SOCIAL MEDIA SEARCHES AND THE REASONABLE EXPECTATION OF PRIVACY

Brian Mund
19 YALE J. L. & TECH. 238 (2017)

ABSTRACT

Under existing law, social media information communicated through behind password-protected pages receives no reasonable expectation of privacy. The Note argues that the Fourth Amendment requires a greater degree of privacy protection for social media data. Judicial and legislative activity provides indicia of a willingness to reconsider citizens' reasonable expectation of privacy and reverse an anachronistic equation of privacy with secrecy. Government monitoring of private social media pages constitutes a deeply invasive form of surveillance and, if government agents employ covert tactics to gain access to private social media networks, then the Fourth Amendment controls government use of that private social media information.

TABLE OF CONTENTS

I. INTRODUCTION

Everyday conversations amongst friends—the sort that traditionally constituted private speech—now transpire over social platforms like Facebook, Twitter, and LinkedIn. However, unlike traditional "offline" conversations, online social conversations leave a lasting digital footprint. As such, social platforms create a trail of digital evidence of an individual's behavior. With users of social networking sites increasingly sharing their life experiences online, social platforms may contain an extensive record of information documenting an individual's activities, preferences, and opinions. Moreover, this rise in social sharing of personal information has been accompanied by a misguided sense of security that information shared within personal social networks will remain private. This assumption of data privacy is not necessarily correct. To the contrary, under the current legal framework, information shared within private networks is not protected from greater circulation.

Information shared on social platforms may offer a valuable resource to government investigators. For example, some individuals actually confess to committing crimes to members of their social network.1 Other social data can help the government understand motives, track potential threats, create associative links, confirm alibis, or provide prosecutorial evidence. While government searches of information are generally limited to reasonable searches supported by probable cause, the government has ways to access vast amounts of social data without triggering the "search" threshold. Social networking platforms such as Facebook, Twitter and LinkedIn allow for data sharing within a closed social network. When users publish social content, they share that content with the other members of the private network.

This Note focuses on the reasonable expectation of privacy in the communications posted on private social media networks and the accompanying Fourth Amendment protections against intrusive government searches. An exploration of the extant case law shows that social media users have no reasonable expectation of privacy in their social media postings—even if users communicate their information behind password-protected pages. As such, courts allow the government to search private social media information without applying Fourth Amendment protections. The law treats these "private" social pages as deserving the same protections as if they were publically posted on the Internet. Therefore, courts allow the government to search private social media information without any legally cognizable privacy protections. This doctrinal stance creates the troubling reality that law enforcement officials can and do engage in "covert friending" operations.[2]

I argue that the Fourth Amendment requires a greater degree of privacy protection for social media data. Judicial and legislative activity provides indicia of a willingness to reconsider citizens' reasonable expectation of privacy and reverse an anachronistic equation of privacy with secrecy. Government monitoring of private social media pages constitutes a deeply invasive form of surveillance. Government monitoring of social media pages also implicates individuals' First Amendment rights. While private actors should have the ability to voluntarily disclose third party social media

---

[1] *See e.g.* United States v. Flores, 802 F.3d 1028, 1033 (9th Cir. 2015) (discussing the admissibility of defendant's Facebook messages referencing her carrying marijuana between the United States and Mexico).

[2] United States v. Gatson, 2014 WL 7182275, at *22 (D.N.J. Dec. 16, 2014) ("As part of their investigation into Gatson and other co-conspirators, law enforcement officers used an undercover account to become Instagram 'friends' with Gatson . . . No search warrant is required for the consensual sharing of this type of information.")

information, the balance between government interests and privacy interests favors applying Fourth Amendment safeguards in the case of covert government friending.

II. PRIVACY AND SOCIAL DATA

The proliferation of social technologies has facilitated the ease with which both private and public actors can collect personally identifiable data. Many privacy advocates have watched this and other technological developments with concern, noting the detrimental effect to consumer privacy. In fact, this trend has gone so far as to lead some to claim an end to a reasonable expectation of data privacy.[3] However, the law does not leave consumers without any privacy protection; individuals enjoy privacy rights deriving from the common law, statutory protections, and protections stemming from the Bill of Rights. This Note focuses on the reasonable expectation of privacy in communications posted on private social media networks and the accompanying Fourth Amendment protections against government intrusions.

A. The Fourth Amendment

The Fourth Amendment grants the American people the right to remain free from unreasonable governmental searches.[4] As interpreted by the Supreme Court, "A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[5] In *Katz v. United States*, the Supreme Court outlined the framework governing this right in modern case law.[6] As interpreted by the Court, the Fourth Amendment poses a requirement for a judicially-sanctioned warrant for government search behavior that violates an individual's "reasonable expectation of privacy."[7] As Justice Harlan explains in his *Katz* concurrence, there are two elements to assessing the reasonableness of expecting privacy: a subjective and objective component.[8]

---

[3] *See* David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CAL. L. R. 1069, 1087 (2014) (noting "some observers . . . write off privacy as a lost cause.")

[4] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . .")

[5] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[6] 389 U.S. 347 (1967).

[7] *Id.*

[8] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). *See also* Kyllo v. United States, 533 U.S. 27, 33 (2001) ("As Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when

When it comes to social media data, the extent to which individuals have a reasonable expectation of privacy in their social network publications determines whether courts will consider government searches of social data information "unreasonable" and therefore protected by the Fourth Amendment. However, one should note that the Fourth Amendment serves as a "floor" for privacy protection against unreasonable government searches. Both federal and state legislators have the ability to supplement Fourth Amendment privacy protections, and have done so. For example, the Electronic Communications Privacy Act of 1986 (ECPA) establishes requirements and procedures for government actors intercepting communications as well as accessing stored information.[9]

B. Exceptions to the Reasonable Expectation of Privacy

Digital data, like traditional information, receives a presumptive privacy protection under the Fourth Amendment. The government cannot access privately stored information without obtaining a search warrant backed by probable cause—individuals have a right to store information without baseless government interference.[10] Citizens may reasonably expect the greatest level of privacy protection against government intrusion when actions and speech transpire within the private confines of an individual's home.[11] On the other hand, citizens

---

the government violates a subjective expectation of privacy that society recognizes as reasonable.")

[9] 18 U.S.C. § 2510-22. In 1986, Congress passed major statutes collectively known as the Electronic Communications Privacy Act (ECPA). ECPA limits the interception and disclosure of electronic communication. This Note assumes that ECPA governs the privacy interests implicated in disclosures from third party providers (both platform providers and non-platform providers), thereby involving a separate legal regime. This Note restricts the scope of its analysis to non-provider social media users accessing a social media network. For cases covering ECPA governance of social media sites, see, for example, Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 669 (D.N.J. 2013) ("Accordingly, the Court finds that non-public Facebook wall posts are covered by the SCA.") and Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010) (finding private messaging or email services to comprise electronic communication services). *But see* Juror No. One v. Superior Court, 206 Cal. App. 4th 854, 863 (2012) (stating that *Crispin* reached its conclusion based on stipulations specific to that case).

[10] *See supra* note 4; *Katz*, 389 U.S. 347 at 349-350..

[11] *See, e.g.*, *Kyllo*, 533 U.S. at 31 ("At the very core of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"); Payton v. New York, 445 U.S. 573, 587 (1980) ("Freedom from intrusion into the home or dwelling is the archetype of the privacy protection secured by the Fourth Amendment."); *see also* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1157, 1194 (2004) ("The primary locus of one's 'reasonable expectation of privacy' is of course in the home").

do not have a reasonable expectation of privacy against government searches or intelligence-gathering efforts that occur in public settings[12] or where citizens expose private information to a third party.[13]

1. Third-Party Doctrine

The third-party doctrine severely cabins Fourth Amendment protections by creating an exception to the reasonable expectation of privacy. First articulated in *Smith v. Maryland*, the third-party doctrine states that once an individual invests a third party with information, and voluntarily agrees to share information with a recipient,[14] the individual loses any reasonable expectation of privacy in that information.[15] While railed against by many privacy advocates,[16] *Smith* still serves as good law.[17]

The third-party doctrine served as only a partial justification for the *Smith* opinion. *Smith* found that the defendant had no reasonable expectation of privacy pursuant to third party disclosure only after first establishing that the government did not perform a Fourth Amendment search.[18] The Court drew on a long-standing jurisprudential distinction

---

[12] *See* Harris v. United States, 390 U.S. 234, 236 (1968) ("It has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence."); *see also* Coolidge v. New Hampshire, 403 U.S. 443, 464-69 (1971) (outlining the three conditions for the plain view doctrine); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, LAW ENFORCEMENT AND NATIONAL SECURITY 50 (2015) (explaining the plain view doctrine).

[13] Smith v. Maryland, 442 U.S. 735, 743-44 (1979); *see also* United States v. Miller, 425 U.S. 435, 442 (1976) (finding that defendant had no legitimate expectation of privacy in bank records stored by third party banks).

[14] With the exception of a few special relationships such as a fiduciary duty, a duty of loyalty, or a privileged relationship.

[15] *Smith*, 442 U.S. at 743-44.

[16] See, e.g., Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C.L. REV. 1 (2013); Andrew J. Defilippis, *Securing Informationships: Recognizing A Right To Privity In Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1086 (2006) (challenging the "so-called third-party doctrine"); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1239 (2009) ("Professor Epstein, Professor Kerr, and I may at times approach legal questions from different perspectives, but there is one thing that we all agree upon: the current configuration of third-party doctrine under the Fourth Amendment is problematic."); Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need A Warrant For That": The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds*, BERKELEY J. CRIM. L. 155, 159 (2014) (agreeing with Justice Sotomayor's concurrence in United States v. Jones, 565 U.S. 400 (2012) that third-party doctrine has no place in the digital age).

