value of Internet relationships and protect the constituent communications, not seek to protect all communications over the Internet.[468] It also seems that incriminating statements would be most likely divulged in the context of relationships, requiring greater protection for these communications from unwarranted government intrusion.

There is room for debate here. The concept of interpersonal privacy could possibly apply to the Gmail or Hotmail communications, and thus serve as a means of overcoming the ISP disclosure problem. Perhaps, an individual has developed a real "relationship" using only Gmail e-mails sufficient to warrant constitutional protection. Or maybe interpersonal privacy considerations should be used to protect all Internet communications that facilitate preexisting relationships; this would still exclude discrete e-mails relating to work or business.[469]

---

[468] Other theories, including those already discussed, may be employed to justify why these communications merit Fourth Amendment protection despite disclosure to an ISP. *See supra* notes 130–209 and accompanying text. My account is not intended to be the only way communications over the Internet can merit protection. It simply represents one way to protect those social networking communications that are constituent of a bona fide relationship.

[469] Again, this business versus personal dichotomy loosely tracks the analysis in *U.S. Jaycees*. *See supra* notes 319–323 and accompanying text.

This would not substantially change the preceding analysis. My basic conclusion remains unassailed. There is a compelling argument to be made that interpersonal privacy considerations serve as a tool to explain why Facebook communications continue to merit Fourth Amendment protection, even though these communications are systematically disclosed to third party servers.[470]

C. *Reevaluating a Reasonable Expectation of Privacy Using Interpersonal Privacy*

Invoking interpersonal privacy in the Internet context thus provides a new way to evaluate a user's reasonable expectation of privacy—one that stands on constitutional principles—when it comes to Facebook communications. After the Supreme Court's 1967 decision, *Katz v. United States*, the objective part of the reasonable expectation test stands as the cornerstone of Fourth Amendment protection.[471] *Katz* defines this as an "expectation . . . that society is prepared to recognize as 'reasonable.'"[472] The appropriate inquiry is whether a court finds that privacy is warranted in this context. How "reasonable" is defined in this context is not a simple matter.[473] The Supreme Court has not adopted a single test for making this assessment.[474] One scholar argues that the Court in fact uses four conceptually different models—or a combination thereof—when making this assessment: two descriptive and two normative.[475] The two descriptive models focus on what a sensible person would do in the situation or whether the authorities have

---

[470] This conclusion does not disrupt how the law would analyze phone or postal communications. Under *Katz v. United States* and its progeny, the Fourth Amendment already protects these communications. *See* 389 U.S. at 353; *Ex Parte* Jackson, 96 U.S. 727, 733 (1877). The insertion of interpersonal privacy here would thus be superfluous.

Further, my analysis simply limits (not overrules) the holding in *Smith v. Maryland* to those transmissions disclosed to a machine that is not part of the relationship. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979); *supra* notes 90–106 and accompanying text. Because the phone numbers disclosed to the pen register are not substantive communications that are part of a relationship, under my theory, they would not garner special consideration using the concept of interpersonal privacy.

[471] *See supra* notes 64–73, 90–106 and accompanying text.

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

[473] *See* Kerr, *supra* note 54, at 504.

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

[475] Kerr, *supra* note 54, at 508.

violated preexisting law in conducting the search.[476] The normative principles focus on the nature of the information searched and policy implications behind allowing this type of search.[477]

As previously discussed, scholars have tried numerous ways—automation/human observation, content/non-content distinction, and technosocial continuity—to apply this test and conclude that the user's communications remain private despite the third party disclosure.[478] The merits of these decisions have already been discussed. Each of these theories—whether explicitly or implicitly—makes descriptive and normative assessments. What does a sensible Internet user think the role of service providers should be? Is there a qualitative difference between the information contained in the body of the e-mail and the information in the "to" and "from" lines? Can the user really disclose information and lose her privacy if the third party is a machine? These questions help assess whether a user has a reasonable expectation of privacy in these communications.

Importing interpersonal privacy into this discussion serves a similar function. It, too, invokes the application of the foregoing normative and descriptive tests. The benefit of using the concept of interpersonal privacy is that any of these various tests (either alone or in combination) would be satisfied, and one could persuasively conclude that a user has a reasonable expectation of privacy in his or her social networking communications.

