I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Status Update: When Social Media Enters the Courtroom[†]

LINDSAY M. GLADYSZ[*]

Abstract. In December 2010, Rodney Knight Jr. broke into Washington Post columnist Marc Fisher's Washington D.C. home, stealing two laptops, a winter coat, and cash. Proud of his heist, Knight uploaded pictures of himself and his loot onto Facebook using one of his newly pilfered computers. In an even more audacious move, Knight posted a picture of himself with a handful of the stolen cash on the victim's Facebook page. The Assistant United States Attorney General on the case, also adept at using the Internet, utilized the information to obtain a warrant and arrested Knight within a month. In the face of such evidence against him, Knight pled guilty. While this may seem like an extreme example, the use of information from Facebook and other social media sites is becoming an important part of police investigations and both criminal and civil litigation.

Due to the popularity and prevalence of social media, there is a multitude of information stored online and on third party servers. Users of social media have become accustomed to posting information depicting every minute detail of their lives, allowing friends and families to communicate easily and often. Status updates, personal information, and photographs loaded onto social media websites have become important sources of discovery in

---

[†] I would like to credit my note advisor, Professor Peter Swire, as well as the I/S Staff with their profound help on this Note. I would also like to extend sincere thanks to my wonderful parents and terrific friends for their support and to the ever-inspirational Brady Hoke.

[*] J.D. Candidate, expected 2012, the Ohio State University Moritz College of Law; B.A. 2009, University of Michigan.

litigation, as these sources make it easier and cheaper to obtain information than ever before. However, courtroom use of information from Facebook and other popular websites often happens largely unbeknownst to users. While E-discovery is an important tool for litigators, what privacy interests are we giving up for the use of this information? This Note addresses the current state of privacy law concerning electronic communications, E-evidence use, and what steps should be taken to protect users' privacy.

I. INTRODUCTION

Thanks to the wonders of social media, socialization and networking have evolved irrevocably.[1] With Facebook's active user base of more than 800 million,[2] the world is now connected and sharing information like never before. From constant status updates to photographs, users post and share information about their personal lives, often without considering any repercussions of such uploads. Law enforcement officials and legal professionals, realizing the value of such highly personal information on Facebook, have increasingly attempted to use such information as evidence at trial.[3] In 2010, a New York court ruled private information taken from a plaintiff's social networking site to be admissible because of its material and necessary nature, broadening previous standards of admissibility.[4] But *should* information gathered from social media be discoverable and admissible in the courtroom?

This Note examines the current legal landscape concerning the use of E-evidence from social media and the privacy and policy concerns that arise with such use. Part II of this Note gives a brief overview of social networking media and its effect on the law and current legal discourse. Part III reviews the most common types of cases that have seen admission of evidence from social media and recent cases dealing with the admission of such evidence. Part IV looks at prevailing

---

[1] RICHARD SUSSKIND, THE END OF LAWYERS? RETHINKING THE NATURE OF LEGAL SERVICES 77 (2010).

[2] *Facebook Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Feb. 1, 2012). Additionally, half of these active users log on every day. *Id.*

[3] Andrew C. Payne, Note, *Twitigation: Old Rules in a New World*, 49 WASHBURN L.J. 841, 845 (2010).

[4] Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 651 (N.Y. Sup. Ct. 2010).

privacy doctrines and the levels of privacy that govern current policy considerations, applying these levels to Facebook content. Finally, Part V examines the future of social media in the courtroom and argues for stricter standards of admissibility and user protection.

II. WELCOME TO THE CYBERWORLD

From humble beginnings at Harvard University in 2004, Facebook first expanded to other colleges, then eventually to anyone with an email address and a desire to socialize online.[5] Facebook's ever-evolving nature calls into question what reasonable expectations of privacy users have had at various points in its existence. What users may have considered quite private during Facebook's first years may no longer be seen as secure. Likewise, once information is uploaded, it is stored on Facebook's servers indefinitely, even when it is removed from the actual website.[6] Because of the expansion in the user base—from American college and university students to anyone in the world with Internet access—and the numerous changes in the interface, what constitutes a reasonable expectation of privacy is truly a good question. It is thus useful to examine the current statutory scheme regarding electronic communications, including social networking media.

A. THE FOURTH AMENDMENT

The Fourth Amendment protects the rights of United States citizens to be secure from "unreasonable searches and seizures."[7] But what qualifies as "reasonable" when it comes to social media remains

---

[5] *Facebook Company Timeline*, FACEBOOK, http://www.facebook.com/press/info.php?timeline (last visited Feb. 1, 2012).

[6] Bill Meyer, *Facebook Data-retention Changes Spark Protest*, CLEVELAND.COM (Feb. 17, 2009, 3:25 P.M.), http://www.cleveland.com/nation/index.ssf/2009/02/facebook_dataretention_changes.html; s*ee also* FACEBOOK DATA USE POLICY, http://www.facebook.com/about/privacy/your-info#deleting (last visited Feb. 1, 2012). If a user does delete his profile with potentially admissible evidence, Facebook will restore access if it is possible. DIGITAL FORENSICS & EDISCOVERY ADVISORY – FACEBOOK SUBPOENAS,CONTINUUM WORLDWIDE LEGAL SOLUTIONS (Oct. 13, 2010), *available at* http://www.continuumww.com/Libraries/PDFs/DF_eD_101310.sflb.ashx. Additionally, Facebook does urge users to use other means to obtain information if possible. *Id.*

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

an open question.[8] As Justice Rehnquist stated in *United States v. Knights*:

> The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.[9]

This balancing act often necessarily places individual interests at odds with those of the judicial system. Individuals want to protect their information from outside intrusion, but such information is at times essential to the promotion of justice. The current test for reasonableness, established in *Katz v. United States* and explored further in Part III of this Note, contains both subjective and objective components.[10] As a result, there are no easy answers as to what is reasonable—especially given the rapidly evolving nature of today's Web.

The Supreme Court has said that the Fourth Amendment "protects people, not places."[11] Though the Framers of the Constitution had no way of predicting the technological advances that have developed since America's birth, their ultimate intention was to protect individual liberties from unreasonable government interference.[12] The recognition of this intention has resulted in the broad interpretation (and reinterpretation) of the language of the Fourth Amendment with the advent of technological and social advances, which is necessary in order to develop the scope of the protections inherent in the Amendment.[13]

---

[8] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504–05 (2007).

[9] United States v. Knights, 534 U.S. 112, 118–19 (2001) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[10] Katz v. United States, 389 U.S. 347, 361 (2004) (Harlan, J., concurring).

[11] *Id.* at 351.

[12] Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 352–53 (2009).