[17] *See e.g.*, United States v. Graham, 824 F.3d 421, 437 (4th Cir. 2016). For a defense of the third-party doctrine (in a modified form), see Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

[18] *Smith*, 442 U.S. at 741 (distinguishing *Smith* from *Katz* on the grounds that "pen registers do not acquire the *contents* of communications.")

between content and non-content information, where the Court affords higher protection to contents of a communication.[19] For example, in *Ex parte Jackson*, the Court found that mailed letters and sealed packages "are as fully guarded from examination and inspection, except as to their outward form and weight."[20] While the government may freely read the information on the cover of an envelope, opening the envelope and searching its contents would violate the Fourth Amendment.[21] Courts have not reached the content versus non-content distinction when assessing social media communications. Instead, courts have found the third-party doctrine dispositive.[22]

When one applies the third-party doctrine to social media information, one finds that individuals do not have a reasonable expectation of privacy in social media data. As a result, government agents can presumably gain access to posted social media data without meeting any probable cause requirements. As soon as one posts information on a social platform, the poster discloses information to the third party platform operator.[23] Moreover, for most social networking posts, all of the members within a user's social network also receive access to the published information. In "Wall-to-Wall"-type conversations between two users,[24] the rest of the users' social network functions as third parties to whom the content publisher and recipient have voluntarily disclosed information. If the third-party doctrine governs social media behavior, then published content voluntarily shared among connections within a private social network loses all reasonable expectation of privacy, including any reasonable expectation that a user's

---

[19] *See Id*. *See also*, In re Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 145 (E.D.N.Y. 2013) (discussing the *Smith* distinction between content and non-content and the accompanying jurisprudential history).

[20] 96 U.S. 727, 733 (1877).

[21] This distinction has also evolved into the classifications of data and metadata, where data refers to the contents of the communication, and metadata serves as the digital equivalent to the outside of the envelope. For example, in the telephone-tracking context, telephone data refers to the communications content, and telephone metadata refers to information such as "telephone numbers dialed (incoming and outgoing), times, and durations of calls." Obama v. Klayman, 800 F.3d 559, 561 (D.C. Cir. 2015).

[22] *See, e.g.*, Palmieri v. United States, 72 F. Supp. 3d 191, 210 (D.D.C. 2014) (citing *Smith* and *Miller* to find that "when a Facebook user allows 'friends' to view his information, the Government may access that information through an individual who is a 'friend' without violating the Fourth Amendment.")

[23] However, platform providers are subject to a separate legal scheme under ECPA and outside the scope of this Note's analysis. *See supra* note 9.

[24] These types of conversations are particularly prevalent on platforms such as Facebook and Twitter.

connections will not turn over their social data to investigative authorities.[25]

2. Voluntary Consent

Similar to the third-party doctrine, individuals also lose a reasonable expectation of privacy when they consent to a government search of private information. Unlike the third-party doctrine, which assesses the expectations of privacy of voluntarily disclosed information, the voluntary consent exception addresses consent to the search itself. The Supreme Court declared in *Schneckloth v. Bustamonte*, "It is . . . well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent."[26] Thus, if an individual freely consents to a government search, the government may freely do so.

A Fourth Amendment search does not require affirmative consent to a search by an announced government actor. According to the Court, "The Fourth Amendment is satisfied when, under the circumstances, it is objectively reasonable for the officer to believe that the scope of the suspect's consent permitted him [to conduct that search that was undertaken]."[27] However, *Schneckloth* provides a "jealously and carefully drawn" consent exception to the rule against unwarranted searches,[28] and only applies when an individual knowingly and voluntarily submits to a search. As such, the Court has found that the consent exception cannot plausibly apply to cases of electronic surveillance.[29] The Court reasons, "The very nature of electronic surveillance precludes its use

[25] This discussion examines posts that are available to all members with access to the social network. Users may have a higher reasonable expectation of privacy for messages communicated through private messenger services. *See* R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) (finding that defendant had a reasonable expectation of privacy regarding private Facebook messages).

[26] U.S. 218, 219 (1973).

[27] Florida v. Jimeno, 500 U.S. 248 (1991); *see also* United States v. Brooks, No. 12-CR-166 RRM, 2012 WL 6562947, at *3 (E.D.N.Y. Dec. 17, 2012) (citing *Jimeno*, 500 U.S. at 249); United States v. Mendenhall, 446 U.S. 544, 558 (1980) (listing factors leading to voluntary consent). However, the same "objectively reasonable" analysis may limit the scope of the permitted search. *See* Florida v. Jardines, 133 S.Ct. 1409, 1416 (2013) ("The scope of a license—express or implied—is limited not only to a particular area but also to a specific purpose.")

[28] Georgia v. Randolph, 547 U.S. 103, 109 (2006) (quoting Jones v. United States, 357 U.S. 493, 499 (1958)); William E. Underwood, *A Little White Lie: The Dangers of Allowing Police Officers to Stretch the Truth As a Means to Gain a Suspect's Consent to Search*, 18 WASH. & LEE J. CIVIL .RTS. & SOC. JUST. 167, 176 (2011).

[29] *See* Katz v. United States, 389 U.S. 347, 358 (1967).

pursuant to the suspect's consent."[30] The Court finds that the efficacy of electronic surveillance relies on the fact that the suspect does not know about the surveillance, and finds that without prior notice, the *Schneckloth* exception cannot apply.[31]

The *Schneckloth* consent focuses on voluntary and non-coerced consent for an agent to conduct a search. This consent remains doctrinally distinct from cases where an individual does not knowingly consent to a government search, but rather unknowingly agrees to the presence of an undercover government agent. Undercover government agents may lawfully gain access based on a misrepresented identity.[32] If an individual offers lawful access to their private information, then that person voluntarily assumes the risk that the access might expose that information to the government.[33] For example, an undercover officer in a public bookstore does not violate the Fourth Amendment by accepting an offer to do business in illegal wares,[34] nor does an undercover officer's acceptance to enter an individual's home to conduct an illegal drug sale pose a constitutional problem.[35] In both cases, "A government agent, in the same manner as a private person, may accept an invitation to do business and may enter upon the premises for the very purposes contemplated by the occupant."[36] In both undercover cases, the individual consents to the agent's access, reflecting an accepted risk that the agent will use or disclose the exposed information. However, in neither case does the individual ever grant permission for the agent to use the information exposed through the business

---

[30] *Id.*; *see also* Lopez v. United States, 373 U.S. 427, 463 (1963) (Brennan, J., dissenting) ("the usefulness of electronic surveillance depends on lack of notice to the suspect.")

[31] *Lopez*, 373 U.S. at 463.

[32] *See, e.g.* Hoffa v. United States, 385 U.S. 293, 302 (1966); United States v. Longoria, 177 F.3d 1179, 1183 n.2 (10th Cir. 1999) ("If a defendant . . . knowingly exposes his conversations to accomplices, even in a room not accessible to the general public, his conversations are not subject to Fourth Amendment protection from disclosure by such accomplices.") (cited by United States v. Davis, 326 F.3d 361, 365 (2d Cir. 2003)).

[33] *Hoffa*, 385 U.S. at 302 (holding that a defendant does not have a privacy interest in matters voluntarily revealed to a government agent, including a confidential informant).

[34] Maryland v. Macon, 472 U.S. 463, 470 (1985).

[35] Lewis v. United States, 385 U.S. 206 (1966) (holding that a defendant who invites an undercover agent into his home for narcotics purchases willingly reveals information relating to the business transaction does not constitute an illegal search).

[36] *Lewis*, 385 U.S. at 211 ("During neither of his visits to petitioner's home did the agent see, hear, or take anything that was not contemplated, and in fact intended, by petitioner as a necessary part of his illegal business.") Thus, to the extent that the undercover agent's presence would be otherwise lawful, "undercover operations . . .are not "searches" under the Fourth Amendment." *See* United States v. Mayer, 503 F.3d 740, 750 (9th Cir. 2007) (citing *Macon*, 472 U.S. at 105).

transaction. In sum, the voluntary consent exception to the requirement for search warrants specifically imagines a narrow carve-out for the knowing consent to announced government searches.

III. SOCIAL DATA AND GOVERNMENT INTELLIGENCE GATHERING

People regularly mistakenly believe that their social discussions are private. As privacy scholars have noted, social networking users consistently underestimate the exposure inherent in the publication of social information.[37] Social networks create a sense of a private space, leading people to converse as if they were behind closed doors and not in the public view.[38] Social conversations often fulfill the subjective prong of the *Katz* reasonable expectations test—while users know that the social networking platforms and other users within their network have the ability to access their conversations, they assume that they have a right to privacy. Below, the Note reviews the existing case law on the reasonable expectation of privacy in social media information, and finds that the third-party doctrine results in no reasonable expectation of privacy in published social data. As a result of the lack of a reasonable expectation of privacy, the current case law allows government agents to employ information-gathering techniques on social data without triggering Fourth Amendment protections against unreasonable searches and seizures. However, judicial and legislative activity suggests a willingness to reconsider the third-party doctrine's improper equation of privacy with secrecy.

A. Publicly Shared Social Data

Many social media users exhibit a mistaken subjective expectation of privacy on social platforms even in situations where the users' privacy settings are set to "public." Some plaintiffs have tried to argue that they held a reasonable expectation of privacy regarding publicly accessible social media postings. However, courts have flatly disabused the

[37] As James Grimmelman has written, "Over a hundred million people have uploaded personally sensitive information to Facebook, and many of them have been badly burnt as a result. Jobs have been lost, reputations smeared, embarrassing secrets broadcast to the world." James Grimmelman, *Saving Facebook*, 94 IOWA L. REV. 1137, 1140 (2009).

