REASONABLE EXPECTATIONS OF PRIVACY SETTINGS: SOCIAL MEDIA AND THE STORED COMMUNICATIONS ACT

CHRISTOPHER J. BORCHERT, FERNANDO M. PINGUELO, AND DAVID THAW[†]

ABSTRACT

In 1986, Congress passed the Stored Communications Act ("SCA") to provide additional protections for individuals' private communications content held in electronic storage by third parties. Acting out of direct concern for the implications of the Third-Party Records Doctrine—a judicially created doctrine that generally eliminates Fourth Amendment protections for information entrusted to third parties—Congress sought to tailor the SCA to electronic communications sent via and stored by third parties. Yet, because Congress crafted the SCA with language specific to the technology of 1986, courts today have struggled to apply the SCA consistently with regard to similar private content sent using different technologies.

This Article argues that Congress should revisit the SCA and adopt a single, technology-neutral standard of protection for private communications content held by third-party service providers. Furthermore, it suggests that Congress specifically intended to limit the scope of the Third-Party Records Doctrine by creating greater protections via the SCA, and thus courts interpreting existing law should afford protection to new technologies such as social media communications consistent with that intent based on individuals' expressed privacy preferences.

[†] Authors are listed in alphabetical order by last name, and this ordering does not reflect the contributions of any one author. Christopher J. Borchert is an Associate of the law firm Connell Foley LLP. He received his J.D., with Honors, and Intellectual Property Certificate from the University of Connecticut School of Law and his B.A. in Political Communication from the George Washington University. Fernando M. Pinguelo is a Partner in the New Jersey and New York offices of Scarinci Hollenbeck and Chair of the firm's Cyber Security & Data Protection Group. He received his J.D. and B.A. magna cum laude from Boston College. David Thaw is an Assistant Professor of Law and Information Sciences at the University of Pittsburgh and an Affiliated Fellow of the Information Society Project at Yale Law School. David received his J.D. from Berkeley Law, Ph.D. in Information Management and Systems and M.A. in Political Science from UC Berkeley, and B.S. in Computer Science and B.A. in Government and Politics from the University of Maryland.

TABLE OF CONTENTS

INTRODUCTION

Over the last decade, social networking platforms such as Facebook, Twitter, LinkedIn, and Google+ have exploded in popularity, fundamentally changing the way individuals and organizations communicate. Facebook, the world's largest social networking platform, currently claims more than one billion monthly active users.[1] Twitter recently surpassed the 200 million monthly active user mark,[2] while LinkedIn and Google+ claim more than 160 and 135 million monthly active

[1] *Company Info*, FACEBOOK, http://newsroom.fb.com/Key-Facts (last visited Nov. 18, 2014).

[2] Darrell Etherington, *Twitter Passes 200M Monthly Active Users*, TECHCRUNCH (Dec. 18, 2012), http://techcrunch.com/2012/12/18/twitter-passes-200m-monthly-active-users-a-42-increase-over-9-months/.

users, respectively.[3] As these companies continue to develop the functionality and expand the reach of their social networking platforms, so too will users continue to increase their reliance on social media for an even wider range of communication needs. And because these platforms provide varying communication channels—from wall posts and tweets to direct messages and private chats—users will eventually and necessarily foster varying expectations of privacy with regard to each communication channel.

Yet for a variety of legal and practical reasons, it remains unclear whether Fourth Amendment protections extend to communications shared and stored online. Although Congress sought to remedy this uncertainty in 1986 by enacting the Stored Communications Act ("SCA"),[4] courts have embraced varying and often contradictory interpretations of the Act's language, especially when applying the statute to modern technology that did not exist at the time of its enactment.[5] As a result, seemingly private electronic communications, such as e-mails stored on Gmail or private messages saved on Facebook, may not receive full privacy protection under the SCA, whereas semi-public wall posts could potentially trigger the Act's highest protections.[6] In all cases, however, since these electronic communications are "records" entrusted to "third parties" by individuals, but for the SCA they would enjoy no Fourth Amendment protection due to the Third-Party Records Doctrine ("TPRD").[7]

Recent events suggesting expansive federal surveillance operations based on the acquisition of information from these third-party providers further highlight the importance of addressing the role of Fourth Amendment protections for online communications. The protections in the

---

[3] Salvador Rodriguez, *LinkedIn Had 160 Million Active Users, Up 20% in Two Months*, L.A. TIMES (Jan. 14, 2013), http://articles.latimes.com/2013/jan/14/business/la-fi-tn-linkedin-160-million-members-20130114; Amir Errata, *Google+ Announces 135 Million Users, Debuts Instagram Competitor*, WALL ST. J. TECH. BLOG (Dec. 6. 2012, 9:00 AM), http://blogs.wsj.com/digits/2012/12/06/google-announces-135-million-users-debuts-instagram-competitor/.

[4] S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555; *see infra* pp. 5–7.

[5] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1211–12 (2004).

[6] For further discussion of statutory protections afforded to private messages and wall posts, see *infra* Part II.B.1–2.

[7] *See* United States v. Miller, 425 U.S. 435, 443–44 (1976) (holding that an individual does not have a Fourth Amendment interest in bank records released to a third party); *see also* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that the installation and use of a pen register device does not constitute a search under the Fourth Amendment).

SCA are critical in an age where Gmail, Facebook, and Skype have nearly replaced the use of the Postal Service and telephone system for regular communication. Furthermore, this shift in technology and the resulting ambiguity of protection under the SCA demonstrate the shortcomings of the TPRD and suggest that Congress sought to limit the scope of this doctrine to certain contexts such as personal correspondence.

This Article proceeds in three Parts. Part I provides a brief contextual background of the SCA and its interaction with the TPRD. It summarizes the SCA's legislative history, provides an overview of the statute's key components, and lays a foundation suggesting Congress's intent to provide privacy protections limiting the scope of the TPRD. Part II examines the current split between the traditional interpretation of the SCA—as promulgated by the Department of Justice and most recently embraced by the Supreme Court of South Carolina in *Jennings v. Jennings*—and the Ninth Circuit's interpretation as to whether opened e-mails are held in "electronic storage" as defined by the Act. It then proceeds to address the SCA's application in the context of social media and examines empirical data relating to the efficacy of social networking platforms' privacy settings. Part III suggests Congress amend the SCA in order to return the Act to its original intent: providing universal privacy protections for private electronic communications regardless of whether those communications are in transit or in storage. This Article further recommends Congress adopt technology-neutral statutory language, which has enduring as opposed to temporary efficacy, to protect more effectively communications content now and in the future. It suggests language to help effect this goal and also provides suggestions for how courts should act in the interim to preserve the additional protections Congress created with the SCA, which are directly responsive to the Supreme Court's recognition of the TPRD.