[13] *Id.* As highlighted in Scolnik's article, even Originalist Justice Antonin Scalia commented in *Kyllo v. United States*, "It would be foolish to contend that the degree of privacy secured

Simply put, the Fourth Amendment limits government intrusion into private individuals' lives.[14] Despite this, there have been countless instances where courts found other legitimate government interests that outweighed Fourth Amendment privacy protections. In *Katz v. United States*, the Supreme Court held that the Fourth Amendment must be construed based on what the writers of the Constitution considered "unreasonable search and seizure" and does not absolutely shield an individual's privacy from investigation.[15] Under this Originalist perspective, the Fourth Amendment does not apply as strongly to electronic information, which exists outside of the home, as it does to physical objects contained in the home, such as papers or other items.[16] Additionally, because of the "reasonable expectation of privacy" test and concerns about overreaching government intrusions, especially those pertaining to emerging technologies, Congress began promulgating statutes defining reasonable expectations of privacy as applied to specific items and places, leading to the first wiretapping laws and other related statutes.[17]

In defining the limits of the Fourth Amendment, the legislature and courts have struggled with balancing an individual's privacy concerns with the compelling need for information. Recent years have seen the ratification of the Patriot Act and Freedom of Information Act, which have reframed some privacy rights and invoked the compulsory release of stored information at both the federal and state level.[18] Such statutes have allowed law enforcement greater use of surveillance mechanisms, especially by electronic means, and have bypassed some of the statutory protections in place.

---

to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." Kyllo v. United States, 533 U.S. 27, 33–34 (2001). A staunch Originalist, Scalia nevertheless observed the dangers inherent if the Fourth Amendment was not construed in a flexible manner. Such flexible interpretation would thus ensure "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 34.

[14] Nicholas Matlach, Comment, *Who Let the* Katz *Out? How the ECPA and SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles in* Katz v. United States *Will Fix It*, 18 COMMLAW CONSPECTUS 421, 422 (2010).

[15] *Katz*, 389 U.S. at 361.

[16] Sarah Salter, *Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages*, 32 HASTINGS COMM. & ENT. L. J. 365, 370-71 (2010).

[17] Matlach, *supra* note 14, at 424–26.

[18] Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 311 (2011); *see also* Salter, *supra* note 16, at 372.

B. THE 2006 E-DISCOVERY AMENDMENTS

Due to the rapid development and evolution of technology, Congress and state legislatures have had a difficult time keeping up with promulgating changes in the law, often leaving courts to construct new common law through their jurisprudence.[19] Despite the difficulties inherent in enacting and amending laws to keep pace with new information technologies, there have been several advances.

In 2006, the E-discovery amendments were added to the Federal Rules of Civil Procedure, creating distinctions between paper and electronic documents.[20] Before the adoption of formal rules governing E-discovery, courts generally admitted any relevant computerized evidence.[21] However, as technology progressed and the admission of E-evidence became litigated more often, the courts and Congress came to a consensus that "digital is different" and began looking at revisions to the existing statutes.[22] An amendment to Rule 34 added the term "electronically stored information" to the types of documents that may be requested[23] and specified procedures for requesting electronically stored information.[24] The Advisory Committee defined "electronically stored information" rather broadly, including information "'stored in any medium' to encompass future developments in computer technology."[25]

The Committee also made changes to Rule 26's duty to disclose, creating "specific limitations on electronically stored information."[26] Under the new two-tiered approach: (1) parties must disclose information if it is at no undue burden or cost (by request or court order) and; (2) the court may yet order discovery if it finds good

---

[19] Payne, *supra* note 3, at 850. As one scholar humorously observed: "Modern communication follows Moore's law: technology grows exponentially. Congress follows the turtle law: slow and steady wins the race." Matlach, *supra* note 14, at 457.

[20] Payne, *supra* note 3, at 856.

[21] *Id.* at 851.

[22] *Id.*

[23] FED. R. CIV. P. 34(a)(1)(A).

[24] FED. R. CIV. P. 34(b)(1)-(2).

[25] FED. R. CIV. P. 34 advisory committee's note (2006 amendment).

[26] FED. R. CIV. P. 26(b)(2)(B).

cause—even if showing undue burden or cost is made.[27] These moves by the legislature, while seemingly minor in nature, indicate a congressional stance toward disclosure, rather than disallowance, of electronic information.

C. ELECTRONIC COMMUNICATIONS PRIVACY ACT

With the Electronic Communications Privacy Act (ECPA), Congress sought to extend the protections of wiretapping laws specifically to new forms of electronic communications.[28] While the act is primarily aimed toward electronic communications, the language of the act recognizes that the legislation's goal is to protect the "sanctity and privacy of the communication."[29] Despite Congress's goal of extending greater protections to emerging technologies, the courts have often held that little constitutional protection from the prevailing Fourth Amendment shield is allotted to communications that are open to the public.[30] In these rulings, the courts often cite the absence of a reasonable expectation of privacy when stating that the communications lack Fourth Amendment protection. This is where electronic surveillance law steps in: legislation, such as the ECPA, operates independently of the Fourth Amendment.[31] Because of this, even if a search is deemed reasonable under the Fourth Amendment, these laws can work to bar such evidence (and vice versa).[32]

The ECPA is the progeny of the Communications Act of 1934, which authorized the Federal Communications Commission to regulate common carriers, such as telephone companies and prohibited the unlawful interception of voice communications without the user's consent.[33] In *United States v. Rathbun*, the Supreme Court

---

[27] *Id.*

[28] Electronic Communications Privacy Act, 18 U.S.C. § 2511 (2006).

[29] 132 Cong. Rec. 14, 886 (1986) (statement of Rep. Kastenmeier).

[30] *See, e.g.*, Freedman v. Am. Online, 412 F.Supp. 2d 174, 181 (D. Conn. 2005); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004).

[31] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 303 (3d ed. 2009).

[32] *Id.*

[33] Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1103–04 (1934); *see also* Matlach, *supra* note 14, at 426 (examining Congress's policies in enacting the Communications Act of 1934).

ruled that only one party to a telephone conversation needs to consent for interception of the conversation to be lawful under the Communications Act.[34] However, unlike the Stored Communications Act (discussed below), the complicated definitions and additional statutory requirements make obtaining warrants under the ECPA extremely difficult.[35] Described as a "'super' warrant,"[36] law enforcement officers must submit a warrant request containing sworn statements and the specific nature and location of the communications sought to justify the interception.[37]

The ECPA is only marginally applicable to social networks because of the limited types of communications it governs. The ECPA applies to any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[38] As such, the ECPA only applies to communications in transmission—from the moment the communication is sent until it is opened—but does not apply to communications that have already been delivered to the recipient or that are "stored communications."[39] Communications governed by the ECPA are subject to stringent standards of discoverability, while communications that have already been delivered to the recipient are governed by the Stored Communications Act, as explored below.

D. THE STORED COMMUNICATIONS ACT

The Stored Communications Act (SCA), which governs social media such as Facebook and e-mail communications, prohibits entities such as Facebook and MySpace from disclosing personal information to the government without the account owner's consent.[40] While the SCA was generally intended to cover email, text messages,

---

[34] Rathbun v. United States, 355 U.S. 107, 111 (1957).