[38] *See Id.* at 1160 (looking at Facebook and finding that the nature of the social networking website suggests "an intimate, confidential, and safe setting").

notion that plaintiffs could have a reasonable expectation of privacy for publically available social media content. One judge offered the following consideration of the reasonableness of the privacy claim:

> Consider the following: a man walks to his window, opens the window, and screams down to a young lady, "I'm sorry I hit you, please come back upstairs." At trial, the People call a person who was walking across the street at the time this occurred. The prosecutor asks, "What did the defendant yell?" Clearly the answer is relevant and the witness could be compelled to testify. Well today, the street is an online, information superhighway, and the witnesses can be the third party providers like Twitter, Facebook, Instagram, Pinterest, or the next hot social media application.[39]

In the above example, Judge Sciarrino, Jr. compares a public social media post to screaming the content out of an open window, and that sharing information on the internet is akin to sharing information in the middle of a public street. Anyone with an internet connection could access the published information. The judge concludes that society cannot reasonably protect the person who expects such behavior to remain private. Thus, the publisher of this public information cannot expect the law to protect against government use of the information. The government did not "search" for this data; the publisher left this data in plain view of all internet users.[40] In short, regardless of subjective intent, the courts have declared that society refuses to grant an objective expectation of privacy to information disclosed onto the public internet.

B. Intelligence-Gathering on Private Networks

However, much of social networking data lies within closed private networks. Unlike publicly available data, which Judge Scariarrino equated to screaming in the street, data shared within a private social network more closely resembles a conversation in a private room. In the latter scenario, the publisher has made an active effort to shut out strangers. By limiting the social network's privacy settings to social media "friends," an individual has shown that "he seeks to preserve

---

[39] People v. Harris, 949 N.Y.S.2d 590, 594 (Crim. Ct. 2012).

[40] *See* California v. Greenwood, 486 U.S. 35, 41 (1988) ("[T]he police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public."); Harris v. United States, 390 U.S. 234, 236 (1968) ("[I]t has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence."); *see also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, LAW ENFORCEMENT, AND NATIONAL SECURITY (2015) (explaining the plain rule view).

[something] as private."[41] Thus, the protected network forum naturally operates with greater privacy than the publicly available alternative. Does this difference have an impact on the reasonable expectation of privacy against government access of this data? According to the current case law, it does not.[42] When users post to their social networks, most courts have ruled that the publishers lose all reasonable expectation of privacy to that data.

With social media communications, the publisher knows that the content is being recorded on the website's platform. To the extent that a publisher "takes a risk that the [social media connection] may repeat all he hears and observes,"[43] the publisher knows that the social connection has access to the recorded information. The social media connections can repeat the shared information to anyone, including government officials. Just as the social media publisher takes the risk that his network connections will alert law enforcement to the content of his posts, that publisher also assumes the risk that a social media connection is actually an undercover government agent.[44] As stated in *United States v. Miller*, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose

[41] *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing *Katz v. United States*, 389 U.S. 347, 351 (1967)).

[42] This Note limits its focus to the surveillance of content-based data, but recognizes that the social networking websites provide extremely revealing "non-content" metadata that have traditionally lain outside of the scope of the Fourth Amendment.

[43] Dietemann v. Time, Inc., 449 F.2d 245, 249 (9th Cir. 1971). The Court's decision in *Lopez* further supports the proposition that if "friends" can disclose data from memory, they can also disclose actual recorded content. To do otherwise, Justice Harlan suggests, would be to suggest a "constitutional right to rely on possible flaws in …memory." Lopez v. United States, 373 U.S. 427, 439 (1963).

[44] United States v. Brooks, No. 12-CR-166 RRM, 2012 WL 6562947, at *3 (E.D.N.Y. Dec. 17, 2012) ("Indeed, if Sawyer and Ladeau assumed the risk that one of his "friends" would alert law enforcement to the fact that he was trading child pornography, Brooks equally assumes the risk that one of his "friends" is *actually* a law enforcement agent.") *Brooks* appears to conflate the third-party doctrine and the voluntary consent doctrine. In Part II.B of the opinion, Judge Mauskopf cites *Schneckloth* for the proposition that the defendant had voluntarily (yet unknowingly) consented to a government search. *Id.* at *3. Judge Mauskopf continues his analysis by citing cases like *Lewis* that concern voluntary consent to covert access, not consent to search. *Id.* at *4. The rest of the *Brooks'* consent analysis pursues the "risk of third party exposure" reasoning, yet categorizes its reasoning under the *Schneckloth*-type consent exception to the search warrant requirement.

and the confidence placed in the third party will not be betrayed."[45]

In the following sub-sections, the Note explores the Fourth Amendment privacy protections against two strategies that the government may employ to gather its citizens' social media data. First, a social network connection may voluntarily turn over published social media information to a government agent. Second, a covert government agent may request to directly join an individual's social media network. Under both strategies, the law allows the government to search and use the data without the probable cause restraints of the Fourth Amendment.

1. Sharing Information with the Government

Courts have found that third-party social network connections have the ability to use data voluntarily shared on social media and turn that information over to the government. In the past, some courts have considered the third-party social connections to be the intended recipients.[46] The law has traditionally given little protection to ill-considered disclosures, such as sharing damning evidence within a shared social network.[47] Under the existing legal regime, once an individual voluntarily exposes information to another party, that individual impliedly waives their privacy rights and cannot reasonably expect to limit the recipient's usage of that information. As the Supreme Court articulated, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[48] Under the third-party doctrine, this use includes the ability to share received information with the government.[49]

The Southern District of New York considered the disclosure of Facebook data to the government in *United States v. Meregildo*. In *Meregildo*, the court recognized that the

---

[45] 425 U.S. 435, 443 (1976). Some scholars have critiqued this doctrine, arguing that controlled disclosures that "represent the limited, focused sharing of information" between two parties should be seen as a legitimate transaction between two parties. As a result, they analogize these disclosures to "communications encompassed by evidentiary privileges," and should not lose all reasonable expectation of privacy to the information. Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J. L. & POL'Y 211, 258–259 (2006).

[46] *See, e.g.* United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (characterizing a Facebook friend as a party to any social network conversation).

[47] See discussion on government friending, *infra* Section B.2.

[48] Katz v. United States, 389 U.S. 347, 351 (1967).

[49] James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1197 (2009) ("Similarly, under the third-party doctrine, a Facebook user who makes a fact known only to a small group of contacts has no Fourth Amendment grounds for complaint if one of those contacts reveals the fact to the police.").

defendant "undoubtedly believed that his Facebook profile would not be shared with law enforcement."[50] However, despite the defendant's subjective expectation of privacy, he failed the objective prong. The court found that the defendant "had no justifiable expectation that his 'friends' would keep his profile private" . . . because those 'friends' were free to use the information however they wanted—including sharing it with the Government."[51] Due to the fact that the government received information from a cooperating party with legitimate access to that information, the government did not perform a "search" within the meaning of the Fourth Amendment, and the Amendment's protections did not apply.[52]

Several other courts have considered the question of disclosure of third party social media connections' data and have reached the same conclusion—social media users do not have an objectively reasonable expectation of privacy to data published within a private social media network.[53] The courts' reasons for finding a lack of objective expectation of privacy have included the notion that people use social networking sites for the very purpose of connecting with friends and meeting new people,[54] the fact that individuals knowingly expose their information to hundreds or thousands of their social media connections' own connections,[55] or just as a

---

[50] *Meregildo*, 883 F. Supp. 2d at 526.

[51] *Id*.

[52] *See also* Palmieri v. United States, 72 F. Supp. 3d 191, 210 (D.D.C. 2014) ("When a Facebook user allows "friends" to view his information, the Government may access that information through an individual who is a "friend" without violating the Fourth Amendment."); Rosario v. Clark Cty. Sch. Dist., No. 2:13-CV-362 JCM PAL, 2013 WL 3679375, at *6 (D. Nev. July 3, 2013) ("This logic applies with equal force in the social media context. When a person tweets on Twitter to his or her friends, that person takes the risk that the friend will turn the information over to the government.")

[53] *E.g.,* Chaney v. Fayette Cty. Pub. Sch. Dist., 977 F. Supp. 2d 1308, 1315 (N.D. Ga. 2013) ("Even if she had a subjective expectation of privacy in her Facebook photos, Chaney cannot show that her expectation is legitimate."); United States v. Brooks, No. 12-CR-166 RRM, 2012 WL 6562947, at *2 (E.D.N.Y. Dec. 17, 2012) ("In applying this principle to emerging internet technologies, courts have uniformly held that a user of a private or 'closed' peer-to-peer network such as GigaTribe who makes available files to his 'friends' does not have an objectively reasonable expectation of privacy in those files he shared."); McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285 ("while it is conceivable that a person could use them as forums to divulge and seek advice on personal and private matters, it would be unrealistic to expect that such disclosures would be considered confidential."); United States v. Ladeau, No. CRIM 09-40021-FDS, 2010 WL 1427523, at *5 (D. Mass. Apr. 7, 2010) ("Once Ladeau turned over the information about how to access the network to a third party, his expectation of privacy in the network became objectively unreasonable. Because the files he claims were private were made available to anyone on the network, his expectation of privacy in those files was also objectively unreasonable.").

[54] Hummingbird Speedway, Inc., 2010 WL 4403285.

[55] *Chaney*, 977 F. Supp. 2d at 1315.

consequence of exposing the information to the entirety of the private network.[56] Because the courts find the voluntary exposure of the information dispositive, court have not reached the question of whether the surveillance of "content" of social media communications impact the analysis of a reasonable expectation of privacy.[57] Due to the lack of a reasonable expectation of privacy in the social media data, an individual may allow a government agent access to that person's social network accounts, and the agent would then have the ability to search any of that individual's information posted within the shared network. In sum, courts have consistently held that agents do not need a search warrant before looking through social network data provided by a cooperating private party with access to a protected network. The next section analyzes the Fourth Amendment restrictions when a covert government agent adds a social network "friend" to covertly monitor the friend's network.