I. A BRIEF CONTEXTUAL BACKGROUND OF THE SCA

The SCA is a federal statute that governs the privacy of stored Internet communications.[8] Congress enacted the SCA in 1986 to provide a set of Fourth Amendment-like privacy protections for communications made online because it was, and still remains, largely unclear whether traditional Fourth Amendment protections extend to the online context.[9] Professor Orin Kerr suggests three reasons why the constitutional

[8] Kerr, *supra* note 5, at 1208. Some states have statutes analogous to the federal SCA, including Texas, Florida, and Minnesota. *See* Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals*, 16 VA. J. L. & TECH. 116, 150-188 (2011) (setting forth a multi-state survey of cyber-related statutes).
[9] *Id.* at 1210–11.

protections against unreasonable searches and seizures may not reach the virtual world. First, Supreme Court privacy jurisprudence has created "uncertainty over whether and when Internet users can retain a 'reasonable expectation of privacy' in information sent to network providers, including e-mails."[10] In *United States v. Miller*, the Supreme Court established the third-party doctrine, which denies Fourth Amendment protections to information disclosed to an entity not originally party to the communication.[11] Because virtually all Internet communications are shared with a network service provider, i.e., a third party, users may be categorically prohibited from enjoying a reasonable expectation of privacy online. Second, Fourth Amendment rules governing grand jury subpoenas suggest that the government may subpoena online communications held by third-party network service providers without first obtaining a warrant based on probable cause.[12] Third, most providers are private actors and may therefore disclose stored communications without violating the Fourth Amendment.[13]

A. Legislative History of the SCA

In October 1985, the Office of Technology Assessment issued a report entitled "Electronic Surveillance and Civil Liberties," which concluded that "current legal protections for electronic mail are weak, ambiguous, or non-existent," and that "electronic mail remains legally as well as technically vulnerable to unauthorized surveillance."[14] One year later, Congress passed the Electronic Communications Privacy Act ("ECPA"), and with it 18 U.S.C. §§ 2701–2712, or the SCA, "to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[15] The Senate Report on the SCA highlights Congress's desire to extend to electronic communications the underlying privacy protections already afforded to postal mail and private telephone conversations:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations. Voice communications transmitted via common carrier are protected by title III of the Omnibus Crime Control and Safe Streets Act of 1968.

---

[10] *Id.* at 1210.
[11] *Miller*, 425 U.S at 443.
[12] Kerr, *supra* note 5, at 1212.
[13] *Id.*
[14] S. REP. NO. 99-541, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3358.
[15] *Id.* at 1.

> But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology. This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.[16]

In passing ECPA, Congress sought to promote technological innovation, encourage the commercial use of "innovative communications systems," discourage unauthorized users from obtaining access to communications to which they are not a party, and establish clearer standards to protect both law enforcement officials from liability and the admissibility of legitimately obtained evidence.[17] Congress explicitly sought to achieve a "fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies."[18]

The Senate Report on the SCA plainly indicates Congress's intent to protect certain information stored electronically in the same manner as information stored locally: "With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information . . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change."[19] This sentiment is repeated throughout the report: "Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right."[20] The SCA's fundamental parts reflect Congress's dueling priorities of promoting technological innovation while securing reasonable expectations of privacy, as the next section explains.

B. Key Components of the SCA

The SCA affords privacy protections to online communications held by two types of Internet service providers ("ISPs"): providers of electronic communication services ("ECS") and providers of remote computing services ("RCS").[21] The SCA defines ECS as "any service which provides to users thereof the ability to send or receive wire or

---

[16] *Id.* at 5.
[17] *Id.*
[18] *Id.*
[19] *Id.* at 3.
[20] *Id.* at 5. For a more detailed discussion of how these sentiments demonstrate Congress's intent to establish additional protections under law designed to limit the scope of the TPRD, see Part I.C.
[21] 18 U.S.C. § 2702(a)(1)–(2) (2012).

electronic communications."[22] By way of example, Google or Yahoo! acts as an ECS provider when a user employs the Gmail or Yahoo! Mail service to send or receive an e-mail.[23] The SCA defines RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system."[24] For example, Amazon acts as an RCS provider when a user employs Amazon Cloud Drive to store data remotely for long-term safekeeping.

In determining whether the SCA covers an ISP, the first inquiry is whether the ISP storing the communication is acting as a provider of ECS or RCS with regard to that communication.[25] If the ISP is acting as neither, then the SCA does not apply to the communication at issue.[26] These classifications necessarily depend on the context of the implicated communications: "the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract."[27] Importantly, ISPs can (and often do) function as both ECS and RCS providers.[28]

The SCA categorizes online information into content and non-content information and affords different standards of protection to each.[29] Content information generally consists of the user's actual communications, whereas non-content information generally includes records and other information pertaining to the user.[30] The SCA prohibits ECS providers from voluntarily divulging content information held in electronic storage to third parties.[31] It also prohibits RCS providers from voluntarily divulging content information to third parties, but only when the RCS provider maintains the information "solely for the purpose of providing storage or computer processing services to [the] subscriber or customer."[32] The SCA is more permissive respecting voluntary disclosure to government entities, and prohibits only disclosure of non-content information by both ECS and

---

[22] *Id.* § 2510(15).
[23] *See* Kerr, *supra* note 5, at 1216 (explaining distinctions between providers of electronic communication services and providers of remote computing services); *see also* Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (holding that the statutory definition of an ECS provider includes basic e-mail services).
[24] 18 U.S.C. § 2711(2).
[25] Kerr, *supra* note 5, at 1213.
[26] *Id.*
[27] *Id.* at 1215.
[28] *Id.*
[29] Simon M. Baker, *Unfriending the Stored Communications Act: How Technological Advancement and Legislative Inaction Have Rendered Its Protections Obsolete*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 75, 88 (2011).
[30] *Id.*
[31] *Id.* at 89.
[32] 18 U.S.C. § 2702(a)(2)(B) (2012).

RCS providers.[33] Furthermore, these provisions apply only when the ISP is providing a service to the public.[34] This latter inquiry is fairly straightforward: an entity is providing a service to the public if it provides that service to "the community at large," irrespective of whether it charges a fee.[35] Most university and government e-mail accounts are non-public providers and therefore are not covered by the SCA.[36]

While § 2702 regulates voluntary disclosure of content and non-content information, § 2703 regulates the processes by which government entities may compel network service providers to release electronically stored information. The government may compel the disclosure of content information from an RCS provider in three ways.[37] First, the government may require disclosure without providing notice to the subscriber or customer "if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction."[38] The second and third means of compelling disclosure of content information from RCS providers require the government to provide notice to the subscriber or customer.[39] After satisfying the prior-notice requirement, the government may obtain either "an administrative subpoena authorized by a Federal or State statute or grand jury trial," or "a court order for such disclosure under § 2703(d)."[40]

For ECS providers, the government must adhere to certain timetable requirements for compelling disclosure. If the content information is held in electronic storage for 180 days or fewer, the government must obtain a warrant to compel disclosure.[41] If the content information is held in electronic storage for more than 180 days, the government may compel disclosure after providing prior notice and obtaining either an administrative subpoena or a court order.[42]

For the communication at issue to be covered by the rules governing ECS, it must be held in "electronic storage," as that term is defined in the statute.[43] The SCA provides two definitions of electronic

---

[33] Baker, *supra* note 29, at 89.
[34] *Id.*
[35] Anderson Consulting LLP v. UOP, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998).
[36] *See* Kerr, *supra* note 5, at 1216.
[37] 18 U.S.C. § 2703(b)(1).
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.* § 2703(a).
[42] *Id.* § 2703(a)–(b).
[43] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 982 (C.D. Cal. 2010).

storage.[44] The first definition includes "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[45] The second definition of electronic storage includes "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[46] Neither the statute nor the legislative history provides a definition for the term "purposes of backup protection," and, consequently, courts have struggled with its interpretation.[47]

C. The Third-Party Records Doctrine and the SCA

Scholarly defenses of the TPRD include arguments that the protections of the Fourth Amendment do not extend to property controlled by others,[48] and that the doctrine is advantageous in the face of technological change because it is technology-neutral.[49] Such justifications are insufficient, however, in a highly interconnected world where Congress has failed to create an adaptable standard for additional protection of *content* as technology advances.