[35] Matlach, *supra* note 14, at 443.

[36] Salter, *supra* note 16, at 373.

[37] *Id.*

[38] 18 U.S.C. § 2511(1)(a).

[39] Matlach, *supra* note 14, at 448–49.

[40] Stored Communications Act, 18 U.S.C. § 2701(a)(1)-(2) (2006).

and online bulletin boards,[41] it arguably also applies to communications on Facebook because such communications are stored on Facebook's servers (though the courts have yet to rule on this application definitively).[42] The SCA was designed to balance the government's legitimate interest in gaining access to information with the privacy rights of individuals who have entrusted their communications to Internet service providers.[43] Despite this protection, courtrooms are admitting such social media evidence largely unbeknownst to the user base and with consequences that remain to be seen.

Enacted in 1986, the Stored Communications Act was designed by Congress to create a zone of privacy, protecting Internet users' personal information while balancing the countervailing need for access to that information.[44] This "Fourth Amendment Lite" was created to bridge the gap in the Fourth Amendment created by new technologies, ensuring the continued vitality of the Amendment, and to protect against the erosion of privacy rights.[45] In enacting the SCA, Congress had two main goals: to prohibit Internet Service Providers (ISPs) from voluntarily releasing stored information and to ensure that law enforcement officials have a vehicle by which to access stored communications if such communications were reasonably necessary to protect litigants from injustice.[46] To carry out these goals, Congress

---

[41] Timothy G. Ackermann, *Consent and Discovery Under the Stored Communications Act*, FED. LAW. 42, 43 (2009).

[42] Payne, *supra* note 3, at 848. There has been one court order applying the SCA to social media E-evidence, where the subpoena was to the websites themselves. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010). The *Crispin* court held that Facebook and other social media sites were electronic communications services, and therefore subpoenas to these sites for private messages could be quashed. *Id.* at 991. The SCA does not apply, however, where the subpoena is for wall posts or other "public" messages. *Id.* at 990. As explained in this section, it also does not apply if the subpoena is to an individual, whether a party or non-party, as the SCA only governs communications service providers. Largent v. Reed, No. 2009-1823, 2011 WL 5632688, *11–12 (Pa. Com. Pl. 2011) (Trial Order).

[43] Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 569 (2007).

[44] 18 U.S.C. §§ 2701–2712; *see also* Ackermann, *supra* note 41, at 42.

[45] Zwillinger & Genetski, *supra* note 43, at 575–76.

[46] *Id.* at 576.

enacted a categorical ban on ISPs voluntarily releasing information, as well as a series of exceptions, found in 18 U.S.C. § 2703, which enable law enforcement officials to seek disclosure through a precise process.[47]

As opposed to the ECPA, the SCA governs communications once they are received and stored, whether in a user's inbox or in other document storage.[48] Within 180 days of transmission, a warrant is required to allow the government access to the communications; however, after 180 days have passed, law enforcement officials simply need a subpoena or court order, which merely requires a showing of probable cause.[49] Whether a communication is in transmission or has been received, pinpointing the instant at which a communication becomes "stored" is an important issue due to the much higher standards governing the disclosure of communications under the ECPA.[50]

The SCA applies to service providers as parties in civil litigation, as well as to non-parties, disallowing disclosure of electronic communication in their possession.[51] In general, the SCA prohibits electronic communications services, which enable the sending of messages between users, from knowingly divulging information without the user's permission. Under the exceptions of the Stored Communications Act, electronic communications services may voluntarily divulge the contents of online communications if "lawful consent" is given by the account holder—whether he or she is the sender or recipient of the communication.[52] Like the ECPA, the SCA only requires the consent of one party for disclosure of a communication to be lawful.

Issuing subpoenas to Internet Service Providers (ISPs) presents an additional question for the courts and legislature. If a party seeks information that falls under the statutory authority of the SCA, the party seeking admission must first ascertain who has control over the communication—whether it is a party to the proceeding or a third

---

[47] *Id.*

[48] Matlach, *supra* note 14, at 448–49.

[49] Scolnik, *supra* note 12, at 382–93; *see also* 18 U.S.C. § 2703(b) (2008).

[50] Matlach, *supra* note 14, at 449; *see also* Salter, *supra* note 16, at 368.

[51] Ackermann, *supra* note 41, at 42.

[52] 18 U.S.C. § 2702(b)(3) (2008); *see also* Ackermann, *supra* note 41, at 43.

party—and then petition the court to compel disclosure or consent.[53] While the issue has not been decided definitively, several courts have quashed subpoenas to ISPs seeking the release of electronic communications.[54] This is not the case, however, when the subpoena is directed to the person who controls the information; under Federal Rule of Civil Procedure 34, when discovery is directed to a sender, recipient, addressee, or subscriber who exercises control over the communications, such communication is subject to discovery.[55] Further, in *Flagg v. City of Detroit*, the court not only held that a court has the ability to order a person to produce documents, but that it can order that person to give consent so someone else can disclose documents and communications on their behalf.[56] Further, courts may seek disclosure of information from whoever controls the communication, even if that person is not a party in the proceeding.[57] However, just because the court possesses the power to compel consent does not mean it must always exercise such power upon request. Rather, a court must weigh the communication's value against privacy considerations.[58]

When seeking evidence from Facebook, the "third party" is often Facebook itself. Since all material posted on the website is accessible by the company, the party seeking admission must simply petition the court to compel consent or disclosure from Facebook.[59] While this is an easy and direct course to the information, what are the costs associated with such free access? The next section examines current

---

[53] Ackermann, *supra* note 41, at 46.

[54] *See, e.g.*, *In re* Subpoena Duces Tecum to AOL, LLC, 550 F.Supp.2d 606 (E.D. Va. 2008); Hone v. Presidente U.S.A. Inc., No 5-08-MC-80071-JF, 2008 U.S. Dist. LEXIS 55722 (N.D. Cal. July 21, 2008)(unpublished); J.T. Shannon Lumber Co v. Gilco Lumber Inc., No. 2-07-cv-119, 2008 WL 3833216 (N.D. Miss. Aug. 14, 2008), *reconsideration denied*, 2008 WL 4755370 (N.D. Miss. Oct. 29, 2008).

[55] FED. R. CIV. P. 34(a)(1).

[56] Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008).

[57] Thomas v. Deloitte Consulting LP, No. 3-02-cv-0343-M, 2004 WL 1372954, at *4 (N.D. Tex. June 14, 2004).

[58] *In re* J.T. Shannon Lumber Co., No. 2-07-cv-119, 2008 WL 4755370, at *1 (N.D. Miss. Oct. 29, 2008).

[59] Facebook's Terms of Service even explicitly state to users that they will comply with legitimate law enforcement requests for information. FACEBOOK DATA USE POLICY, http://www.facebook.com/about/privacy/other (last visited Feb. 1, 2012).

jurisprudence, focusing on the areas of law that have seen the greatest advancement in the use of social media E-evidence.