2. Covert Government "Friends"

The government may also attempt to access social networking data more directly—by creating an account and asking an individual to permit entry into their social network. Traditionally, parties have no legal recourse to misreading their friends or from falling prey to overtures by covert operatives. In *Hoffa v. United States*, the Court found that information voluntarily offered to an undercover informant as a result of misplaced confidence did not represent a legitimate privacy interest under the Fourth Amendment.[58] Similarly, in *Lewis v. United States*, the Court reaffirmed the constitutionality of covert information gathering, relying on an important government interest in maintaining the ability to deploy undercover agents.[59] Together, *Hoffa* and *Lewis* stand for the proposition that "a person does not have a privacy interest in the loyalty of her friends."[60] As such, if an individual accepts a friend request from an undercover government agent,

---

[56] *Ladeau*, 2010 WL 1427523, at *5.

[57] *See, e.g.*, United States v. Brooks, No. 12-CR-166 RRM, 2012 WL 6562947, at *2 (E.D.N.Y. Dec. 17, 2012) (citing *Smith* for the proposition that one has no reasonable expectation of privacy in information voluntarily disclosed to third parties); United States v. Sawyer, 786 F. Supp. 2d 1352, 1355 (N.D. Ohio 2011) (same).

[58] 385 U.S. 293 (1996).

[59] 385 U.S. 206, 210 (1966) ("Were we to hold the deceptions of the agent in the case constitutionally prohibited, we would come near to a rule that the use of undercover agents in any manner is virtually unconstitutional per se. Such a rule would, for example, severely hamper the Government . . . ").

[60] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, LAW ENFORCEMENT, AND NATIONAL SECURITY 18 (2015).

that acceptance provides the same access as if the individual knowingly exposed permitted their private social media publications to the government agent.[61]

The voluntariness of assuming the risk of exposure has played a key role in cases considering covert government friending. The mere request to join a private social network does not violate any privacy interest; asking to join a social media network draws analogues to an individual knocking on a door of one's home and requesting to enter. The Supreme Court has held that "a police officer not armed with a warrant may approach a home and knock, precisely because that is 'no more than any private citizen might do.'"[62] The friend request itself does not invade the defendant's privacy rights, and the defendant may simply reject the request to expose their data to the requesting party. When the defendant chooses to accept the friend request, the defendant bears the accompanying risks of third party disclosure of the private information. This includes the risk of a government agent accessing and searching their private information. In *United States v. Sawyer*, an Ohio district court noted,

Here, by becoming "friends" with "[covert government informant] SB," Defendant Sawyer granted the "SB" username the authority to access any files or folders designated as shared. The owner of the "SB" name then voluntarily consented to Agent Couch using that username to access the shared folders and files on Sawyer's computer. [Doc. 23–3.] It makes little difference that "SB" was granted authority to access and download the files on the computer over the internet, rather than through a grant of physical access to the computer actually storing those files, particularly since Agent Couch only accessed the files remotely over the internet.[63]

Even with heightened privacy interests at stake, the voluntary nature of the Sawyer's acceptance of SB's friend request strikes a hard blow both against any reasonable expectation of privacy that SB will not share the information in the shared files with Agent Crouch. While the defendant's acceptance of SB's friend request does not constitute a voluntary consent to a search,[64] by exposing his files to the SB, the defendant effectively eliminates the Fourth Amendment privacy protections that would have otherwise limited SB's search of those files. Since the defendant willingly allowed access to anyone interested in such material, the acceptance

---

[61] *See* United States v. Gatson, Crim. No. 13-705, 2014 WL 7182275, at *22 (D.N.J. Dec. 16, 2014). However, as noted in Section II.B.2, this type of voluntary disclosure remains doctrinally distinct from a consensual search.

[62] Florida v. Jardines, 133 S. Ct. 1409, 1416 (2013) (quoting Kentucky v. King, 563 U.S. 452, 469 (2001)).

[63] United States v. Sawyer, 786 F. Supp. 2d 1352, 1357 (N.D. Ohio 2011).

[64] *See* discussion *supra* note 30.

did not wrongfully infringe upon the defendant's fundamental property rights.[65] Instead, the defendant relinquished a reasonable expectation of privacy in the accessible material. As a rule, just as surveillance does not automatically violate the Fourth Amendment when conducted in a public place because the monitored user has no reasonable expectation of privacy,[66] the surveillance of publically exposed social media data will generally not violate the Fourth Amendment due to the lack of a reasonable expectation of privacy. In short, covert government friends may add and monitor individuals' social networks without violating the Fourth Amendment.

C. Third-Party Doctrine: A Chink in the Armor

While the third-party doctrine remains good law, it totters on its last legs—and with good reason. A reasonable expectation of privacy should not require secrecy as a requisite condition. The third-party doctrine heavily relies on an equation between a lack of secrecy arising from information exposure and an abrogation of any reasonable privacy interest in that exposed information. As recently as *United States v. Graham*, the Fourth Circuit court lamented the doctrine, proclaiming that if only the doctrinal landscape provided greater juridical flexibility, the court would have "ceased to treat secrecy as a prerequisite for privacy."[67] Finding its hands tied by precedent, the judges "recognize the appeal—if we were writing on a clean slate—in holding that individuals always have a reasonable expectation of privacy in large quantities of location information . . . [but] the third-party doctrine does not afford us that option."[68] Instead, "unless and until" the Supreme Court holds that secrecy is no longer necessary for privacy, "we are bound by the contours of the third-party doctrine as articulated by the Court."[69]

The jurisprudential approach of ceasing to equate secrecy with privacy has a long history, and has gained greater

---

[65] The *Sawyer* court relies on Sixth Circuit precedent to offer the proposition that "an undercover officer may gain entrance [to a home] by misrepresenting his identity and may gather evidence while there." United States v. Sawyer, 786 F. Supp. 2d 1352, 1356-57 (N.D. Ohio 2011) (quoting United States v. Pollard, 215 F.3d 643, 649 (6th Cir. 2000)).

[66] United States v. Wells, 789 F. Supp. 2d 1270, 1273 (N.D. Okla. 2011), *aff'd*, 739 F.3d 511 (10th Cir. 2014) ("However, neither video nor audio surveillance automatically violates the Fourth Amendment; when such surveillance is conducted in a public place such as a bank, where no reasonable expectation of privacy exists, the surveillance is not subject to suppression.")

[67] United States v. Graham, 824 F.3d 421, 437 (4th Cir. 2016) (citing United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring)).

[68] Id.

[69] *Id* (citation omitted).

support in recent years. In 1967, *Katz v. United States*, the Court held that the defendant had a reasonable expectation of privacy to the contents of his communication, despite the fact that he had voluntarily communicated via a service that enabled the telephone company to monitor his calls.[70] According to the *Katz* Court, if a person seeks to keep information private, even in a publically accessible area, then that information may be constitutionally protected.[71] *Smith* distinguished the *Katz* ruling by highlighting the difference between monitoring which captures the content of communications versus monitoring that does not capture content.[72] As a result, capturing non-content information does not constitute a constitutional search.[73] The surveillance of social media communications concerns the contents of communication, thereby invoking the *Katz* analysis.[74]

In *United States v. Warshak*, the Sixth Circuit rejected the notion that the risk of third party exposure necessarily erases a reasonable expectation of privacy.[75] The court distinguished electronic communications from bank records in *United States v. Miller*[76] and explicitly found that "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[77] The *Warshak* judges justified their distinction on the basis that *Miller* concerned "simple bank records," as opposed to deeply confidential information and that the depositor disclosed the bank records for the bank's use

---

[70] 389 U.S. 347, 351 (1967) ("But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.") Going even further back, the Court ruled in *Ex parte Jackson*, 96 U.S. 727 (1877) that individuals had a reasonable expectation of privacy to the contents of their mail even though the post office had the ability to open the mail.

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

[72] Smith v. Maryland, 442 U.S. 735, 741 (1979).

[73] *Id.*

[74] *Smith* and *Katz* dealt with monitoring through electronic interception, while social media surveillance occurs after the reception of the electronic transmission. This technical variation in monitoring methods should not impact the privacy analysis. In the social media context, the government does not intercept social media messages in electronic transit, but monitors them once they reach their intended destination. While the Stored Communications Act and Wiretap Act (18 U.S.C. §§ 2510-22) may create a statutory distinction, the Fourth Amendment concern over covert government electronic surveillance encompasses both scenarios. As *Katz* emphasizes, the constitutional violation arises not from the interception of communication, but from the fact that the government conducted electronic surveillance without meeting "the procedure of antecedent justification." *Katz,* 389 U.S. at 358.

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

[76] 425 U.S. 435 (1976).

[77] *Warshak*, 631 F.3d at 286-87. By identifying the communications as "content," *Warshak* effectively distinguished *Smith*, see *id.*

in the ordinary course of business.[78] *Warshak*'s distinctions can apply to social media information as well. Several courts have also found that the disclosure of cell site location information does not preclude reasonable expectations of privacy under the third-party doctrine.[79] New York courts have also stridently objected to the application of the third-party doctrine to digital data.[80]

Recent Supreme Court decisions suggest a limited application of third-party doctrine to electronic data, yet the Court has not overruled the third-party doctrine. Justice Sotomayor's concurring opinion in *United States v. Jones* provides an early indication of an unwillingness to apply the third-party doctrine to digital data. In *United States v. Jones*, Justice Sotomayor highlighted the fact that digital information such as GPS monitoring produces "a wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations."[81] Access to such data reveals private information about one's social connections, and this chills one's "associational and expressive freedoms."[82] The extent of exposure leads Justice Sotomayor to conclude that sheer amount of informational data gathered in some types of

---

[78] *Id*. at 288.