Sections A and B of this Part provide background on the SCA and discuss Congress's purpose behind the Act. Preserving the "privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology" was of paramount importance to Congress.[50] Congress was, for the time, technology-neutral in this language—it did not *limit* protections to electronic mail or computer-based bulletin boards; rather, it used these as examples to contrast with prior technologies such as the postal service or telephones.[51] Congress noted that the content of communications was often the same,[52] but that the protections afforded

---

[44] 18 U.S.C. § 2510(17).
[45] *Id.* § 2510(17)(A).
[46] *Id.* § 2510(17)(B).
[47] *See Crispin*, 717 F. Supp. 2d at 983 (noting the lack of definition for "purposes of backup protection").
[48] *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 589 (2009) ("By knowingly disclosing information to a third party, an individual consents to another person having control over it.").
[49] *See, e.g.*, *id.* at 579–81.
[50] S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.
[51] *Id.*
[52] *See id.* ("American citizens and American businesses are using these new forms of technology *in lieu of, or side-by-side with,* first class mail and common carrier telephone services." (emphasis added)).

identical content through different communications systems were vastly different.[53]

This language is critical to understanding the role and purpose of the SCA as respects the TPRD. Congress was not oblivious to the existence of the doctrine,[54] and viewed the necessity of affording protections to such communications—whether in transit under ECPA, or in storage under the SCA—as critical in limiting the reach of the TPRD. Nor did Congress intend this protection to be limited either to criminal investigations or to Federal jurisdiction—both the Senate Report[55] and the final language of the statute itself support the intent that these be very broad protections.

Why then did the SCA not achieve this goal? As described in Part II of this Article, the failure lies in the final statutory language, which perhaps in an attempt to be technology-neutral, created ambiguity that was substantially technology-specific. This language, drafted in the 1980s, failed to provide an easily adaptable framework.[56] The result is a circumstance in which courts must interpret whether, and if so to what extent, users of a new technology enjoy Fourth Amendment-like privacy interests in the content of communications using modern technologies such as Facebook, Google, and Apple's iPhone. Such an outcome could be desirable if the underlying statute provided a framework clarifying what *types of activities and interests* Congress sought to protect.

Unfortunately, as Part II of this Article suggests, the SCA provides anything but such a framework—leaving substantial ambiguity resulting in

---

[53] *Id.* at 5.

[54] *Id.* at 3 (citing *United States v. Miller*, 425 U.S. 435 (1976), for the proposition that records subject to control by a third party computer operator may be subject to no constitutional privacy protection).

[55] *See id.* at 4 (noting the broad scope of the TPRD).

[56] An alternative approach Congress might have employed, had it felt a technology-neutral framework could not be drafted without leaving too much interpretive ambiguity to the courts, would have been to provide a technology-specific framework that would expressly require Congress, perhaps through sunset provisions, to revisit the framework as technology advanced. This approach seems suboptimal, however, as *a priori* timing the sunset provisions to the development of new technology would be difficult. Additionally, such provisions might risk political inaction overturning policy that otherwise would remain intact. A third alternative, delegating the responsibility for updating these provisions to an administrative agency, might have facial appeal but could be more costly over the long term. Additionally, such delegation could face challenges as the expertise required might span several agencies (e.g., the National Institute of Standards and Technology, the Department of Justice, the Federal Communications Commission, etc.) and thus further increase costs. Therefore, a technology-neutral approach embedded in statutory language likely was and likely remains the most appropriate option.

disparate judicial outcomes. Nonetheless, while the 1986 language of the statute fails to provide clarity for modern-day technology, Congress's original intent is clear—a desire to provide heightened protections for communications content in the face of advancing technology, specifically including limitations on the TPRD.

D. Civil Discovery and the SCA

For the practitioners slugging it out in the trenches, the SCA plays a significant role in civil litigation strategy. While FRCP 45[57] generally governs subpoenas in federal courts, and FRCP 26[58] generally governs discovery requests in federal courts, the SCA specifically applies to subpoena requests issued to *nonparties*.[59] As such, the SCA governs subpoena requests issued to Internet communications content holders, such as Yahoo!, Facebook, and Google.

More and more, parties routinely seek discovery of communications shared and stored on social networking platforms. Consequently, courts must not only grapple with the various state and federal procedure rules governing the discovery of electronically stored information, but also devise methods by which parties can obtain relevant social media content—such as status updates, private chats, and protected tweets—without violating established privacy protections. While different courts have fashioned different methods[60] to facilitate the exchange of such content *between the parties*, absent the SCA, courts would often face the privacy-offensive result of granting litigants' requests to compel wholesale disclosure of communications content by *nonparties* because of the TPRD.[61]

Yet, the SCA's outdated language compels courts to engage in unnecessary statutory analyses to determine the extent to which particular communications are covered.[62] For instance, in *In re Jetblue Airways Corp.*

---

[57] FED. R. CIV. P. 45.
[58] FED. R. CIV. P. 26.
[59] Rudolph J. Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 WASH. & LEE L. REV. 1259, 1277 (2012).
[60] *See, e.g.*, Offenback v. L.M. Bowman, Inc., No. 1:10-1789, 2011 WL 2491371, at *1 (M.D. Pa. June 22, 2011) (conducting an in camera review of Plaintiff's Facebook account to determine what content is discoverable); Gallion v. Gallion, No. FA114116955S, 2011 WL 4953451, at *1 (Conn. Super. Ct. Sept. 30, 2011) (ordering counsel for each party in a divorce proceeding to exchange their clients' Facebook and dating website login credentials).
[61] *See In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp 2d 606, 609 (E.D. Va. 2008) (upholding a magistrate judge's order quashing a subpoena seeking a nonparty's e-mails from AOL because the SCA does not provide an exemption for such disclosure).
[62] *See infra* Part II.

Privacy Litigation, a class of plaintiffs asserted, among other claims, that JetBlue violated ECPA "by divulging stored passenger communications without the passengers' authorization or consent."[63] While JetBlue CEO David Neelman publicly acknowledged[64] that the company had violated its own privacy policy by transferring its customer's personal identifying information to a private data mining company, the New York district court nevertheless dismissed plaintiffs' ECPA claims. Because JetBlue was acting as neither a provider of ECS nor RCS, the judge ruled, the SCA did not apply to the communications in question.[65]

The *Jetblue* court principally relied on the holdings in C*rowley v. CyberSource Corp.* and *Andersen Consulting LLP v. UOP*.[66] In *Crowley*, a district court in California held that the "online merchant Amazon.com was not an electronic communication service provider despite the fact that it maintained a website and receives electronic communications containing personal information from its customers in connection with the purchase of goods."[67] In *Andersen*, the court "drew a distinction between companies that purchase Internet services and those that furnish such services as a business, and found that a company that purchases Internet services, such as e-mail, just like any other consumer, is not an electronic communication service provider within the meaning of the ECPA."[68]

As discussed above, in the context of discovery *between the parties*, the normal civil discovery process at least provides the parties opportunities to fully address the issue before disclosure—thus entrusting the issue of privacy protections to the adversarial system.[69] Yet, in the