III. CURRENT E-EVIDENCE JURISPRUDENCE

While every area of law may soon see social media introduced into the courtroom, there are several practice areas that have encountered this issue the most in recent years. Since 2008, federal judges have issued more than two dozen search warrants granting access to individuals' private Facebook profiles, and the trend is increasing. In fact, 2011 saw more than double the number of search warrants granted than in 2010.[60] Where courts have allowed evidence from Facebook, generally it has been evaluated on a case-by-case basis, with judges carefully weighing the benefits and allowing only that which is probative and relevant to the outcome of the case.[61] As such, it is beneficial to understand how information from Facebook is being used in these areas and how the bench is coming to understand this novel type of evidence.

A. INSURANCE AND PERSONAL INJURY CASES

In tort cases involving insurance and personal injury, introduction of material from Facebook is often used to combat claims of serious injury. Typical examples of this type of use include insurance companies seeking to admit evidence from an allegedly injured plaintiff's page that illustrates an active, happy life.

In *Romano v. Steelcase*, the Suffolk County Supreme Court in New York allowed evidence from Facebook to disprove the plaintiff's claims that her injuries resulted in a serious loss of enjoyment of life.[62] While

---

[60] Jeff J. Rogers, *A New Law-Enforcement Tool: Facebook Searches*, THOMPSON REUTERS (July 12, 2011), http://newsandinsight.thomsonreuters.com/Legal/News/2011/07_-_July/A_new_law-enforcement_tool__Facebook_searches.

[61] *See, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 654 (N.Y. Sup. Ct. 2010)

[62] *Id.* at 651. While *Romano* is not the most recent case, it has set the precedent of allowing such breadth of information. A subsequent case has followed *Romano*'s example, granting a motion to compel evidence from social media sites where there is a high chance of relevant information and the plaintiff puts his or her personal condition at issue. *See* Zimmerman v. Weis Markets, Inc., No. cv-09-1535, 2011 WL 2065410, at *6 (Pa. Com. Pl. 2011). The *Zimmerman* court did add, however, "fishing expeditions will not be allowed," only compelling access when non-private information suggests relevant information resides on the private page. *Id.* at *6 n.8.

Romano is a lower court decision, the case received media attention because of the unprecedented breadth and type of information allowed.[63] The defendant sought information from the plaintiff's current and historical Facebook and MySpace pages—including private and deleted material—which was postulated to contain information relating to the extent of the plaintiff's injuries. Notably, the defendant contended that the plaintiff's Facebook and MySpace pages contained images of her on vacation and engaging in an active lifestyle. The plaintiff had previously claimed such activities were unfeasible due to her injuries, which had allegedly confined her to her house and bed.[64] After viewing the public postings on the plaintiff's social media pages, the court stated that there was a high likelihood that highly relevant material would be found on her private pages and may lead to the discovery of admissible evidence.[65]

The *Romano* court used a test of "usefulness and reason" for the information requested, but stated that public policy weighs heavily in favor of open disclosure.[66] Significantly, the court noted that "[p]laintiffs who place their physical condition in controversy, may not shield from disclosure material which is necessary to the defense of the action,"[67] thus permitting discovery of materials relevant both to the extent of the injuries and damages. Denying the defendant access to the pages, the court noted, would only "condone Plaintiff's attempt to hide relevant information behind self-regulated privacy settings."[68] The court also stated that the production of information from Facebook and MySpace was not violative of the plaintiff's privacy, and that any such concerns are outweighed by the need for the information.[69] Indeed, the court cited the very nature of social networking websites—designed to share personal information with

---

[63] Andrew S. Kaufman, *The Social Network in Personal Injury Litigation*, N.Y.L.J., Dec. 15, 2010, at 1–2, *available at* http://kbrlaw.com/kaufman6.pdf.

[64] *Romano*, 907 N.Y.S.2d at 654.

[65] *Id.* at 655.

[66] *Id.* at 652.

[67] *Id.*

[68] *Id.* at 655.

[69] *Id.*

one's social network—as evidence of the lack of a reasonable expectation of privacy.[70]

Other personal injury cases follow similar fact patterns to that in *Romano*. In *Ledbetter v. Wal-Mart Stores, Inc.*, the court denied the plaintiff's motion for a protective order on information from Facebook, MySpace, and other social media sites, finding that such information is reasonably calculated to lead to the discovery of relevant and admissible evidence.[71] The defendant sought the information to disprove the plaintiff's injury claims and his wife's loss of consortium claims. Additionally, the court stated that by injecting the issue of the relationship between herself and the plaintiff into the courtroom, co-plaintiff Disa Powell waived any spousal privileges she may have had.[72]

Foreign courts have established more concrete discovery procedures pertaining to social media. For example, in *Leduc v. Roman*, the Ontario Superior Court of Justice affirmed a lower court holding that postings on the plaintiff's Facebook profile were documents within the meaning of the Rules of Civil Procedure and therefore must be produced if relevant to the action at issue.[73] Leduc commenced the action after a motor vehicle accident, asking for damages for loss of enjoyment of life; however, images and postings on the plaintiff's Facebook showed him fishing and enjoying other physical activities. Thus, the court concluded that Leduc had an obligation to produce any relevant documents, including information from Facebook.[74] As evidenced in the above cases, the social nature of Facebook and related sites can contain a treasure trove of information regarding a plaintiff's injuries, or lack thereof, leading judges to often allow such evidence into trial.

B. DIVORCE AND CUSTODY CASES

In family law cases, social media evidence is often requested as proof of a party's character or fault in the matter, including evidence

---

[70] *Id.* at 657.

[71] Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *1 (D. Colo. Apr. 21, 2009).

[72] *Id.*

[73] Leduc v. Roman, 308 D.L.R. (4th) 353 (Can. Ont. Sup. Ct. J. 2009).

[74] *Id.*

of extramarital affairs and engagement in activities that would adversely affect the best interests of a child. While it is not uncommon for parties to introduce evidence of their opponent's character flaws in order to gain a favorable divorce settlement or custody agreement, taking such evidence from social media sites is not directly analogous to more conventional forms of evidence.

Individuals who have everyday access to a party's Facebook account generally are allowed to use such information in court; since the parties are "friends," there is no expectation of privacy between them. However, due to the embattled nature of many family law proceedings, it is common for estranged spouses to "unfriend" each other—disallowing access to the page if privacy settings dictate as such. Though it has been established that, absent password protection, information on a shared spousal computer does not have a reasonable expectation of privacy,[75] the quasi-private nature of Facebook complicates matters. Despite this, courts are increasingly inclined towards admitting E-evidence from Facebook in family law cases, favoring open disclosure over any possible privacy concerns.