[79] *See e.g.*, In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1029 (N.D. Cal. 2015), *appeal dismissed* (Feb. 5, 2016) ("[T]he Court concludes that historical CSLI generated via continuously operating apps or automatic pinging does not amount to a *voluntary* conveyance of the user's location twenty-four hours a day for sixty days."); United States v. Cooper, No. 13-CR-00693-SI-1, 2015 WL 881578, at *6 (N.D. Cal. Mar. 2, 2015) ("[T]he pen registers employed in 1979 bear little resemblance to their modern day counterparts."); Tracey v. State, 152 So. 3d 504, 523 (Fla. 2014), *reh'g denied* (Dec. 8, 2014) ("The Supreme Court, in stating this principle, has clearly recognized protection of 'personal and societal values' regarding expectations of privacy that a society is willing to recognize even where such activities are not fully concealed." (citing California v. Ciraolo, 476 U.S. 207, 210 (1986)). *But see* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) ("All of our sister circuits to have considered the question have held, as we do today, that the government does not violate the Fourth Amendment when it obtains historical CSLI from a service provider without a warrant."); United States v. Davis, 785 F.3d 498, 514 (11th Cir.), *cert. denied*, 136 S. Ct. 479 (2015) (finding that recent Supreme Court decisions "leave the third-party doctrine untouched"); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013) ("This crabbed understanding of voluntary conveyance would lead to absurd results.").

[80] *See e.g.* People v. Thompson, 28 N.Y.S.3d 237, 251 (2016) ("At a time when many people routinely relay sensitive personal information by email, the assertion that no Fourth Amendment protections apply to such communications because email requires an email account, in this Court's view, is an archaic notion which negates the protection of the Fourth Amendment for many of our most private communications.")

[81] United States v. Jones, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring) (citation omitted).

[82] *Id*. at 956.

electronic surveillance methods violates a reasonable expectation of privacy and constitutes a search under the Fourth Amendment, regardless of the voluntary exposure. In dicta, Justice Sotomayor goes even further, suggesting the need to reconsider the third-party doctrine, noting that the rule is "ill suited to the digital age."[83]

Finally, in *Riley v. California*, an eight Justice majority cited Justice Sotomayor's concurring opinion in *Jones* to find that a warrantless search of a smartphone's call log violated the Fourth Amendment, even when that search was conducted incident to arrest.[84] Relying on the quantitative and qualitative differences in electronic data, the Court found that the pervasiveness of the digital information stored on cell phones requires greater privacy protections than a traditional search would mandate. [85] While the government legitimately confiscated the defendant's cell phone incident to arrest, the defendant still maintained a privacy interest in the contents in the cell phone despite the third party exposure.[86]

Legislative activity also offers some support for overturning the notion that society necessitates secrecy for a reasonable expectation of privacy. ECPA served as an early inhibitor to third party disclosure, mandating that electronic communications providers faced barriers to disclosing private wire, oral, and electronic communications information relayed through their networks.[87] The Health Insurance Portability and Accountability Act (HIPAA) limits third party disclosures, despite that fact that the individual has exposed his or her data to medical professionals. [88] While the ACLU notes that government agents can circumvent the HIPAA protections with

---

[83] *Id.* at 957. Judge Leon went so far as to refuse to apply the third-party doctrine to NSA surveillance, asking if "present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—[are] so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like Smith simply does not apply?" Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013), *vacated and remanded on other grounds*, 800 F.3d 559 (D.C. Cir. 2015). For an academic analysis of the third-party doctrine post *Jones*, see Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J. L. & TECH. 431 (2013).

[84] Riley v. California, 134 S. Ct. 2473, 2493 (2014) ("[A] warrant is generally required before such a search, even when a cell phone is seized incident to arrest.").

[85] *Id*. at 2494-95.

[86] *Id*. at 2493.

[87] Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22*, U.S. DEP'T OF JUSTICE (Jul. 30, 2013), https://it.ojp.gov/privacyliberty/authorities/statutes/1285.

[88] *Your Rights Under HIPAA*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

relative ease,[89] the legislation still reinforces the notion that privacy does not necessarily require secrecy. Thus, Congress has indicated that it does not want to equate privacy with secrecy. To the extent that Congressional intent reflects society's notions of reasonable expectations of privacy, legislative action indicates society's willingness to extend an expectation of privacy to private-but-not-secret information. Since "personal and societal values" influence the reasonable expectation of privacy analysis in the Fourth Amendment context,[90] legislative indicia of society's privacy expectations outline the proper contours for Fourth Amendment protections.

In sum, while the third-party doctrine still reigns supreme, judicial decisions consistent with legislative activity have slowly undercut the third-party doctrine's core equation between secrecy and privacy. Courts have begun to discuss the inapt appropriation of the old third-party doctrine to the reasonable expectation of privacy in a digital world. The following section argues that privacy interests implicated in social media surveillance offer a particularly robust case for demonstrating the need for the Fourth Amendment to better protect the privacy vulnerabilities created by modern digital behavior.

IV. REVISITING THE SCOPE OF REASONABLE EXPECTATION OF PRIVATE SOCIAL DATA

An increasingly powerful chorus of judicial voices has called for a reconsideration of the reasonable expectation of privacy for digital information.[91] The academic community has also grappled with the meaning of a reasonable expectation of privacy in an increasingly omni-connected world,[92] and has found the third-party doctrine "horribly wrong."[93] For example,

---

[89] *FAQ On Government Access To Medical Records*, AM. CIVIL LIBERTIES UNION, http://www.aclu.org/faq-government-access-medical-records.

[90] Tracey v. State, 152 So. 3d 504, 523 (Fla. 2014), *reh'g denied* (Dec. 8, 2014) ("The Supreme Court, in stating this principle, has clearly recognized protection of 'personal and societal values' regarding expectations of privacy that a society is willing to recognize even where such activities are not fully concealed." (citing California v. Ciraolo, 476 U.S. 207, 212 (1986)).

[91] *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *see also* United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (recognizing that Circuit Court judges would like to see a change to third-party doctrine, but must wait for Supreme Court action).

[92] *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1222-25 (2016) (reconceptualizing online service providers as subject to governance as information fiduciaries).

[93] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009) ("The third-party doctrine is the Fourth Amendment rule scholars love to hate. . . . The verdict among commentators has been frequent and apparently unanimous: The third-party doctrine is not only wrong, but

William Baude and James Stern have advocated applying a positive law model to replace the third party-doctrine.[94] David Sklansky believes that a reasonable expectation of privacy test misreads the spirit of the Fourth Amendment, and that courts must refocus on privacy as a sovereign zone of sanctuary.[95] Jed Rubenfeld has also considered the detrimental effects of technological developments on privacy interests in his aptly-named article, "The End of Privacy." Like Sklansky, Rubenfeld contends that courts must refocus Fourth Amendment jurisprudence away from the "Stranger Principle" embedded in the third-party doctrine in order to maintain a cognizable Fourth Amendment protection in the modern era.[96]

In this section, I argue that courts should reconsider the reasonable expectation of privacy of social data. I contend that government monitoring of private social media pages invades an even greater privacy interest than that of the home. I also argue that allowing for government monitoring of social media pages implicates individuals' First Amendment rights. Finally, I find that the balance between government interests and privacy interests favors applying Fourth Amendment safeguards in the case of covert friending, yet leaving voluntary information disclosures by third party connections beyond the scope of Fourth Amendment protections.

A. Special Considerations of Privacy for Private Social Media Data

While privacy advocates have many reasons to push for a broad reversal of the third-party doctrine, social media use offers an exceptionally striking case for the need to narrow the third-party doctrine loophole to Fourth Amendment protections. Under the governing third-party doctrine, social media users have no reasonable expectation of privacy of any

---

horribly wrong." (footnotes omitted)); *see also* David Alan Sklansky, *Too Much Information: How Not To Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1089 (2014) ("An all-or-nothing approach to privacy--denying that people have any interest in controlling the use or dissemination of information that is less than fully confidential--has long been, with justification, one of the most heavily criticized aspects of the Supreme Court's Fourth Amendment jurisprudence." (footnote omitted)).

[94] William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1871-73 (2016) (advocating the application of a positive law model to replace third-party doctrine).

[95] Sklansky, *supra* note 92 at 1107-10.

[96] *See* Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113 (2008) ("The only problem: the Stranger Principle is completely untenable. It implies that, once an individual has exposed information to a third party, the government may seize that information--with or without that third party's assistance. And that implication would spell the end of the Fourth Amendment almost altogether." (footnote omitted))

information that they post on their private networks because of the information exposed to their social media connections.[97] Allowing a general right to third party disclosure of private information for government use enables a relatively easy means of conducting invasive, widespread surveillance. Due to social media users' vulnerability to third party infiltration, active government surveillance can also dampen citizens' will to voice private dissent and exert a chilling effect on free speech.

1. Intrusive Social Media Monitoring

At present, government agents have the expansive ability to search private social media information, either through covert agent friending or through the cooperation of a social media friend. This creates the threat of extremely invasive violations of one's privacy. A search of social media information often reveals far more than a search of an individual's home, the archetypical locus of Fourth Amendment protections.[98] A government search of a private social media page can therefore pose an even more invasive threat to an individual's privacy.[99] Due to the plethora of associational and other intimate information repeatedly available through a user's social media homepage, government monitoring proves tantamount to ongoing surveillance. Like other forms of audio and video surveillance, social media monitoring tracks an unknowing user's behavior for extended periods of time. As a general rule, courts apply the Fourth Amendment more strictly to protect individuals where the government utilizes more intrusive methods of performing searches.[100]

Courts have distinguished the privacy intrusions implicated in a singular search versus those in a case of ongoing surveillance. Outside of the Fourth Amendment context, in the well-known *Nader* case, Chief Judge Fuld recognized that while "the mere observation of the plaintiff in a public place does not amount to an invasion of his privacy. . . .