Under a descriptive model, it makes sense to say that a reasonable Facebook user would expect the government not to intrude on her Internet relationships because these relationships are just as "real" as face-to-face relationships. Invoking interpersonal privacy also means that the government is contravening constitutionally entrenched principles—ones that seek to foster the interpersonal bonds in relationships—by intercepting these communications.

Normative principles also support an expectation of privacy. These communications are more than just discrete transmissions. Indeed, understood as simply a single transmission, any Facebook communication would appear to be no different than other communications voluntarily disclosed to a third party. But because this communication is understood as a necessary constituent of a resultant relationship—one where the ISP serves merely as an intermediary—an argument can be made

---

[476] *Id.* at 508–12, 516–19.

[477] *Id.* at 512–15, 519–22.

[478] *See supra* notes 130–209 and accompanying text.

that this transmission *should* be worthy of protection.[479] Together these communications create relationships that can be just as deep and meaningful as face-to-face relationships. The concept of interpersonal privacy and the protection of interpersonal bonds—something the Court has recognized outside the Internet context—thus provides the normative framework to conclude that a person has a reasonable expectation of privacy in this Facebook communication.

D. *Applying Interpersonal Privacy Protection: A Real World Hypothetical*

Take the following scenario to highlight the potential real-world application of the instant theory. Amit and Monica were mere acquaintances in college and both joined the military after graduating. They were deployed in different parts of the world. Amit came across Monica through one of his Facebook friends and decided to "friend" her. She accepted. Over a period of months, they communicated very regularly. They video chatted, e-mailed, instant messaged, and even created a Facebook group that included only the two of them. This allowed Amit and Monica to post pictures and updates that only these two could see. Although they did not see each other face-to-face during this period, they had strong feelings for each other and developed a very close relationship. Amit disclosed very private things about himself to Monica, and she did the same.

Now imagine the police back home are investigating a murder that occurred near campus while both were in school. They have suspicion that Amit may be involved. Further assume that Amit did send something incriminating to Monica regarding this murder. This could be an incriminating e-mail, post, or photograph. Under the Third Party Doctrine, there is no Fourth Amendment protection for this communication, as it was voluntarily disclosed to Facebook (an ISP).[480] Accord-

---

[479] This type of analysis can be likened to the mosaic theory of privacy, where discrete public movements (with seemingly no Fourth Amendment protection) add up to something more significant that is worthy of protection. *See supra* note 280. Here, too, when discrete Facebook communications, which may not seem to merit Fourth Amendment protection, are taken together, they create something that is significant and worthy of protection.

[480] *See supra* notes 114–129 and accompanying text. Like all users, Amit accepted a Facebook agreement that detailed Facebook's possession of these communications and their policies relating to disclosure. *See supra* notes 121, 139–164, 210–229 and accompanying text.

ingly, the government can acquire the information from Facebook without probable cause for use against Amit at trial.[481]

The aforementioned theories by scholars would either not provide Fourth Amendment protection on their own terms or come at too high a cost. It is not clear, for instance, whether the automation/human observation distinction will work.[482] For one thing, one would have to determine whether the communication was in fact reviewed by Facebook employees, possibly in the context of a quality control review. More importantly, a proponent of this theory would have to show why the potential of review (based on Facebook's own policies) would not vitiate protection. Similarly, the content/non-content theory may not provide protection in all instances.[483] The incriminating communication could be a photograph or post, which would not readily be amenable to this type of analysis. The techno-social theory may indeed provide a framework for protection but its application would come at too great a cost.[484] This theory would also prevent government agents from acquiring the information through surreptitious means.

This Article's theory of interpersonal privacy squarely provides Fourth Amendment protection without sacrificing too much.[485] The communication is part and parcel of a bona fide relationship and thus would pass the Fourth Amendment reasonable expectation of privacy test. Making this factual determination would be no different than any determination of whether Fourth Amendment protection applies. The only difference would be the factors analyzed.

Instead of looking at where and under what circumstances the communication was made (e.g., house, public area), the court will look to whether the communication was constituent of a relationship worthy of protection.[486] If such a relationship existed when the communica-

---

[481] It is not clear that legislation would protect this communication from being used against Amit. For one thing, we could imagine that this particular incriminating communication was not read or otherwise downloaded by Monica for over 180 days because of an emergency deployment. Moreover, as previously discussed, even if the government were required to provide a warrant supported by probable cause but failed to get one, the SCA does not currently allow exclusion at trial as a remedy for mere violation of the statute. *See supra* notes 250–251 and accompanying text.