In *Dexter, II v. Dexter*, an Ohio Court of Appeals custody case, the court held that the trial court did not abuse its discretion in its grant of custody, which was based in part on the mother's MySpace profile.[76] The mother contended that the trial court erred in considering her religion, lifestyle choices, and other information from her profile, absent any evidence that such matters adversely affected the child.[77] In her public MySpace blog, the mother had written about her sado-masochism, bisexuality, and paganism. The trial court allowed this evidence and concluded from the evidence that such personal choices would have an effect on her child. Courts in similar cases have also chosen to allow evidence from social media to determine parental fitness or settle divorce proceedings, deeming such information relevant in determining a litigant's character and permitting it to influence the outcomes of such cases.[78]

---

[75] Camille Calman, *Spy vs. Spouse: Regulating Surveillance Software on Shared Marital Computers*, 105 COLUM. L. REV. 2097, 2098 (2005).

[76] Dexter, II v. Dexter, No. 2006-p-0051, 2007 WL 1532084, at *7 (Ohio Ct. App. 2007).

[77] *Id.* at *4.

[78] *See also*, B.M. v. D.M., 927 N.Y.S.2d 814, at *5 (N.Y. Sup. Ct. 2011) (where the court allowed evidence from the wife's blog and Facebook about her belly dancing in a divorce proceeding); *In re* T.T., 228 S.W.3d 312, 322–23 (Tex. App. 2007) (court allowed evidence from MySpace in a case involving termination of parental rights).

C. CRIMINAL CASES

Criminal courts and police departments have also begun to utilize information from Facebook and other social media sites to gather information and to prosecute criminals. Indeed, some criminals have been foolish enough to brag about their illegal acts via Facebook, as in the case of a recent burglar who not only uploaded pictures of himself with his stolen spoils onto his Facebook page, but then also "friended" the man that he burgled (and was promptly thereafter arrested).[79]

While it is possible that social media can serve directly as evidence of the crime at trial, it is more often the case that such evidence is used to illustrate a defendant's character and lifestyle.[80] Law enforcement officers are able to see any publicly posted photographs and use them either as supplemental information about a party or even as evidence that a crime was committed.[81] While most (though probably not all) criminals would be surreptitious enough to resist posting updates or pictures of an assault or robbery, lesser crimes, such as underage drinking or driving under the influence, are more commonly shared online. This is especially the case for Facebook because of its largely young user base; college students upload photographs from late Saturday nights without considering the consequences, which can be harsh.[82]

A now-infamous example of the use of such postings happened after a Pennsylvania State University football game in October 2005. Photographs taken at a post-game riot soon turned up on Facebook, which the police then used to identify and cite about fifty students.[83] Similarly, in 2007, evidence from Facebook was used by the University of Connecticut Police to link a driver to a hit and run incident.[84] Additionally, prosecutors have used E-evidence in drunk

---

[79] Gabe Acevedo, *World's Dumbest Criminal Would Like to Add You as a 'Friend'*, ABOVE THE LAW (Mar. 11, 2011), http://abovethelaw.com/2011/03/worlds-dumbest-criminal-would-like-to-add-you-as-a-friend.

[80] Daniel Findlay, *Tag! Now You're Really "It" What Photographs on Social Networking Sites Mean for the Fourth Amendment*, 10 N.C. J. L. & TECH. 171, 171 (2008).

[81] *Id.* at 176–79.

[82] *Id.* at 171–72.

[83] Matthew J. Hodge, Comment, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and Myspace.com*, 31 S. ILL. U.L.J. 95, 95 (2006).

[84] Edward M. Marsico, Jr., *Social Networking Websites: Are Myspace and Facebook the Fingerprints of the Twenty-First Century?*, 19 WIDENER L. REV. 967, 969–70 (2010).

driving trials, showing photographs of defendants in an embarrassing light—evidence that such defendants habitually engage in irresponsible behavior or are unrepentant since their D.U.I. arrest.[85]

Evidence from Twitter and Myspace has also been used by police to gather information about gang activity.[86] Suspects who cannot resist bragging online about their latest gun purchase or extortion end up aiding police and district attorneys in their own prosecutions.[87] Using photos of gang symbols or weapons on Facebook and Myspace pages, law enforcement officials have been able to identify and gather information about potential suspects.[88]

Other issues arise when evidence from Facebook is used in criminal cases. Unless the information is publicly available, under the Stored Communications Act the State will likely need to serve Facebook itself with legal process in order to obtain the information.[89] This, by itself, does not present a large hurdle for the prosecution. Questions do arise, however, concerning whether the defendant has the same ease of access to social media information. While criminal defendants do have access to any messages sent to or by them personally, they may not be able to obtain access to alleged victims' profiles and deleted material, and may therefore lose an opportunity for a defense.[90] Additionally, while governmental entities are granted an exception to the blanket protections of the Stored Communications Act, defendants do not have that benefit.[91] It thus becomes a question of fairness as to whether criminal defendants should have the same reasonable access to social media information that is afforded to the prosecution.

---

[85] Findlay, *supra* note 80, at 178.

[86] Marsico, *supra* note 84, at 970.

[87] *Id.* at 972. This is most often the case with career criminals, who take pride in their criminal activities and are therefore the most likely to post about them online. *Id.*

[88] *Id.*

[89] Zwillinger & Genetski, *supra* note 43, at 580.

[90] *Id.* at 385.

[91] *Id.* at 590–91; *see also* 18 U.S.C. § 2702 (2008).

D. VOIR DIRE AND OTHER JURY CONSIDERATIONS

The latest way that attorneys are using social media to further their clients' interests is through jury selection; Facebook and other social media sites are valuable in the determination of which potential jurors are most favorable to a litigant's case.[92] While tangential to the direct issue of E-evidence admissibility, this emerging area is proving to be ripe with issues of its own. If used free from any deceit, potential jurors' online profiles can offer a host of information which may prove quite significant in determining the jurors with the "right" characteristics for a particular case—especially since some of the information may contain information about subjects disallowed from voir dire questioning. Attorneys and jury experts look at such profile details as: favorite television programs, which may indicate a bias, especially if those shows are crime-related; number of friends, which may indicate an ability to be swayed; and rants or especially strong-opinioned Tweets, which can suggest that such a person might dominate jury deliberations, or may even run the risk of posting information from the case and causing a mistrial.[93] Social media is especially useful in the jury selection context because parties usually have limited time to question potential jurors, in addition to the candid nature of some posts—a quality not often found in juror questioning. However, this area of use is not without controversy. Privacy experts argue that using social networks to investigate private citizens is invasive, and some experts also argue that it may grant unfair advantage to those with resources to bring in the required equipment. Additionally, scholars question the veracity of online profiles to begin with.[94] Even more controversial is the proposition of granting potential jurors free wireless Internet access during their time at the courthouse if they agree to give the lawyers access to their private Facebook accounts (which is generally met with apprehension from the jury pool).[95] Despite the seemingly lax restrictions on such

---

[92] Ana Campoy & Ashby Jones, *Searching for Details Online, Lawyers Facebook the Jury*, WALL ST. J. (Feb. 22, 2011), http://online.wsj.com/article/SB10001424052748703561604576150841297191886.html.