---

[97] *See supra* p. 6.

[98] *See* Riley v. California, 134 S. Ct. 2473, 2491; Kyllo v. United States, 533 U.S. 27, 31 (2001).

[99] *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) ("[A]n explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button.").

[100] *See e.g.*, United States v. Wells, 739 F.3d 511, 518 (10th Cir.), *cert. denied,* 135 S. Ct. 73 (2014); *see also* United States v. Shabazz, 883 F. Supp. 422, 424 (D. Minn. 1995) (finding that the government's video and audio surveillance of a rented hotel room was "so massive and unregulated as to require the suppression of its product").

under certain circumstances, surveillance may be so 'overzealous' as to render it actionable."[101] The court goes on to state, "a person does not automatically make public everything he does merely by being in a public place."[102] In other words, the New York Court of Appeals found that merely exposing oneself to a public place does not compromise all legitimate expectation to privacy rights, and an extended surveillance campaign may breach an individual's right to privacy.

Other courts have applied a similar distinction between short searches and long-term surveillance when assessing government behavior. For example, in *Jones*, Justice Sotomayor and Justice Alito's concurring opinions differentiated between "short-term monitoring of a person's movements on public streets,' which would not infringe a reasonable expectation of privacy, and 'longer term GPS monitoring,' which would."[103] Similarly, the circuit court case leading to the *Jones* decision found evidence of state laws suggesting a "nationwide societal understanding" that prolonged GPS surveillance "defeats an expectation of privacy that our society recognizes as reasonable."[104] The D.C. Circuit court advanced a "mosaic theory of government surveillance, emphasizing that a key difference between a limited search and ongoing surveillance rests on the fact that the whole "reveals more—sometimes a great deal more—than does the sum of its parts."[105] In *United States v. Nerber*, the Ninth Circuit cites Ninth Circuit precedent[106] as well as decisions from the Fifth Circuit,[107] Seventh Circuit,[108] and Tenth

---

[101] Nader v. Gen. Motors Corp., 25 N.Y.2d 560, 570 (1970) (citation omitted); *cf.* United States v. Powell, 943 F. Supp. 2d 759, 776 (E.D. Mich. 2013) ("[W]arrantless long-term tracking by electronic means violates an individual's reasonable expectation of privacy . . . because the information obtained through such means is, in the aggregate, so comprehensive.")

[102] *Nader*, 25 N.Y.2d, at 570.

[103] United States v. Graham, 824 F.3d 421, 435 (4th Cir. 2016) (quoting United States v. Jones, 132 S. Ct. 945, 964 (2012)) (Alito, J., concurring in the judgment); *see also Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

[104] United States v. Maynard, 615 F.3d 544, 564 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[105] *Id.* at 558, ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation.")

[106] United States v. Taketa, 923 F.2d 665, 677 (9th Cir. 1991) ("[T]he silent, unblinking lens of the camera was intrusive in a way that no temporary search of the office could have been.")

[107] *See* United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987) (arguing that society considers Orwellian hidden video surveillance as more egregious than other kinds of intrusions).

[108] *See* United States v. Torres, 751 F.2d 875, 882 (7th Cir. 1984) ("We think it . . . unarguable that television surveillance is exceedingly intrusive, especially in combination (as here) with audio surveillance, and inherently

Circuit,[109] emphasizing the exceptionally intrusive nature of electronic video surveillance.[110] The *Nerber* Court also directly quoted Judge Kozinski, stating that "every court considering the issue has noted [that] video surveillance can result in extraordinarily serious intrusions into personal privacy.... If such intrusions are ever permissible, they must be justified by an extraordinary showing of need."[111] As such, case precedents suggest a higher bar for allowing warrantless government surveillance activity than a discrete search, indicating that warrantless social media monitoring amounts to "an extraordinary intrusion into personal privacy."[112]

The Ninth Circuit later distinguished the *Jones* decision as addressing only exceptionally invasive levels of surveillance. In *United States v. Wahchumwah*, the Circuit court explored a case where the defendant invited an undercover agent into the defendant's home, and the agent used a concealed audio-visual device during the course of the visit.[113] The court found significant that the surveillance only lasted for a few hours (versus the 48-hour GPS surveillance in *Jones*) and that the surveillance only transpired while the agent remained in the defendant's home.[114] When the government gathers private social media via surveillance techniques, the government could conceivably undertake searches limited to few hours, but agents would more likely conduct surveillance for a more extensive time period. The monitoring would therefore fall into the exceptionally invasive category even under the *Wahchumwah* test. Such a position remains consistent with *Katz*'s requirement for procedural safeguards to prevent permission for searching electronic surveillance to lay "only in the discretion of the police."[115]

---

indiscriminate, and that it could be grossly abused--to eliminate personal privacy as understood in modern Western nations.").

[109] *See* United States v. Mesa-Rincon, 911 F.2d 1433, 1442 (10th Cir.1990) ("Because of the invasive nature of video surveillance, the government's showing of necessity must be very high to justify its use"); *see also* United States v. Wells, 789 F. Supp. 2d 1270, 1273 (N.D. Okla. 2011), *aff'd*, 739 F.3d 511 (10th Cir. 2014) (Video and audio surveillance are highly intrusive forms of investigative mechanisms and, for that reason, have been subjected to a high level of scrutiny under the Fourth Amendment and the wiretap statute, with video surveillance deemed even more intrusive than audio 'bugging.' (citation omitted)).

[110] United States v. Nerber, 222 F.3d 597, 603-04 (9th Cir. 2000).

[111] *Id.* At 603 (citing United States v. Koyomejian, 970 F.2d 536, 551 (9th Cir.1992) (Kozinski, J., concurring)).

[112] *Nerber*, 222 F.3d at 603.

[113] United States v. Wahchumwah, 710 F.3d 862 (9th Cir. 2013).

[114] *Id.* at 868 ("[T]he GPS device in *Jones* enabled constant surveillance of a vehicle over a period of twenty-eight days, *id.* at 948, whereas the recording by Agent Romero lasted for only a few hours and for no longer than Romero remained an invited guest in Wahchumwah's home.")

[115] Katz v. United States, 389 U.S. 347, 359 (1967).

Courts have also found that the greater intrusiveness of new technologies require judges to reinforce constitutional safeguards to ensure that technological innovations do not erode traditional Fourth Amendment protections. For example, in *People v. Weaver*, the New York state court recognized that "contemporary technology projects our private activities into public space as never before."[116] However, the court argued that the technological advancement had not "been accompanied by any dramatic diminution in the socially reasonable expectation that our communications and transactions will remain to a large extent private."[117] Stated more broadly, the *Weaver* court adopted the position that technological developments should not dictate the level of privacy that society finds reasonable. While the Supreme Court's decision in *Kyllo v. United States* suggested that technology's integration into public use could eventually affect the analysis of an individual's reasonable expectation of privacy, *Kyllo* agreed with *Weaver*'s main thrust that technology should not dictate reasonable expectations of privacy.[118] The Sixth Circuit in *Warshak* interpreted *Kyllo* to stand for the proposition that courts needed to update the Fourth Amendment to "keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." [119] Thus, as technologies allow for more invasive surveillance, courts must ensure that the Fourth Amendment safeguards remain agile in protecting a reasonable expectation of privacy.

Finally, the fact that the government monitors private communications when searching social media data further bolsters the need for a strict application of Fourth Amendment protections. The Supreme Court has ruled that "broad and unsuspected government incursions into conversational privacy necessitate the application of Fourth Amendment safeguards." [120] As the discussion above demonstrates, government surveillance of social media data is both broad in scope and unsuspected by the social media publisher. Even in

---

[116] People v. Weaver, 12 N.Y.3d 433, 442-43, 909 N.E.2d 1195, 1200 (2009).

[117] *Id.*; *see also* State v. Jackson, 150 Wash. 2d 251, 263, 76 P.3d 217, 224 (2003) ("[U]se of a device that enabled the police to locate a person within a 40-mile radius day or night 'is a significant limitation on freedom from scrutiny' and 'a staggering limitation upon personal freedom.'") (citing State v. Campbell, 306 Or. 157, 172, 759 P.2d 1040, 1049 (1988)).

[118] Kyllo v. United States, 533 U.S. 27, 34 (2001) (suggesting that whether or not a surveying technology has entered general public use may affect the analysis of an individual's reasonable expectation of privacy, but reinforcing that changing technological abilities should not override expectations of privacy "with roots deep in the common law").

[119] United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) (citing *Kyllo,* 533 U.S. at 34).

[120] United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 313 (1972).

Smith, which developed the third-party doctrine, the Court found that the degree of the surveillance's intrusiveness affects the speaker's reasonable expectation of privacy (and thus impliedly the reasonableness of applying the third-party doctrine).[121] In sum, the particularly invasive nature of social media surveillance lends itself to a high level of privacy protection even in the case of limited third-party disclosures.