[482] *See supra* notes 139–164 and accompanying text.

[483] *See supra* notes 165–181 and accompanying text.

[484] *See supra* notes 182–209 and accompanying text.

[485] *See supra* notes 382–479 and accompanying text.

[486] Presumably, this would require the court to examine the nature and amount of the communications between Monica and Amit on the site and make a determination as to whether a relationship existed. One could imagine default rules that would allow presumptions in favor of Fourth Amendment protection unless the government proved oth-

tion was made, under my theory, the fact that the communication was disclosed to an ISP would not matter. The government thus would require probable cause and a warrant before acquiring this information from Facebook.[487] Yet, if Amit simply posted this incriminating information for all his Facebook friends to see, this would militate against finding a relationship, and thus against protection of the constituent communication. Disclosure to the ISP then would be sufficient to vitiate any privacy interest.

My theory still preserves the government's ability to use certain investigative tools free from Fourth Amendment scrutiny. The framework simply seeks to put any bona fide social networking relationship on equal footing with its face-to-face counterpart. In other words, the government remains free to acquire the information from Monica. There would be no Fourth Amendment violation here. Similarly, the government may pose as a fake Facebook friend and seek to gather the information from Amit that way.[488] These are the same risks that all of us face when disclosing something to a friend, whether online or offline.

Conclusion

It is interesting how narrowly focused Fourth Amendment scholarship has been when talking about the Internet and social networking sites like Facebook. Scholars have focused on the actual communication when trying to counter the Third Party Doctrine. This has led to various theories primarily focusing on the nature of the discrete communication and the information being transmitted. To be sure, a significant amount of ink has been spilled on how, if at all, the Third Party Doctrine should apply to these Internet communications. But this scholarship has failed to recognize the overall effect of these communications. In doing so, scholars have overlooked the importance of social

---

erwise. This Article is less concerned about the logistics of employing the concept of interpersonal privacy (though this is certainly an important enterprise) and more interested in constructing the framework that would justify its use in the first place.

[487] There might be an exception to the warrant requirement that could apply. *See, e.g.*, Crocker, *supra* note 28, at 67 ("Government may not intrude without invitation into protected interpersonal relations without a warrant or an established exception to the warrant requirement."); *supra* note 54. If the government failed to obtain a warrant or an exception did not apply, the communication could not be used at trial against Amit. *See* Davis v. United States, 131 S. Ct. 2419, 2423 (2011) (noting that the Court-created exclusionary rule bars introduction of evidence obtained by the government in violation of the Fourth Amendment).

[488] *See* Semitsu, *supra* note 62, at 322–24; *supra* notes 459–462 and accompanying text.

networking on the Internet and how the concept of interpersonal privacy may provide a unique way to avoid the pitfalls of the Third Party Doctrine. This Article finally begins this discussion.

It should come as no surprise that this Article does not adopt a static interpretation of the reasonable expectation of privacy doctrine. What is reasonable—whether interpreted as normative principle or descriptive norm—will naturally change over time. This is particularly true as technology advances. *Katz* itself came at a time when individuals were using phones outside the home, thus warranting a change in the property-dominated framework of privacy protection. The same is true today. A reasonable expectation of privacy assessment must go beyond the analysis of communications as communications. It must recognize the unique role that Internet communications play in creating and maintaining relationships.

This focus on interpersonal privacy does not mean that the Third Party Doctrine has no effect in today's technology-based world. There may still be appropriate applications. Single e-mails over systems like Gmail or Hotmail (e.g., business e-mails) may not necessarily rise to the level of having a reasonable expectation of privacy under my framework because they are not part of a bona fide relationship.

Outside the communication context, this doctrine also remains a viable mechanism by which Fourth Amendment protection can be lost. Take the *Jones* case and the use of GPS technology. Assuming the device was property installed, my argument would not alter the third party disclosure implications. Because a car's movements are disclosed to the public at large, there would be no expectation of privacy. The concept of interpersonal privacy plays no countervailing role because there is obviously no relationship to speak of this situation. There may be other reasons why individuals have a reasonable expectation of privacy in these public movements, but this has not been my focus.

This Article has exclusively analyzed how interpersonal privacy considerations can be introduced into the discussion of Fourth Amendment protection as it relates to Facebook communications. To this end, the Article presents a different way of thinking about the Internet and our corresponding Fourth Amendment rights.