[93] *Id.*

[94] *Id.*

[95] *Id.* Such access would be granted through temporarily "friending" a certain legal office. Jurors found this practice invasive, not seeing the reward of temporary Internet access attractive enough to allow the litigators to invade their private lives. *Id.*

use of social networking sites, this is one area that may soon be regulated and followed more closely by ethics committees. Until then, it remains an ethically ambiguous—yet perfectly legal—tool at a litigator's disposal to sway the outcome of the case favorably for his or her client.

Further, courts are beginning to limit jurors' use of Facebook inside and outside the courtroom. Some jurisdictions are adding policies and specialized rules to jury instructions about the use of social media and other Internet tools for independent research on the players of their trial. As far-fetched as this may seem, instances of jurors polling their Facebook friends on which way to vote, "friending" parties in the proceeding, or blogging about jury deliberations have made such measures necessary.[96] Some states, such as Michigan, New York, Oregon, Texas, and Alaska, have baned jurors from bringing their cellular phones into the courtroom or jury deliberations in reaction to several instances where jurors were Tweeting during the trial.[97] Other states have added sections to their jury instructions explicitly explaining that Googling or otherwise searching online for parties to the proceeding is not allowed.[98] Courts across the nation have begun to examine the promulgation of new rules individually, but the trend in restricting use in order to avoid improper Internet communications—and possibly a mistrial—is becoming stronger throughout the country and will most likely become more prevalent in coming years.

IV. REALMS OF PRIVACY IN THE FAR REACHES OF CYBERSPACE

In addition to statutory protections—or lack thereof—promulgated by Congress, important doctrines have emerged from common law jurisprudence and privacy policy that have affected and continue to shape the legal conversation concerning social media E-evidence. This section explores such over-arching doctrines, applying them by example to relevant Facebook communications.

---

[96] *See* Sharon Nelson, John Simek & Jason Fotlin, *The Legal Implications of Social Networking*, 22 REGENT U. L. REV. 1, 3 (2010); *see also* Eva-Marie Ayala, *Tarrant County Juror Sentenced to Community Service for Trying to 'Friend' Defendant on Facebook*, FORT WORTH STAR-TELEGRAM (Aug. 28, 2011), http://www.star-telegram.com/2011/08/28/3319796/juror-sentenced-to-community-service.html.

[97] Nelson, Simek & Foltin, *supra* note 96, at 5–6.

[98] *Id.* at 6–7.

A. KATZ'S LEGACY

The case of *Katz v. United States* has become a landmark opinion in the area of privacy law, still affecting the way the Supreme Court views the Fourth Amendment more than forty years after it was decided.[99] The issue in *Katz* concerned the legality of government wiretaps of a suspected criminal's phone conversations, which were introduced as evidence against the defendant Katz at trial.[100] The taped phone conversations took place in a public phone booth, where the surveillance by law enforcement officers was of limited scope and duration, and provided evidence of Katz's illegal gambling.[101] Nevertheless, the Court held that invasion of a constitutionally protected area without a search warrant is presumptively unreasonable, and therefore this wiretap was unconstitutional.[102] In so holding, the Court noted that Fourth Amendment "considerations do not vanish when the search in question is transferred from the setting of a home . . . Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[103]

While the majority holding in this case is undoubtedly constitutionally significant, it is Justice Harlan's concurrence that has made an indelible mark on privacy law and the interpretation of the Fourth Amendment.[104] Providing the analysis that the Court still uses today, Harlan established a two-pronged test to determine whether the Fourth Amendment protects certain information. For a person to have a reasonable expectation of privacy necessary to garner Fourth Amendment protection: (1) the person must "have exhibited an actual (subjective) expectation of privacy";[105] and (2) "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[106] Under this test, conversations held in a private home would be considered

---

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

[100] *Id.* at 348.

[101] *Id.* at 354.

[102] *Id.* at 359.

[103] *Id.*

[104] *See, e.g.*, Scolnik, *supra* note 12, at 364.

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

[106] *Id.*

protected by the Fourth Amendment, while those that occur loudly in public do not carry the same expectations of privacy and therefore are afforded less protection.

Additionally, both the majority and Harlan's concurrence recognized the role of technologies in privacy law (though the technologies of 1967 were certainly quite different than those of today), with Justice Harlan stating that "electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment."[107]

Katz affirmed that when individuals voluntarily divulge information to the public, there is no reasonable expectation of privacy.[108] In most cases, the distinction between public and private is relatively easy to discern; however, in the case of social media, with privacy controls and users who do not fully comprehend how the networks function, categorizing what communications are open to the "public" and which are truly private becomes a complicated issue.

B. THIRD-PARTY DOCTRINE

Third-party doctrine is a premise developed upon the theories articulated in *Katz* and subsequent jurisprudence.[109] While its legacy is not as strongly felt as that of the other principles discussed in this Note, the vestiges of the third-party doctrine nonetheless have an influence on privacy law today. The doctrine postulates that if the information in question has been voluntarily turned over to a third party, the individual seeking privacy protection no longer has a reasonable expectation of privacy.[110] For example, in *Hoffa v. United States*, the Supreme Court held that information given to third parties or stored on third-party databases no longer contains the reasonable expectation of privacy necessary to obtain full Fourth Amendment protection.[111] The conversation at issue took place between two individuals, but was held in the presence of a third-party outsider. The

---

[107] *Id.* at 360.

[108] Scolnik, *supra* note 12, at 354.

[109] *Id.*

[110] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

[111] Hoffa v. United States, 385 U.S. 293, 302–03 (1966) (stating that conversations shared with a third party could no longer receive Fourth Amendment protections).

Court thus allowed the subpoena of the third party who bore witness to the conversation; however, it also stated that a party does not forfeit all Fourth Amendment rights upon the sharing of information to a third party, but rather merely shifts the balance slightly more toward disclosure.[112]

The third parties of today are no longer simply other persons present in the room or on another line listening in on a phone conversation; electronic databases are also being used to diminish privacy privileges under the third-party doctrine. The Supreme Court has held that information stored by a third-party, where the third-party has access to the information, is afforded no privacy protections under the Fourth Amendment.[113]

Similarly, Internet Service Providers (ISPs) often maintain databases of users' information, including private emails, which are stored on ISP servers.[114] If courts were to take an expansive view of the third-party doctrine, this is another avenue by which to access otherwise privacy-protected communications located on social media website servers.[115] For, as stated by the Court, the Fourth Amendment does not "protect[] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[116]

C. THE LEVELS OF PRIVACY

As stated in Katz, an individual using a phone booth is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[117] While this may almost always be the case with telephone conversations, there are Internet locations that enjoy these assumptions as well. While some Internet communications may be presumed public, others have privacy controls that garner them more protection.[118] This section examines the three levels of privacy,

---

[112] *Id.* at 301–03.