2. The Chilling Effect of Surveillance

Social media users have shown themselves to make poor privacy judgments. If the government can gather information without users' knowledge, the government surveillance practices would likely exert a chilling effect on private speech within social media networks.[122]

The empirics suggest that carelessness and a lack of information surrounding their social networking privacy render individuals extremely vulnerable to covert friend requests. As a result, the problem of misplaced trust appears to have vastly amplified in the social networking context, despite the disclosure of far more privacy-intrusive information. For example, one study found that forty-one percent of Facebook users would add a user posing as a plastic frog as a friend connection. In other words, nearly half of the study's users agreed to disclose their personal information despite the clear indication that by adding the "frog" connection, they shared personal information with an unknown stranger.[123] Another study of *college students* showed that "between twenty and thirty percent did not know how Facebook's privacy controls worked, how to change them, or even whether they themselves had ever changed them."[124]

One might respond by contending that this problem has an easy solution—social media users should take greater care

---

[121] Smith v. Maryland, 442 U.S. 735, 741 (1979) (holding that the pen registers did not capture content of communications and therefore played a less intrusive role).

[122] The academic literature offers a robust analysis on the chilling effects of surveillance. *See* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1442 (2011); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 143-44 (2007); Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups,* 46 ARIZ. L. REV. 621, 656-57 (2004); Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117 (2016).

[123] James Grimmelman, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009) (citing *Sophos Facebook ID Probe Shows 41% of Users Happy to Reveal All to Potential Identity Thieves*, SOPHOS (Aug. 14, 2007), http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html).

[124] Lauren Amy Gelman, Privacy, Free Speech, and 'Blurry-Edged' Social Networks, 50 B.C. L. REV. 1315 (2009).

in accepting individuals into their social networks. While it is undoubtedly true that individuals could greatly mitigate the threat by exercising greater caution in accepting unknown friend requests, it does not eliminate the problem altogether.[125] First, the nature of social networks creates incentives to share information with friends of friends,[126] but in order to reach those connections, the user has to trust that none of their hundreds or thousands of social connections has mistakenly added an undercover agent. Moreover, even if a user does not reveal their posts to second-degree connections, the mere revelation of an individual's information to a more immediate social network may implicate important privacy interests.

Even if no one accepted unknown social media access requests, covert government friending would still pose a problem. A covert agent could meet an individual in person before adding them on social media, thus providing a more compelling reason for acceptance. Through this tactic, covert agents could exercise invasive and suspicionless surveillance on a discrete group of people. For example, if a law enforcement agent wanted to monitor the behavior of a religious community, the agent could show up at a house of worship and meet members of the community. In this context, a subsequent friend request would not seem unwarranted, and the government agent would have extensive access to the privacy of the minority network, despite the lack of any reasonable suspicion. An agent could undertake this type of operation against another religious group, neighborhood community, or political group. As such, allowing covert friending may facilitate the very unreasonable searches that the Fourth Amendment aims to prevent.

This scenario of covert government "friending" does not exist in a hypothetical academic vacuum. To the contrary, the *New York Times* has reported that government agents have turned to social media sites to identify individuals who the FBI

---

[125] An informed minority problem poses a further problem to creating better privacy practices on social media platforms. Many platforms have overcome the informed minority problem by allowing users to custom-tailor their privacy settings. Thus, those users best educated about the privacy threats of social media use will set their privacy settings very narrowly or will not use the social media sites at all. However, the lack of transparency concerning the privacy settings of one's social media connections means that social media sites can mollify those most aware of the privacy risks while leaving the majority uninformed. *See* R. Ted Cruz & Jeffrey J. Hinck, *Not My Brother's Keeper: The Inability of an Informed Minority to Correct for Imperfect Information*, 47 HASTINGS L. J. 656 (1996).

[126] As Grimmelman finds, "Weak ties are essential for networking (whether it be finding a job or a spouse)." James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1175 (2009).

suspects of harboring a propensity for terrorism.[127] For example, an undercover agent sent a friend request to Hasan Edmonds, a suspected ISIS sympathizer, and maintained an online relationship that led to Edmonds' arrest on terrorism-related offenses.[128] Despite the FBI's widespread access to Edmonds' social media usage, the government did not ever need to approach a court to demonstrate the reasonable nature of its intrusive tracking into Edmonds' life. Moreover, the agents had no obligation to limit their search to Edmonds' own communication—when Edmonds allowed the agent access into his private social network, he also enabled the agent to monitor the social networking behavior of all of Edmonds' friends without any Fourth Amendment barriers.

Furthermore, social media usage has risen in prominence[129] to the extent that it plays a "vital role . . . in private communication."[130] As a result, the use of social media, like the use of traditional forms of communication, implicates free speech issues. Social media users leverage their platforms to air unpopular opinions within a safe, limited-access community. For example, in the wake of recent police shootings, some citizens expressed their approval of police violence.[131] While incitement to violence may result in criminal charges, one may expect that many others may legitimately fear government surveillance even without anything illicit to hide. As the Supreme Court notes, "History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."[132] Thus, a key feature motivating Fourth

---

[127] Eric Lichtblau, *F.B.I. Steps Up Use of Stings in ISIS Cases*, N.Y. TIMES (Jun. 7, 2016) http://www.nytimes.com/2016/06/08/us/fbi-isis-terrorism-stings.html.

[128] *Id*.

[129] *See e.g.*, Maeve Duggan, *The Demographics of Social Media Users*, PEW RES. CENT., (Aug. 19, 2015) http://www.pewinternet.org/2015/08/19/the-demographics-of-social-media-users (finding that fully 72% of online American adults use Facebook—a percentage that increases to 82% and 79% when analyzing the behavior of 18-29 year-olds and 30-49 year-olds, respectively).

[130] *Cf. Katz,* 389 U.S. at 352.

[131] Naomi LaChance, *After Dallas Shootings, Police Arrest People for Criticizing Cops on Facebook and Twitter*, INTERCEPT (Jul. 12, 2016), https://theintercept.com/2016/07/12/after-dallas-shootings-police-arrest-people-for-criticizing-cops-on-facebook-and-twitter.

[132] United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297 (1972). *See also* Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008) ("Surveillance or interference can warp the integrity of our freedom of thought and can skew the way we think, with clear repercussions for the content of our subsequent speech or writing. The ability to freely make

Amendment privacy protections relates to rights of free expression.

Courts have long considered the Fourth Amendment as a bulwark against infringements on private speech.[133] In the *Keith* Case, the Supreme Court expressed its concern that unchecked surveillance would chill freedom of speech.[134]

Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance.

. . .

The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.[135]

The *Keith* Court, writing over forty years ago, feared that allowing the government broad surveillance powers for national security matters would adversely affect the nation's public discourse. If citizens did not feel that they could express their thoughts in private spaces without fearing the notice of government listeners, citizens would not air their thoughts and dissent aloud and private discourse would suffer. As a result, the Court found that the electronic surveillance of defendants plotting to threaten national security still required a court-approved search warrant.[136] While the facts in *Keith* concern a matter of national security, the court's reasoning applies even more strongly regarding government surveillance without a specific national security justification. The Court addresses this explicitly: "Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."[137] Despite the Court's ruling that private speech considerations mandate a search warrant for government surveillance even in

---

up our minds and to develop new ideas thus depends upon a substantial measure of intellectual privacy. In this way, intellectual privacy is a cornerstone of meaningful First Amendment liberties.")

[133] In *Reno v. American Civil Liberties Union*, the Supreme Court clarified that the First Amendment applies to speech on the Internet. 521 U.S. at 885 (1997).

[134] United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297 (1972).

[135] *Id* at 313-314.

[136] *Id.* at 320.

[137] *Id*. However, as recognized in Laird v. Tatum, 408 U.S. 1 (1972), surveillance must be accompanied by a search; the potential for government behavior to create a subjective chilling effect on speech does not provide sufficient grounds for a cognizable First Amendment injury. *See* SOLOVE & SCHWARTZ, at 57.

national security situations, if a government agent adds an individual on a social network, that agent can monitor the entire social network without a search warrant without individualized suspicion. The risk of such extensive exposure could have "a most pernicious effect upon the dignity of man and it would surely lead to guarded conversations."[138] The fear of covert social media surveillance, particularly if the practice continues to emerge into widespread use, "is susceptible to abuse"[139] and could result in a severe chilling effect on private speech. Free speech concerns weigh in favor of limiting covert government surveillance.[140] As a result of the intrusiveness of social media monitoring, combined with public reliance on private social media networks as a forum for private speech, private social network data should receive a reasonable expectation of privacy.

B. Distinguishing Government Intelligence Tactics

Now that the Note has argued for a presumptive expectation of privacy, this Section will distinguish the two government intelligence-gathering tactics introduced in Part III.A. Despite the presumptive expectation of privacy in social media data, this Section contends that the government should have the ability to access social media information shared by a private friend without triggering the Fourth Amendment. Third party disclosures undertaken by cooperative social connections should not lie subject to Fourth Amendment protections. On the other hand, covert friending that results in indiscriminate searches of a private citizen's social data deserves a higher level of privacy protection.

Even if the third-party doctrine does not automatically negate all reasonable expectations of privacy in exposed information, citizens must still justify the expectation of privacy in consensually shared data. After all, social media users accept their friends with the assumption that their friends will access their published material.[141] As such, publishers have no illusion that no one will read their social

---

[138] Dietemann v. Time, Inc., 449 F.2d 245, 249 (9th Cir. 1971).

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

[140] United States v. Mayer, 503 F.3d 740, 753 (9th Cir. 2007) articulates a balancing test, finding that ". . . an investigation threatening First Amendment rights, like any government investigation, be justified by a legitimate law enforcement purpose that outweighs any harm to First Amendment interests."

[141] Maryland v. Macon, 472 U.S. 463, 470 (1985) ("A government agent, in the same manner as a private person, may accept an invitation to do business and may enter upon the premises for the very purposes contemplated by the occupant.")

media posts—in fact, social media elicits responses from other social media users in the network that explicitly remind posters that other users see their published social media information.[142]

Individuals must demonstrate a vital privacy interest to overcome their voluntary disclosure of social media information. In the case of voluntary third party disclosures to the government, the searched party cannot demonstrate such a high privacy interest. Both the government's more limited surveillance capacity as well as the disclosing party's First Amendment rights weighs towards allowing the government to freely search information disclosed by a third-party connection.