---

[63] *In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 306 (E.D.N.Y. 2005).
[64] *Id.* at 305.
[65] *Id.* at 309–10.
[66] *Id.* at 308 (citing Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263 (N.D. Cal. 2001) and Anderson Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998)).
[67] *Id.* (citing *Crowley*, 166 F. Supp. 2d at 1270).
[68] *Id.* (citing *Andersen*, 991 F. Supp. at 1043).
[69] It may *also* be the case that the adversarial civil discovery process provides insufficient protections; that question is outside the scope of this Article. However, courts in such circumstances should at least consider the fact that, as discussed above, Congress passed the SCA in response to the TPRD and, accordingly, to what degree civil discovery requests of electronic material must be narrowly tailored to protect against privacy violations stemming from over-broad requests. For example, by way of analogy to the physical world, a discovery request of an entity for all its files pertaining to "Benzene" would not entitle the discovering party general access to the entity's files on employee discipline. Yet, in the case of *Gallion v. Gallion*, that is precisely what occurred—by turning over access credentials to the social networking platform Facebook, the parties effectively

context of disclosure requests served on *nonparties*, absent the SCA's protections—in a world where nearly all communications are facilitated *and stored* by third parties—requests served on third parties would become a "backdoor" to the discovery process, taking it out of the hands of the normal civil litigation process. Such a fundamental change to civil discovery procedures was not what Congress contemplated as evidenced by its enactment of the SCA and specifically the § 2702 confidentiality limitations on voluntary disclosure.

II. INTERPRETIVE DIFFERENCES WITHIN SCA JURISPRUDENCE

Courts across the country have embraced varying and often contradictory interpretations of the SCA's language, especially when applying it to modern technology that did not exist at the time of the Act's enactment.

A. The Split: Whether Opened E-mails are Held in "Electronic Storage"

Whether an ISP is acting as a provider of ECS or RCS with regard to a particular communication is a critical distinction due to the different privacy protections afforded to each type of provider. This distinction is especially challenging to determine in the context of opened e-mails, and there is a genuine split as to whether opened e-mails are held in "electronic storage" for the purposes of the SCA. The traditional approach, promulgated by the Department of Justice and embraced by most courts,[70] maintains that opened e-mails are not held in "electronic storage" because they are not backup copies of incidental wire or electronic communications held in temporary or intermediate storage.[71] This interpretation assumes that the second definition of "electronic storage"—"any storage of such communication by an electronic communication service for purposes of

---

turned over the keys to the entire filing room and allowed them unrestricted ability to search it, rather than only having the party produce the relevant files.

[70] COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf; *see also* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635–38 (E.D. Pa. 2001) (concluding that already-accessed e-mails are not in "electronic storage"), *aff'd in part and vacated in part*, 352 F.3d 107 (3d Cir. 2003).

[71] *See* Orin S. Kerr, *South Carolina Supreme Court Creates Split with Ninth Circuit on Privacy in Stored E-mails—and Divides 2-2-1 on the Rationale*, VOLOKH CONSPIRACY (Oct. 10, 2012, 4:24 PM), http://www.volokh.com/2012/10/10/sourth-carolina-supreme-court-deepens-split-on-privacy-in-stored-e-mails-and-divides-2-2-1-on-the-rationale/ (noting that the traditional view adopted by the DOJ is that subsection (B) refers to backup copies in subsection (A)).

backup protection of such communication"—contained in subsection (B) of § 2510(17)) applies only to messages in subsection (A).[72]

The Ninth Circuit in *Theofel v. Farey-Jones* rejected this reading of § 2510(17), explaining that the phrase "such communication" in subsection (B) "does not, as a matter of grammar, reference attributes of the type of storage defined in subsection (A)."[73] Therefore, the court analyzed whether the e-mails at issue fit the definition in either subsection (A) or subsection (B). The court held that e-mail messages delivered to and retrieved by a user and stored by an ISP were stored for "purposes of backup protection"—falling squarely under subsection (B)—and were therefore protected under the ECS rules.[74] The court reasoned that users frequently rely on e-mail servers to preserve e-mail messages in the event the user accidentally erases or misplaces the original messages, and concluded that "prior access is irrelevant to whether the messages at issue were in electronic storage."[75] Under *Theofel*, "what matters is not whether the e-mail has been accessed, but rather whether the e-mail 'has expired in the normal course.'"[76]

In *United States v. Weaver*, an Illinois district court attached significant weight to the particular e-mail system at issue in *Theofel*, noting that the Ninth Circuit relied "on the assumption that users download e-mails from an ISP's server to their own computers."[77] In *Weaver*, the e-mail system at issue was a Hotmail account, which is "web-based" and "remote."[78] The *Weaver* court reasoned that communications stored on web-based e-mail systems are not stored for purposes of backup protection, but rather are maintained "solely for the purpose of providing storage or computer processing services," and therefore must be governed by the RCS rules.[79] But therein lies an important distinction. The reasoning in *Weaver* assumes that the determination of whether an ISP is a provider of ECS or RCS turns on the ISP's intentions, and not those of the user, with regard to the communication at issue. The *Weaver* court states:

> [U]nless a Hotmail user varies from default use, the remote computing service is the only place he or she stores messages, and Microsoft is not storing that user's opened messages for backup purposes. Instead, Microsoft is maintaining the messages "solely for the purpose of

---

[72] *Id.*
[73] Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2003).
[74] *Id.* at 1075.
[75] *Id.* at 1075–77.
[76] Kerr, *supra* note 5, at 1218 (quoting *Theofel*, 359 F.3d at 1076).
[77] United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009).
[78] *Id.*
[79] *Id.*

> providing storage or computer processing services to such subscriber or customer."[80]

The *Weaver* decision ultimately turned on the intentions of the ISP and not those of the user. Yet, as the Ninth Circuit in *Theofel* noted, "nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user."[81]

The *Weaver* court further argued that the decision in *Theofel* cannot be squared with legislative history.[82] For instance, the court cited a passage from the House Report on the SCA, which includes in part the following language: "Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that . . . such communication should continue to be covered by section 2702(a)(2)," which governs RCS providers.[83] But the Ninth Circuit addressed this point in *Theofel* and explained that the ECS rules would *also* apply, just as both the RCS and ECS rules govern already-accessed e-mails: "If section 2702(a)(2) applies to e-mail even before access, the committee could not have been identifying an exclusive source of protection, since even the government concedes that unopened e-mail is protected by the electronic storage provisions."[84]

The ECS–RCS distinction can also be outcome-determinative in the context of civil liability. In *Quon v. Arch Wireless Operating Co., Inc.*, the attachment of civil liability turned on whether Arch Wireless, a private company that provided text-messaging pager services to the city of Ontario, was acting as a provider of ECS or RCS with regard to stored text messages.[85] The district court held that Arch Wireless, acting as a provider of RCS, was permitted to release transcripts of private text messages under the exemption in § 2702(b)(3) because it had obtained consent from the city, which was a "subscriber" for the purposes of the statutory exemption. The determination that Arch Wireless was acting as a provider of RCS was critical because ECS providers are not exempt from liability for releasing such content even if they obtain permission from a subscriber.[86]

The Ninth Circuit reversed and found that Arch Wireless was a provider of ECS.[87] Interpreting the "plain language of the SCA, including

---

[80] *Id.* (quoting 18 U.S.C. § 2702(a)(2)(B) (2012)).
[81] *Theofel*, 359 F.3d at 1075.
[82] *Weaver*, 636 F. Supp. 2d at 772–73.
[83] *Id.*
[84] *Theofel*, 359 F.3d at 1077.
[85] Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 900 (9th Cir. 2008), *rev'd on other grounds in* Ontario v. Quon, 560 U.S. 746 (2010).
[86] *See* 18 U.S.C. § 2702(b)(3) (2012).
[87] *Quon*, 529 F.3d at 901.