[113] United States v. Miller, 425 U.S. 435, 444 (1976) (holding that bank records held by a third-party bank were not protected by the Fourth Amendment).

[114] Scolnik, *supra* note 12, at 359.

[115] Zwillinger & Genetski, *supra* note 43, at 575–76.

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

[117] Katz v. United States, 389 U.S. 347, 352 (1967).

and applies them in terms of today's most significant social networking website: Facebook.

1. PUBLIC COMMUNICATIONS

Public communications are those that, because they are shared openly, are not shielded by a constitutionally-protected expectation of privacy.[119] In the early days of social media, courts were generally very willing to allow E-evidence into the courtroom without pause for several reasons, which are still advanced by some courts and scholars today.[120] First, courts are hesitant to give protection to parties who choose to disclose the information in controversy online.[121] Second, most courts favor the production of relevant evidence over consideration of an individual's privacy interests.[122] Finally, some courts find reasonable expectation of privacy considerations absent from social media postings.[123]

Today, public communications include any text or media that is available to the general public.[124] Examples of public communications include radio broadcasts,[125] websites, and open blog posts.[126] Under these standards, social networking communications are unequivocally unshielded by the Fourth Amendment if they are free from any privacy protections that may be available for individual websites. By

---

[118] Evan E. North, Note, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1288 (2010).

[119] Matlach, *supra* note 14, at 459.

[120] Payne, *supra* note 3, at 860–61.

[121] *Id*. at 861; s*ee also Ledbetter*, 2009 WL 1067018, at *1.

[122] *See, e.g.*, *Ledbetter*, 2009 WL 1067018, at *2.

[123] Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862–63 (Cal. Ct. App. 2009).

[124] North, *supra* note 118, at 1288.

[125] *See, e.g.*, Edwards v. Bardwell, 632 F. Supp. 584, 589 (M.D. La. 1986), *aff'd,* 808 F.2d 54 (5th Cir. 1986) (holding that there is no reasonable expectation of privacy in communications broadcast over the radio that can be overheard by countless people).

[126] *See, e.g.,* United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) (stating that privacy protection is unavailable to a person who undertakes no measures to protect the information and that a person who places a photograph online and unsecured by privacy controls forfeits any Fourth Amendment protection).

this logic, the user, having taken no steps to guard his or her communications, has no reasonable expectation of privacy. If a social media user's profile is available to anyone on the Internet, or even simply to every registered user of a particular social networking website, the current standard holds this data as a public communication.[127]

Applying the principles of public communications to Facebook, it is clear that those profiles or parts of profiles that are open to anyone with an account—or anyone with a familiarity with Google—are considered public communications and thus are freely discoverable. A user can have a completely public profile, but privacy controls also let the user make certain sections of their profile private and others public. For example, a user may control who can view their "wall" and photos, but allow anyone to see their basic information. If this is the case, the contents of the profile are split between those public communications and the privacy-controlled sections, which would fall into one of the two categories discussed below.

2. PRIVATE COMMUNICATIONS

Private communications are those that, both subjectively and objectively, are viewed as being only accessible by a very limited number of people. These communications are afforded the highest level of protections allowed by the Fourth Amendment, denying law enforcement access to such information.

Examples of such private communications include a phone call between two or an otherwise small number of individuals,[128] instant messaging, emailing, and other communications between individuals that are not intentionally open to the public. While there are always chances that an email will be sent to someone unintentionally or instant messages will become unencrypted, the parties to the conversation still hold a subjectively and objectively reasonable belief that they are private and act in confidence of this. Thus, the communication receives full Fourth Amendment protections.

Analogizing these principles to Facebook, private communications would be those kept between a small number of people, such as the use of Facebook messaging—an email equivalent between friends—or

---

[127] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1967) (holding that information provided freely to others confers no reasonable expectation of privacy); *see also* Matlach, *supra* note 14, at 460.

[128] Katz v. United States, 389 U.S. 347, 352 (1967).

Facebook chat—an instant messaging service.[129] These types of communications are not intentionally exposed to the public and are similar to any other form of closed communications, such as a phone call, email, or other types of instant messaging services.[130] Because of the expectations that these conversations will remain private, they should carry the same protections as phone calls and similar communications. Such private Facebook communications, therefore, should earn full Fourth Amendment protections.

3. QUASI-PRIVATE COMMUNICATIONS

The nature of quasi-private communications, which straddle the divide between public and private, makes this category the most difficult to define concretely. Generally, these communications would otherwise be considered public, but are utilized in a way that attaches a reasonable expectation of privacy to their use.[131]

Because of such expectations, lawmakers and courts should grant these communications some protection under the Fourth Amendment and privacy statutes. The exact level of protection afforded would depend on several factors, including the type of information, steps taken by the user to shelter the information from the public, and the individual website's privacy policies. A fact inquiry is often necessary to ascertain just how reasonable a user's expectation of privacy may be.[132] However, because a legitimate expectation of privacy exists, a warrant or court order (as required by the SCA) should be required for law enforcement to gain access to the material.

A good portion of social networking communications fall under this category due to the amalgamation of both large networks of people granted access to the information and the user's own (reasonable) view of her information as guarded from the public. An example of this is information on a Facebook user's profile, if such information is protected by the website's available privacy controls. Because of such controls, the user often views this information as closed off to the "public" at large, regardless of how many friends he

---

[129] *See Crispin*, 717 F. Supp. 2d at 991.

[130] Matlach, *supra* note 14, at 461.

[131] *Id.* at 460.

[132] *Id.*

or she might have that are allowed to see the information.[133] However, the current "objective" test of reasonability views this information as public because of the potentially large amount of people who are still able to view the information (including people the user might not know well).[134]

Application of this principle to social networking communications can be analogized to simple face-to-face conversations: A conversation between a small group of close friends is likely to be considered private, but if such a conversation was held in a large, filled lecture hall that would most likely not be the case.[135] Put another way, private information that is shared with strangers happened upon is no longer private;[136] but if such information is shared merely with close confidants, there is an expectation that it will not be repeated publically.[137]

Herein lies a divide in understanding: While lawmakers and courts generally argue that quasi-private communications are discoverable, the average user regards these communications as private. Because of the divergence, the law should err on protecting the privacy rights of individuals absent other prevailing interests.

In terms of Facebook communications, quasi-private communications are those posts that are hidden to the general public through the use of privacy controls, but are still open to certain networks or large groups of people. Additionally, because of the nature of Facebook, even communications shared only with "friends" have the chance of being copied and shared with larger networks of people—disseminating information without user consent—and they are thus deemed less worthy of Fourth Amendment protection.[138]

Because of the vast number of controls available, defining a specific location along the public-private spectrum for all quasi-private communications simply is not a workable proposal. Instead, in determining where along the spectrum certain communications lie, there are several factors to look at, individual to each post or

---

[133] North, *supra* note 118, at 1296.

[134] *Id.*

[135] Smith v. Maryland, 442 U.S. 735, 743–44 (1967).