1. Surveillance Capacity

The nature of the cooperating party's consent limits the scope of the government's ability to search the disclosed social connection's network. A government agent would only have access to the information that the cooperating party chose to disclose.[143] If a third party shared access information to their social network account with an agent, the government may have a limited ability to wander through the social network unless the disclosing party had already viewed those files. In *Walter v. United States*, the Supreme Court held that the government could not view films provided by a private party that the private actors had not previously viewed.[144] However, the Court also found an exception for items in "plain view."[145] Due to the fact that the government would need to conduct digital searches to pull up the relevant information, searching the social media network for additional information would likely constitute "a significant expansion of the search" and require a search warrant.[146] This is particularly likely given

[142] This dynamic creates a contrast to United States v. Nerber, 222 F.3d 597, 604 (9th Cir. 2000), where the privacy damage came in part from a false sense of being alone.

[143] Walter v. United States, 447 U.S. 649, 657, 100 S. Ct. 2395, 2402, 65 L. Ed. 2d 410 (1980) ("If a properly authorized official search is limited by the particular terms of its authorization, at least the same kind of strict limitation must be applied to any official use of a private party's invasion of another person's privacy.")

[144] *Id.* (The projection of the films was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search.")

[145] *Id.* ("Even though some circumstances—for example, if the results of the private search are in plain view when materials are turned over to the Government—may justify the Government's re-examination of the materials, surely the Government may not exceed the scope of the private search unless it has the right to make an independent search.")

[146] *Id*. *See also* United States v. Galpin**,** 720 F.3d 436, 447 (2d Cir. 2013) (finding a need for "heightened sensitivity in the context of digital searches").

the Court's decision in *Riley v. California*, [147] limiting a warrantless search of a cell phone incident to arrest due to the invasive nature of searching such a vast store of digital data. For similar reasons, the government would probably not have permission to use an exposed account to view social media information published after the cooperating party exposed the social media data without receiving express consent.

Even if a third party could hand over a password and allow for an ongoing search without previously viewing all searched material, the fact that the duration and secrecy of the search would depend upon ongoing private party cooperation offsets the degree of privacy harm. When the government gains access to social media data through a cooperating party, the government has a more limited search capability—limited in both scope and time. For example, *Meregildo* involved a cooperating witness providing access to Facebook data, so the information that the government received remained contingent upon cooperating party's continued cooperation. [148] The cooperating party had the power to revoke government access to future social media data at any time, or could selectively share the information given to government agents.

In contrast, when a government agent gains direct access to social media communication, the target connection's consent allows for a far more expansive form of surveillance. Once an individual consents to an uncover agent's friend request, the agent has unfettered access to all of the target individual's social media data, as well as significant amounts of information from "friends of friends."[149] Without a private actor mitigating the government control over tracking an individual's activities, government monitoring imposes the level of extraordinarily intrusive surveillance addressed in Part IV.A.1.[150]

While government actors can take advantage of preexisting social media relationships, asking an individual to request access to another individual's social network for the express purpose of searching the target user's social data may pose an additional difficulty. The Fourth Amendment does not apply to searches undertaken by private parties, but only when

---

[147] Riley v. California, 134 S. Ct. 2473 (2014).

[148] This analysis sets aside the question of whether giving unrestricted access to another party violates the Terms of Service of a given social network, which goes beyond the scope of this Note.

[149] *See* United States v. Wahchumwah, 710 F.3d 862, 868 (9th Cir. 2013) (noting that the amount of time of a surveillance operation may substantively effect the privacy analysis). Once an individual accepts a covert agent's friend request, they can expect to remain friends for years.

[150] In United States v. Gatson, 2014 WL 7182275, at *22 (D.N.J. Dec. 16, 2014), Judge Martini dismissed these concerns with a cursory paragraph noting that "No search warrant is required for the consensual sharing of this type of information."

those parties do not act as agents on the government's behalf.[151] If the government commissioned the friend request, then the friend request constitutes government behavior and would fall under the covert friending analysis.[152] Due to the fact that disclosures by a cooperating party require the consent of a private intermediary, government surveillance capacity remains in greater check than the unchecked surveillance allowed through covert government friending.

2. First Amendment Rights

Regardless of how the third-party doctrine develops, private social media users should not face limits in their ability to disclose social media information to the government. Social media users have a far more direct relationship with their connections than they do with third party operators. Moreover, as discussed above, users post the information on their social media network for the benefit of their social connections. In fact, restricting social media connections to disclose troublesome material to law enforcement could infringe upon the social connections' First Amendment free speech rights. As the Court notes in *Fernandez v. California*, "Any other rule (that would forbid consensual disclosures) would trample on the rights of the occupant who is willing to consent."[153] Specifically, a third party connection might want the police to conduct a search in order to dispel any suspicion raised by their association with the suspect in question.[154]

Moreover, forbidding voluntary disclosures by cooperating third parties instills a socially detrimental policy. If a social media user finds that one of their social connections posts something so worrisome that the user turns to the police for help, it seems irrational to interfere with that report. While turning over social media data to law enforcement may violate the standard social norms governing social media use, limiting those disclosures would adversely affect communal well-being. Therefore, under any presumption of a reasonable expectation of privacy,[155] the law should not seek to limit third party

[151] United States v. Jacobsen, 466 U.S. 109, 113-14 (1984).

[152] For example, the Tenth Circuit utilized a two part test, asking "1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends." United States v. Ackerman, 2014 WL 2968164, at *7 (D. Kan. July 1, 2014). If the private party's friend request counts as government behavior, then the act receives an identical privacy analysis to cases where a covert government agent solicits social network access.

[153] Fernandez v. California, 134 S. Ct. 1126, 1137, 188 L. Ed. 2d 25 (2014).

[154] *Id.*

[155] And the fact that many users do not exhibit a subjective understanding that their social media data may end up as incriminating evidence.

disclosures from a cooperating party. In contrast, covert friending involves government actors acting in an official capacity, so these free speech concerns do not weigh as heavily.[156]

3. Power Differential

One might also challenge the distinction between government intelligence-gathering via a cooperating party and intelligence-gathering via covert government friending as involving the same level of risk. After all, if a defendant assumed the risk that one of his "friends" would alert law enforcement to the fact that he had committed a crime, the defendant equally assumes the risk that one of his "friends" is actually a law enforcement agent.[157] However, this creates a false comparison. Attempted comparisons between the government activity and private party activity ignore the power differential between the two groups.

Citizens and the police are not the same. We should never treat them the same. The police can do things that ordinary citizens cannot, for the most part, do: carry guns, lock people up, and conduct searches. The police benefit from default presumptions that ordinary citizens lack: police desires and actions are presumed to be consonant with their public protection mission, whereas the same desires and actions by a private person are presumptively illegal or criminal. The police are protected from consequences in a way that ordinary citizens are not.[158]

Erin Murphy eloquently dissects the power differences between police and citizens. As a result, individuals may justifiably maintain a reasonable expectation that they do not have to assume the risk of accidentally consenting to police spies conducting secret surveillance even if the same actions risk exposing the information via third party.

V. CONCLUSION

Reasonableness governs the Fourth Amendment privacy analysis. Traditionally, legal jurisprudence has not found a

---

[156] *See* Garcetti v. Ceballos, 547 U.S. 410, 421 (2006) ("[W]hen public employees make statements pursuant to their official duties, the employees are not speaking as citizens for First Amendment purposes, and the Constitution does not insulate their communications from employer discipline.")

[157] *See* United States v. Brooks, 2012 WL 6562947, at *3 (E.D.N.Y. Dec. 17, 2012).

[158] Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1249-1250 (2009).

reasonable expectation of privacy in social media data exposed to other connections in a private network. A public comment on a popular blog receives the same privacy protection as a comment on a private social media page—no privacy protection at all. This Note considers the possibility of government agents conducting warrantless searches of an individual's social media data through either the cooperation of a social network connection or through covertly friending social media users. In both scenarios, courts currently allow the government to monitor and search this information without a warrant. I argue for a reasonable expectation of privacy in social media data and a limitation on the third-party doctrine. When applied to two government surveillance strategies, I find that the government should have the ability to search information disclosures by third parties without a search warrant. However, I find that the Fourth Amendment requires the government to obtain a search warrant before searching and monitoring information acquired through the more intrusive covert friending strategy. Such a search restriction protects citizens from baseless government monitoring and helps mitigate concerns over a chilling effect on free speech. A probable cause standard would restore the proper balance between privacy interests and legitimate law enforcement interests.

Finally, the reasonable analysis ultimately rests on normative perspectives. The Supreme Court finds that the "the correct inquiry is whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment."[159] Of course, those values depend on society's willingness for a government imprint in their private lives. David Sklansky has suggested that modern Americans no longer care strongly about data privacy.[160] If he is right, then government surveillance may not constitute as great a harm. However, Sklansky recognizes that many academics disagree,[161] and the plaintiffs in *Clapper* offer empirical evidence to the contrary.[162] Either way, the Court's understanding of the Fourth Amendment protections remains in flux, and the next few years will likely both reflect and define society's reasonable expectations of privacy in social data.

---

[159] Oliver v. United States, 466 U.S. 170, 182-83 (1984)

[160] Sklansky, *supra* note 3 at 1086 ("people expect less privacy and do less to preserve it").

[161] *Id*., *supra* note 3 at 1094-1099.

[162] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013) (finding that respondents have failed to show impending injury despite fears of surveillance).