its common-sense definitions," the Ninth Circuit argued that the definition of an ECS provider ("any service which provides to users thereof the ability to send or receive wire or electronic communications") describes exactly the function Arch Wireless was contracted to provide.[88] The court contrasted this function with that of an RCS provider, explaining that "before the advent of advanced computer processing programs such as Microsoft Excel, businesses had to farm out sophisticated processing to a service that would process the information."[89] Furthermore, the Ninth Circuit relied on *Theofel*, writing, "Although it is not clear for whom Arch Wireless 'archived' the text messages—presumably for the user or Arch Wireless itself—it is clear that the messages were archived for "backup protection," just as they were in *Theofel*."[90]

The split deepened further in 2012 when the Supreme Court of South Carolina rejected the holding in *Theofel* and found that e-mail messages stored on a web-based e-mail system are not held in electronic storage. In *Jennings v. Jennings*, the Supreme Court of South Carolina considered whether an individual, who, without authorization, accessed another user's web-based Yahoo! Mail account and retrieved already-accessed e-mails, was subject to civil liability under § 2701 of the SCA.[91] Lee Jennings initiated the lawsuit when he learned that his wife's daughter-in-law had correctly guessed the security questions associated with his Yahoo! Mail account and accessed his e-mails in order to obtain information about an alleged affair.[92] The action turned on whether the e-mails were held in electronic storage as defined by the SCA. If the e-mails were found to fall outside the statute's definition of electronic storage, then Jennings would be precluded from advancing a claim under § 2701. Specifically, the court considered whether the e-mails were stored for "purposes of backup protection."[93]

Previously, the South Carolina Court of Appeals applied, or perhaps extended, the Ninth Circuit's decision in *Theofel* to find that the e-mail messages maintained on the web-based e-mail system were held in electronic storage.[94] The court first found that Yahoo! was acting as an ECS provider with regard to the e-mails at issue, specifically noting that Yahoo! "was providing email services to [Jennings] at the time the emails at issue were accessed."[95] The court next considered whether the e-mails at

---

[88] *Id.*
[89] *Id.* at 902 (citing Kerr, *supra* note 5, at 1213–14).
[90] *Id.*
[91] Jennings v. Jennings (*Jennings I*), 736 S.E.2d 242 (S.C. 2012).
[92] *Id.* at 243.
[93] 18 U.S.C. § 2510(17)(B) (2012).
[94] Jennings v. Jennings (*Jennings II*), 697 S.E.2d 671 (S.C. Ct. App. 2010).
[95] *Id.* at 677.

issue were stored for purposes of backup protection, and found that "the previously opened e-mails were stored on Yahoo's servers so that, if necessary, [Jennings] could access them again."[96] The court made express reference to the Ninth Circuit's holding in *Theofel*, writing: "Like the Ninth Circuit, we believe that one of the purposes of storing a backup copy of an email message on an ISP's server after it has been opened is so that the message is available in the event that the user needs to retrieve it again."[97]

The Supreme Court of South Carolina, however, rejected this interpretation, holding instead that the retention of an opened e-mail does not constitute storage for purposes of backup protection under the Act.[98] The *Jennings* court placed substantial weight on the dictionary definition of the word "backup," which Merriam–Webster Dictionary defines as "one that serves as a substitute or support."[99] The court (incorrectly)[100] concluded that web-based e-mail systems maintain only a single copy of an e-mail message, and held that the e-mails were not maintained for purposes of backup protection. Therefore, the e-mails were not held in electronic storage for purposes of the SCA.[101]

Notably, South Carolina Supreme Court Chief Justice Toal, while concurring in the result, explained that the exact definition of "backup" varies from dictionary to dictionary, and application of the definition proffered in the majority opinion ("backup" defined as "one that serves as a substitute or support") may very well suggest that an e-mail message on an ISP's server could be stored for support in the event that the user needs to retrieve it.[102] Under this definition, the e-mail can be considered stored for purposes of backup protection despite whether or not there exists a second copy.[103] Chief Justice Toal instead relied on the statutory and historical context of the phrase "backup protection," writing that the "'traditional interpretation' of the [SCA], advanced by the Department of Justice, coupled with the fact that Congress never contemplated this new form of technology, provide a sounder basis to reach [a] decision."[104] This approach, however, places inordinate emphasis on the technology of 1986 and does not afford due consideration to the privacy concerns at the heart of

---

[96] *Id.* at 678.
[97] *Id.* at 677–78.
[98] *Jennings I*, 736 S.E.2d 242, 245 (S.C. 2012).
[99] *Id.*
[100] Virtually all web-based e-mail systems maintain multiple copies of electronic messages. *See generally* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 777–840 (5th ed. 2010).
[101] *Jennings I*, 736 S.E.2d at 245.
[102] *Id.* at 246 (Toal, J., concurring).
[103] *Id.*
[104] *Id.* at 245 (citation omitted).

the SCA, as evidenced by the legislative history. Additionally, as discussed above in Part I, Section C, the Senate Report discussing the SCA suggests that Congress was not trying to "contemplate [a] new form of technology," but rather was trying (if albeit unsuccessfully) to develop a technology-neutral definition for affording protections to emerging technology.

B. Social Media and the SCA

Application of the SCA in the context of social media poses numerous practical and legal challenges. For one, the scope of the SCA is limited to electronic communications "not intended to be available to the public."[105] Yet recent court decisions suggest that some communications made via social networking platforms may receive SCA protections, even if they were disclosed to hundreds or even thousands of third parties.

1. Crispin v. Christian Audigier, Inc.

In *Crispin v. Christian Audigier, Inc.*, a California district court considered whether the SCA applies to communications shared and stored on social networking platforms.[106] The three social networking platforms at issue were Facebook, MySpace, and Media Temple.[107] In finding that all three sites provide private messaging or e-mail services, the court concluded that each platform is an ECS provider.[108] The *Crispin* court further held that each social networking platform could also serve as an RCS provider.[109] Specifically, the *Crispin* court wrote:

> As respects messages that have not yet been opened, those entities operate as ECS providers and the messages are in electronic storage because they fall within the definition of "temporary, intermediate storage" under § 2510(17)(A). As respects messages that have been opened and retained by Crispin . . . [Facebook, MySpace, and Media Temple] operate as RCS providers providing storage services under § 2702(a)(2).[110]

Under this analysis, a social networking platform would be prohibited from voluntarily "divulging to any person or entity the contents of a

---

[105] *See* S. REP. NO. 99–541, at 35 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3589.
[106] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).
[107] Media Temple is a web hosting and Internet services company that provides "simple tools for domain registration, web hosting, business applications, virtual servers, and other cloud servers to power more than 1.5 million websites." *About Media Temple*, MEDIA TEMPLE, http://mediatemple.net/company/about-us/ (last visited Nov. 19, 2014).
[108] *Crispin*, 717 F. Supp. at 982.
[109] *Id.* at 987.
[110] *Id.*

communication" made through an e-mail or private message, without first obtaining proper authorization. Under the reasoning in *Crispin*, unopened private messages maintained for fewer than 180 days are governed by the ECS provisions, and social networking platforms may only disclose them if the government presents a valid warrant. Opened private messages are governed by the less stringent RCS provisions: the government must provide notice to the user and need only present the social networking platform with a trial subpoena or court order in order to obtain them.