[136] *Id.*

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

[138] North, *supra* note 118, at 1288, 1296.

communication. Factors may include, but are not limited to: the amount of friends a user has (and are thus allowed to view certain information), how privacy controls are used (whether access is limited to a "network," "friends of friends," just "friends," or an even smaller number though the utilization of customizable "friend groups"), and similar considerations.[139]

By limiting access to selected content, the user logically believes she has protected herself. If a user has gone through the necessary steps to reasonably protect her information, this should place such communications nearer to private communication on the spectrum, and thus allow the information greater Fourth Amendment considerations.

V. ANALYSIS

The current state of disconnect between those communications that users view as reasonably private and those that courts view as reasonably private is disconcerting. Many users are not aware of how little protection they have, and are thus unable to protect themselves. Further, given the current popularity and power of social networks, it is simply unreasonable to suggest that users significantly alter or altogether stop using these websites for fear that Big Brother is watching. Instead, lawmakers must be willing to change with the times and realize further protections for users of social media are necessary.

It is my proposition that courts alter their consideration on whether quasi-private communications, as defined above, should be discoverable. Instead of presuming that such communications are admissible absent other interests or issues, current statutes governing the discoverability of social media evidence need to be amended and viewed from a new perspective: Rather than presuming such evidence is discoverable unless proven otherwise, this quasi-private information should not be regarded as discoverable unless the moving party can prove prevailing interests under which to admit the evidence.

While at times this type of evidence may have high probative value, for example, proving a fact in dispute or an alibi, much of the potential character or circumstantial evidence is taken out of context and contains great risk of being overly prejudicial or confusing. Due to the nature of such information contained on social media websites, a

---

[139] *Id.* at 1298.

vast majority of this information should be disallowed from the courtroom.

In their analysis of a reasonable expectation of privacy on social networks, courts fail to consider some of the more complicated issues that plague networks such as Facebook. For example, Facebook has not always existed in its current state. At its advent, Facebook was available only to college students. At that time, students posted information freely and this information was usually available only to others in the user's "network"—other students on their campus. Neither these users nor Facebook's executives themselves could have predicted such rapid and extensive evolution into the multi-platformed network with 750 million users that exists today. This change is not only a technical marvel, but a privacy concern. Courts consider reasonable expectations of privacy under standards of today, not by what kind of network existed when the information was posted. While it is true that less recent posts are inherently less probative and thus less likely to be admitted into evidence, the concern exists nevertheless. No matter when the information was posted, it is stored on Facebook's servers and is discoverable under today's legal landscape without sight of what privacy rights are given up.

Privacy policy dictates the use of discretion in allowing evidence believed by the user and deemed by the website to be private to be subpoenaed. Unless this information is highly probative and essential to the case at hand, courts should err on the side of caution before admitting the evidence, in keeping with the Fourth Amendment. There are certain circumstances where such character evidence should be admitted into the courtroom, such as instances when the party's character or reputation are elements of the crime itself. An example of this would be the use of social media evidence in a child custody hearing. In this instance, admitting pictures of a parent engaging in irresponsible behavior found on a social media site—such as drinking, drug use, or other risky behaviors—may be highly probative in determining whether the individual is capable of being a fit parent. If information contained in a "private" page proves a fact of the matter in consequence, the court may well find that interests lie on the side of disclosure.

Additionally, other circumstances or considerations may prove to tip the scale in favor of allowing such quasi-private communications. If the information cannot—or at least cannot without significant cost or burden—be found elsewhere, in the interests of justice, the information should be discoverable. Further, there may be times when the specific fact that information was posted online becomes significant. For example, in a criminal juvenile case, the prosecution may want to admit online posts to prove that the defendant is

unrepentant in his actions. Because of the specific value of this information being online, it proves to be valuable enough to forgo the privacy considerations in question.

However, the nature of social media sites calls into question the value of such information, for several reasons. For one, information about a party may have been posted by another user, proving it very difficult to control this information or even know that it is online in the first place. Additionally, not all images or posts can or should be taken at face value and the court should carefully examine both the probative value and veracity of the information in its evaluation of such evidence. Factors in determining whether such evidence is probative enough to be admitted include how recent such evidence is and the context of any text or photograph.

Due to the ubiquity of social media websites—deemed the "permanent chronicle of people's lives" by one privacy scholar[140]—the use of such sites in obtaining potential evidence may prove to be easiest avenue to certain types of information. However, because of the above concerns, courts should only allow evidence taken from social media websites if such information is not available elsewhere. Such a measure allows important evidence to be admitted over any privacy concerns only if the information is necessary and otherwise unavailable, taking heed of Fourth Amendment concerns.

Social media sites encourage users to share personal information,[141] but that does not and should not mean that the use of social media causes users to relinquish their Fourth Amendment and other privacy rights. These websites encourage users to start a conversation, to share aspects of themselves, and to use the site as a tool with which to interact with friends.[142] When one sends a letter to a friend, she has every reason to believe the post office will respect her privacy; the letter writer has not consented to having the contents of such a letter turned over to the police. So why would this expectation be any different for a Facebook user who sends his friend a message or post that he believes is private? The law should evolve along with new media and protect user privacy in a new era. While courts may be hesitant to read these privacy rights into current precedent and statutory material, the legislature is in a prime position to promulgate

---

[140] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 11 (2007).

[141] North, *supra* note 118, at 1288.

[142] *Id.* at 1280.

new laws in order to fully protect users' rights. It may be true that social media is evolving too rapidly for the courts or legislature to keep up with specific laws, but in order to protect individuals' Fourth Amendment rights, it is important to disseminate new statutes and common law that allows for flexibility to grant protection when users truly and understandably believe information they post online is private.

VI. CONCLUSION

The rapid evolution of the Internet and social media has presented the courts and legislatures of our country with the task of reforming United States legal doctrine in keeping with the times. Despite certain efforts in the statutory and common law, the infamously slow-to-change U.S. legal system has yet to fully conform to the new Facebook-centric era. This disparity between the growth of technology and legal theory has shown itself most tellingly in the disconnect between objective and subjective expectations of privacy. While younger generations believe that material posted online is private, older generations of lawmakers and judiciary see such information as open to the masses, and therefore public—and, for better or worse, the latter are those whose voices are most strongly heard. Users, reasonably expecting their online communications to be shielded from the courts, deserve to have their privacy rights recognized by the legislature and court system.

Amidst all of this commotion concerning what privacy is expected of one's Facebook status updates, the Fourth Amendment has been subdued. In order to guarantee Fourth Amendment rights in future generations, privacy rights online must be recognized. There are, of course, certain circumstances that call for the discovery and admission of social media evidence in litigation, but this should be an exception, not the rule. In order to encourage faith in the judiciary and legislature from the new generation of Americans who live their lives online, protection of their Internet identities is crucial. If we do not protect privacy interests now, the future of those liberties guaranteed under the Fourth Amendment are in danger of being silenced forever.