The *Crispin* court embraced the reasoning in *Weaver*, finding that opened messages on social networking platforms should be governed by the RCS provisions.[111] It also denied that its finding conflicted with Ninth Circuit precedent and instead insisted that its holding is supported by dicta in *Theofel*.[112] Yet *Theofel* expressly states that "prior access is irrelevant to whether the messages at issue were in electronic storage."[113] If the *Crispin* court found (as it did) that Facebook, MySpace, and Media Temple are providers of ECS, then it should not matter if the messages have been accessed by the recipient.[114] Accordingly, the *Crispin* court quite clearly departed from *Theofel* in finding that Facebook, MySpace, and Media Temple are ECS providers but acted as RCS providers with regard to the opened messages, when *Theofel* found no such shift in ISP designation.

The *Crispin* court also considered whether Facebook wall posts and MySpace comments are eligible to receive protection under the SCA.[115] First, the court analyzed whether wall posts and comments can be defined as being held in electronic storage.[116] Applying the definition from subsection (A), the court found that wall postings and comments are not protectable as forms of temporary, intermediate storage because, unlike e-mail, there is no step whereby comments or wall posts must be opened.[117] But the court, relying on a critically important analogy, found that wall posts and comments are stored for purposes of backup protection and are therefore covered by the definition from subsection (B).[118] The court analogized wall posts and comments to messages on an electronic bulletin

---

[111] *Id.*
[112] *Id.*
[113] Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2003).
[114] *See Crispin*, 717 F. Supp. 2d at 982.
[115] *Id.* at 981.
[116] *Id.* at 988.
[117] *Id.* at 989.
[118] *Id.* at 981–82.

board service ("BBS")[119]—technology that not only existed in 1986, but also was expressly included in the legislative history.[120]

2. Analogizing Wall Posts and Comments to Private BBS Messages

The Senate Report on the SCA defines BBSs as "communications networks created by computer users for the transfer of information among computers," and notes that "these may take the form of proprietary systems or they may be noncommercial systems operating among computer users who share special interests."[121] The Report acknowledges that BBSs made available to the public are not covered by the SCA, since facilitators of publicly-accessible bulletin boards effectively authorize anyone to access the communications.[122] The statute reflects this in § 2511(2)(g): "It shall not be unlawful for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[123]

The *Crispin* court relied heavily on the Ninth Circuit's decision in *Konop v. Hawaiian Airlines, Inc.* to conclude that postings, once made, are stored for purposes of backup protection.[124] In *Konop*, the Ninth Circuit considered whether an employer violated the SCA when he accessed without authorization a private BBS, which was maintained by *Konop*.[125] The Ninth Circuit expressly stated that the website was a provider of ECS and that the communications on the website were held in electronic storage. Importantly, the court considered the steps taken by Konop to restrict access to the public:

> Konop controlled access to his website by requiring visitors to log in with a user name and password. He created a list of people, mostly pilots and other employees of Hawaiian, who were eligible to access the website . . . Konop programmed the website to allow access when a person entered the name of an eligible person, created a password, and clicked the "SUBMIT" button on the screen, indicating acceptance of the terms and conditions of use. These terms and conditions prohibited any member of Hawaiian's management from viewing the

---

[119] The Senate report refers to bulletin board "services" and bulletin board "systems" interchangeably.
[120] S. REP. NO. 99-541, at 8–9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3572–73.
[121] *Id.*
[122] *Id.* at 36
[123] 18 U.S.C. § 2511(2)(g) (2012).
[124] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010).
[125] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).

> website and prohibited users from disclosing the website's contents to anyone else.[126]

Following this reasoning, the *Crispin* court found that if a user sufficiently restricts access to communications displayed on his social media account, those communications may be covered by the SCA.[127] Specifically, the court stated that "the passive action of failing to delete a BBS post, which is in all material ways analogous to a Facebook wall posting or a MySpace comment, also results in that post being stored for backup purposes."[128] Accordingly, the court held that "Facebook and MySpace are ECS providers as respects wall postings and comments and that such communications are in electronic storage."[129] This finding would require the government to obtain a warrant in order to compel disclosure of sufficiently restricted wall posts and comments.

But the *Crispin* court did not stop there: "In the alternative, the court holds that Facebook and MySpace are RCS providers as respects the wall postings and comments."[130] This alternative conclusion rests largely on the reasoning in *Viacom International, Inc. v. YouTube, Inc*.[131] In *Viacom*, a New York district court determined that YouTube acted as a provider of RCS with regard to user-uploaded videos, which the user designated as private via YouTube's privacy settings.[132] The *Crispin* court analogized these restricted YouTube videos to restricted wall postings and comments, finding that in both instances, the webpages are storing content "for the benefit of the user and those the user designates."[133] The *Crispin* court's reasoning is both conflicted and irresolute, and thus fails to clarify the SCA's applicability to communications made via social networking platforms.

This analysis provides support for our recommendations, discussed below in Part III, that the SCA suggests that Congress intended the scope of the TPRD to have limits respecting certain types of activities and content, such as communications. Furthermore, this analysis supports our concurrence with Professor Kerr's suggestion that ECPA and the SCA be amended to establish a single definition protecting all types of communication in-transit and in-storage with a single, equal standard of

---

[126] *Id.* at 872–73.
[127] *Crispin*, 717 F. Supp. at 991.
[128] *Id.* at 989.
[129] *Id.*
[130] *Id.* at 990.
[131] *Id.*
[132] *See* Viacom Int'l, Inc. v. YouTube, Inc., 253 F.R.D 256, 264–65 (S.D.N.Y. 2008).
[133] *Crispin*, 717 F. Supp. at 990.

protection requiring a warrant for access in most instances of criminal investigation.

While it remains unclear whether communications shared and stored on social networking platforms should be governed by the ECS or RCS rules, the foregoing case law certainly suggests that certain social media users are entitled to some protection under the SCA. In *Crispin*, the court considered whether the communicator put in place sufficient privacy restrictions. This logic aligns with Congress's explicit intent in enacting the SCA: to achieve a "fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies."[134] Moreover, well-established principles of statutory construction compel a reading of the SCA that "effectuates rather than frustrates the major purpose of the legislative draftsmen."[135]

This Article suggests that Congress should amend the SCA to include already-accessed communications made via social networking platforms.[136] Currently, the *Crispin* line of reasoning suggests the threshold question of whether wall posts and comments even fall under the SCA's coverage at all hinges on the sufficiency of the user's privacy settings.[137] Thus, we suggest that social networking platforms should have available privacy settings to restrict access in a manner sufficient for courts to analogize these platforms to private BBSs. This approach raises at least two important questions. First, to what extent must users restrict access to their profiles in order to enjoy the protections of the SCA?[138] Second, are the available privacy settings sufficiently effective so as to make the platform inaccessible to the public?

---

[134] S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.
[135] Shapiro v. United States, 335 U.S. 1, 31 (1948).
[136] *See infra* Part III.
[137] *See Crispin*, 717 F. Supp. 2d at 991 (remanding so the parties could develop a fuller evidentiary record regarding plaintiff's privacy settings and the extent of access allowed to plaintiff's Facebook wall and MySpace comments).
[138] With respect to this first question, Professor Andrea Matwyshyn proposes an approach for delineating when sensitive consumer data should be subject to protection such as breach notification requirements. Professor Matwyshyn's approach essentially indicates that if an authentication credential is required to access the information, it triggers protection under breach notification laws. While perhaps overly broad on its face, the finer technical distinctions of this approach provide insight regarding this question: as a floor, at least any communication access to which is protected by an authentication credential (e.g., a username and password) should be the subject of protection. *See, e.g.*, *Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers? Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Energy & Commerce Comm.*, 113th Cong. (2013) (statement of Andrea Matwyshyn, Assistant Professor, University of Pennsylvania Wharton School of Business).

3. Social Media Privacy Settings: How Private is Private?

Because social networking platforms provide varying channels of communication, users will eventually and necessarily foster varying expectations of privacy with regard to each channel. But the SCA does not afford protections according to reasonable expectations of privacy. The Act instead compels application of language written for the technology of 1986. As a result, users can receive heightened protections for communications displayed to thousands of users, but lesser protections for private messages shared between only two people.[139] The results of these interpretations may frustrate Congressional purpose as indicated in the Senate Report, thus suggesting that existing interpretation, which affords different levels of protection to different technologies, may be improper.[140] Until Congress revisits the SCA, courts have options to address this distinction and afford more consistent levels of protection commensurate with Congress's intent.[141] The *Crispin* court's conclusion that wall posts and comments can be analogized to BBSs relies on the assumption that the available privacy settings are even capable of being sufficiently restrictive. Therefore, an assessment of privacy settings on social networking platforms is appropriate.

A recent study published in the Carnegie Mellon Journal of Privacy and Confidentiality uses data from a longitudinal panel of 5,076 Facebook users to survey how their privacy and disclosure behavior changed between 2005—the early days of the Facebook network—and 2011.[142] The study highlights three contrasting trends:

> First, over time Facebook users in our dataset exhibited increasingly privacy-seeking behavior, progressively decreasing the amount of personal data shared publicly with unconnected profiles in the same network. However, and second, changes implemented by Facebook near the end of the period of time under our observation arrested or in some cases inverted that trend. Third, the amount and scope of personal information that Facebook users revealed privately to other connected profiles actually increased over time—and because of that, so did disclosures to "silent listeners" on the network: Facebook itself, third-party apps, and (indirectly) advertisers.[143]

---

[139] *See Crispin*, 717 F. Supp. 2d at 991 (holding that opened private messages on Facebook and MySpace are governed by the RCS rules, while wall posts and comments, if sufficiently restricted via privacy settings, are governed by the ECS rules).
[140] *See supra* Part I.C.
[141] *See infra* Part III.
[142] Fred Stutzman et al., *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY 7 (2012).
[143] *Id.*

For the purposes of this analysis, it is the third trend that sheds most light on the sufficiency of Facebook's privacy settings. The finding that disclosures users *intended to be private* were often revealed to third parties such as advertisers and apps, unbeknownst to the user, underscores the reality that privacy settings may not restrict content to the extent users—and courts—might assume. For example, the study found that users often unwittingly reveal their birthday, location, photos, and the location of friends to third-party apps.[144] More to the point, the study found that users often estimate incorrectly how many other Facebook members have access to their profile data: "social media users consistently underestimate their audience size for their posts, guessing that their audience is just 27% of its true size."[145] This speaks directly to whether Facebook's privacy settings are sufficiently restrictive so as to equate wall posts to private BBS messages.

A study published by the Department of Computer Science at Columbia University found similar results.[146] The study investigated whether users' Facebook privacy settings matched their sharing intentions and concluded that Facebook's current approach to privacy settings is "fundamentally flawed."[147] Participants of the study completed intentions forms, which required the participants to indicate whether certain profile groups[148] could access certain information categories.[149] Participants were informed that the information categories were based on content rather than data type, and spanned all data types, including wall posts, photos, links, and status updates.[150] The study found that every single one of the 65 participants had at least one "sharing violation" based on their stated sharing intentions.[151] In other words, "every participant was sharing

---

[144] *Id.* at 28.
[145] *Id.* at 29.
[146] Michelle Madejski et al., *The Failure of Online Social Networking Privacy Settings*, COLUM. U. COMPUTER SCI. TECH. REP. (2011).
[147] *Id.* at 4.
[148] The profile groups consisted of the following: "Someone not your Facebook friend"; "Someone who is your Facebook friend"; "Someone who is in your Facebook network but not your friend"; and "Someone who is a friend of a friend." *Id.* at 3.
[149] The information categories consisted of the following: "Negative: Information that is insulting, hateful, or negative"; "Interests: Information that is related to movies, music, books, and your other interests"; "Personal: Information that is personally identifiable, such as your visual appearance, location, age, gender"; and "Family: Information associated with siblings, children, significant other, or family." *Id.*
[150] *Id.*
[151] *Id.* at 14.

something they wished to hide, or was hiding something they wished to share."[152]

In addition, recent FTC consent orders concerning social networking platforms' privacy settings further question the appropriateness of analogizing wall posts and comments to private BBS messages. In November 2011, the FTC issued a consent order stemming from allegations that Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allow[ed] it to be shared and made public."[153] For example, the FTC found that Facebook "told users they could restrict sharing of data to limited audiences—for example with 'Friends Only,'" when "in fact, selecting 'Friends Only' did not prevent their information from being shared with third-party applications their friends used."[154]

Earlier that same year, the FTC took action involving the launch of another social media platform. In March 2011, the FTC issued a consent order stemming from allegations that Google "used deceptive tactics and violated its own privacy promises when it launched its social network, Google Buzz."[155] The complaint alleged that Google made deceptive representations to consumers by suggesting that "consumers would be able to exercise control over what information would be made public through their Google public profile."[156] The FTC found that "the contacts with whom users emailed and chatted the most would become public by default and that user information submitted through other Google products would be automatically broadcast through Buzz."[157]

The foregoing studies and FTC consent orders suggest that privacy settings on social networking platforms may not provide the sort of restrictions that were present on private BBSs in 1986.[158] For example, the Senate Report on the SCA states specifically that § 2701 "does not prevent broad authorizations to the general public to access such a facility."[159] Specifically, the Report states:

---

[152] *Id.*

[153] Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), *available at* http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[154] *Id.*

[155] Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm.

[156] Google, Inc., FTC File No. 102-3136, at 6 (Mar. 30, 2011).

[157] *Id.*

[158] *See supra* notes 119–20.

[159] S. REP. NO. 99-541, at 36 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3590.

> The bill does not for example hinder the development or use of 'electronic bulletin boards' or other similar services where the availability of information about the service, and the readily accessible nature of the service are widely known and the service does not require any special access code or warning to indicate that the information is private.[160]

The *Crispin* court was quick to conclude that wall posts and comments can safely be analogized to a private BBS message provided the communicator of the wall posts and comments employed the available privacy settings.[161] Yet this conclusion relies on the assumption that the available privacy settings on social networking platforms are sufficiently restrictive. As the foregoing suggests, this assumption may not necessarily be appropriate.[162]

III. AMENDING THE SCA

Parts I and II present a historical, operational, and jurisprudential backdrop to the SCA. Part III suggests that Congress should amend the SCA to provide heightened statutory protections for private electronic communications—such as private e-mails stored on Gmail and private messages saved on Facebook—where the user demonstrates a reasonable expectation of privacy by employing sufficiently restrictive privacy settings. Additionally, it suggests that even now, courts can (and some do) interpret existing language and Constitutional protections to afford protection more consistent with Congressional intent regarding private electronic communications.

In 1976, the Supreme Court first recognized the TPRD in *United States v. Miller*. Despite significant and substantial changes to communication methods, interests, and expectations, the Supreme Court has not revisited the TPRD. Professor Kerr opines in a recent Article that "several lower courts have ruled that the Fourth Amendment fully protects the contents of emails held by third party providers."[163] He cites the Sixth Circuit's decision in *United States v. Warshak* and points to several district court decisions that apply the *Warshak* reasoning to other forms of communications content, such as "Facebook messages, text messages, faxes, and password-protected websites."[164] In fact, Kerr concludes, "no

---

[160] *Id.*
[161] *See supra* notes 118–20 and accompanying text.
[162] *See also* David Thaw, *Surveillance at the Source*, Kentucky L. J., (forthcoming 2015), available at http://ssrn.com/abstract=2512121 (discussing the role of private actors in information gathering and usage).
[163] Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 399 (2014).
[164] *Id.* at 399–400.

court has reached the contrary result. *Warshak* has been adopted by every court that has squarely decided the question."[165]

Kerr concedes that the case law is not entirely settled: "only one federal court of appeals has squarely addressed the issue."[166] As the Supreme Court has yet to revisit the issue, *Miller* remains good law. Therefore, while Kerr is correct to characterize the developing case law as substantially supportive of Fourth Amendment protections for communications content stored by third parties, the issue is far from settled.

An initial survey of recent federal decisions addressing related issues in the privacy and technology context suggest that some courts might be less inclined to follow the *Warshak* reasoning. For example, the Fifth Circuit recently held that a mobile phone user does not have a reasonable expectation of privacy in location data stored by a third-party mobile phone service provider—even if that data is necessary for the provision of the service.[167] The Sixth Circuit held similarly in 2012,[168] albeit in a ruling somewhat less clear on the technological distinctions differentiating it from *United States v. Jones*.[169] Many of these decisions, notably including *Jones*, call upon Congress to remedy these ambiguities and construct clear guidelines in the privacy and technology context.[170]

Congressional action may take time. While a legislative remedy is the most appropriate resolution, in the interim courts still have options to preserve the level of privacy protections Congress sought to afford with the SCA. This Article urges courts to follow the reasoning in *Warshak* and require law enforcement to obtain a warrant in order to compel disclosure of online communications content stored by third parties.

---

[165] *Id.* at 400.
[166] *Id.*
[167] *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding that a cell phone user does not have a reasonable expectation of privacy in location data stored by a third party).
[168] *See* United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012) ("There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell-phone.").
[169] *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").
[170] *See, e.g.*, *id.* at 964 (Alito, J., concurring in the judgment) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." (citation omitted)).

Civil litigation poses a separate problem given the natural absence of Fourth Amendment protection. As discussed *supra* in Part I, Section D, this Article suggests that Congress intended for the SCA to create new protections responsive to the Supreme Court's decision in *Miller*, which would prevent litigants from circumventing the discovery process. Courts therefore should seek to limit discovery requests of communications content shared and stored on social networking platforms in light of the SCA's legislative history.

In *The Next Generation Communication Privacy Act*, Professor Kerr offers a thought experiment about "what might happen if Congress repealed ECPA in its entirety and enacted a new privacy statute to replace it."[171] Specifically, Professor Kerr suggests that this new privacy statute should (1) impose the same warrant requirement on access to all contents; (2) impose particularity requirements on the scope of disclosed metadata; (3) impose minimization and non-disclosure rules on all accessed content; and (4) impose a two-part territoriality regime with a mandatory rule structure for United States-based users and a permissive regime for users located abroad.[172]

While this Article largely agrees with Professor Kerr's proposals, it further suggests that Congress should adopt technology-neutral language in a manner that will clarify the content subject to protection while leaving sufficient flexibility for courts to apply the protections Congress intends to future technologies. As discussed in Parts I and II of this Article, Congress attempted to do so with the SCA but failed in drafting. The core challenge in this task is creating technology-neutral language that can encompass as-yet-undefined future technologies. Drafting such language is a plausible goal—by focusing on the protection sought to be afforded, rather than on the specific technology conveying the communication, Congress can achieve this goal. This Article provides a modest suggestion for how, in adopting a single standard for criminal and civil protection of stored communications content, draft legislation might describe the bounds of that protection:

> *Communications content stored on any interconnected information system permitting communications among one or more individuals where the system is configured or is configurable by individuals in a manner sufficient either to demonstrate an expectation of privacy or to allow those individuals the ability to demonstrate an expectation of privacy.*

The inclusion of language directed toward privacy settings reflects the central tenets of *Katz* and its progeny. In *Katz v. United States*, the

---

[171] Kerr, *supra* note 163, at 373.
[172] *Id.* at 377–78.

Supreme Court held that a defendant maintained a reasonable expectation of privacy in telephone calls he made from a closeable public telephone booth.[173] The Court articulated the 'reasonable expectation of privacy' test, which requires a dual finding of a subjective expectation of privacy (on the part of the communicator) and an objective expectation of privacy (one that society finds as reasonable).[174] The phone booth in *Katz* serves as an appropriate analogy to privacy settings because both contexts evince expectations of privacy.[175] While the caller in *Katz* enjoyed Fourth Amendment protections *inside* the closeable telephone booth, the *Katz* opinion suggests that a similar level of protection would not have been available to a public phone *not* housed in a closeable booth.[176]

As discussed in Part II, the privacy settings that allow users to express clear intent are important to drawing boundaries in complex information systems with both public and private components. This concept is not new to the SCA.[177] Likewise, it also has important roots in physical-world Fourth Amendment jurisprudence. Privacy settings in social media and other advanced communications systems—when implemented and employed effectively—sufficiently demonstrate an expectation of privacy that society is willing to recognize as reasonable. Courts can take notice of these settings and societal expectations, similar to the cases like *Katz* discussed above, and implement the protections consistent with language like that proposed in this Part. Congress should use such language to adopt a uniform standard to protect communications content shared and stored on social networking platforms where the user employs sufficiently restrictive privacy settings.

CONCLUSION

Over the past decade, courts have embraced varying and often contradictory interpretations of the SCA when applying it to technology that did not exist at the time of the Act's enactment. As a result, seemingly

---

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

[174] *See id.* at 361 (Harlan, J. concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

[175] *See id.* at 352 (majority opinion) ("No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment.").

[176] *See id.* ("One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

[177] *See supra* note 120 (noting that Congress specifically was aware of the distinction between private and public communications on electronic Bulletin Board Systems commonly in use at the time the SCA was enacted).

private electronic communications, such as e-mails stored on Gmail or private messages saved on Facebook, may not receive full privacy protections under the SCA, whereas semi-public wall posts could potentially trigger the Act's highest protections. In addition, there remains substantial uncertainty as to the efficacy of privacy settings on some of the most popular social networking platforms.

Accordingly, this Article suggests Congress amend the SCA in order to ensure the Act achieves its original intent: providing universal privacy protections for private electronic communications regardless of whether those communications are in transit or in storage. This Article further recommends Congress adopt technology-neutral statutory language to more effectively protect communications content now and in the future. This change not only better reflects the functionality of modern web-based e-mail and messaging systems, but also more accurately incorporates the drafters' original intent. The Article suggests language to help effect this goal, and also provides suggestions for how courts should act in the interim to preserve the additional protections Congress created with the SCA, which are directly responsive to the Supreme Court's recognition of the TPRD in *United States v. Miller*.