Suffolk Journal of Trial and Appellate Advocacy

Volume 17 Article 10

1-1-2012

Compelling Disclosure of Facebook Content under the stored Communications Act

Allen D. Hankins

COMPELLING DISCLOSURE OF FACEBOOK CONTENT UNDER THE STORED COMMUNICATIONS ACT

I. INTRODUCTION

Since 2004, Facebook and other social network sites have dramatically changed the way people stay in touch with friends, family, and other acquaintances.[1] The explosive growth of these sites has resulted in users creating an immense amount of online communications between one another on an ongoing basis.[2] Users often seek some kind of social fulfillment in engaging in those communications, and as a result, they often tend to be more intimate than other types of communications.[3] This very personal and revealing nature increasingly makes them central to the resolution of both civil and criminal actions.[4]

---

[1] *See Timeline*, FACEBOOK, http://newsroom.fb.com/content/default.aspx?NewsAreaId=20 (last visited May 29, 2012) (providing historical growth of Facebook). Facebook allows people to "stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them." *Key Facts*, FACEBOOK, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (last visited May 23, 2012). As of August 2010, United States internet users spend more time on Facebook than searching with Google. *See Facebook Inches past Google for Web Users' Minutes*, USA TODAY (Sept. 10, 2010, 3:44 PM), http://www.usatoday.com/tech/news/2010-09-10-facebook-google_N.htm (citing study finding users spend about 9.9% of their total internet browsing time on Facebook).

[2] *See Key Facts*, *supra* note 1 (providing usage statistics of website). Of the 901 million users, more than fifty percent use Facebook every day. *See id.*

[3] *See* Nicole B. Ellison et al., *The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites*, J. COMPUTER-MEDIATED COMM., http://jcmc.indiana.edu/vol12/issue4/ellison.html (July 2007) (discussing psychological effects of communicating via social network sites). In a study conducted by Ellison, data tended to show that social network users seek to increase their "social capital" by sharing content and information with fellow users. *See id.* Social capital refers to the "useful information, personal relationships, [and] the capacity to organize groups" that result from a social network. *Id.* Social capital increases psychological well-being, and Ellison's study found a connection between Facebook usage and indicators of such social capital. *Id.* In pursuit of this social capital, users are often very candid and include details they would not ordinarily disclose in more formal communication methods. *See* Alexander Y. Thomas et al., *Social Media in Action in Litigation, Evidence & Privilege*, LEGAL BYTES (Mar. 8, 2010), http://www.legalbytes.com/2010/03/articles/social-and-digital-media-law/social-media-in-action-in-litigation-evidence-privilege/ ("Users . . . tend to post messages and photos with little thought, in an informal, spur-of-the-moment manner, from smart phones, BlackBerrys, and personal computers.").

[4] *See, e.g.*, Marshall v. Mayor of Savannah, 366 F. App'x 91, 93-94 (11th Cir. 2010) (analyzing plaintiff's gender discrimination claim resulting from photographs posted on MySpace); Wolfe v. Fayetteville, Ark. Sch. Dist., 600 F. Supp. 2d 1011, 1017-18 (W.D. Ark.

In cases where these communications are integral to the outcome of the case, a party has a profound interest in obtaining them from an opposing party.[5] Although a party may seek a discovery order compelling an opposing party to grant access to his or her Facebook page, this sometimes is not sufficient.[6] Parties may "clean up" their Facebook pages before or during litigation to remove any potentially implicating content.[7] A better alternative is to seek the information directly from the social network provider.[8] However, the quasi-private nature of that content may bring it within the protection of the Stored Communications Act ("SCA").[9] The SCA prohibits certain electronic service providers from disclosing users' communications.[10] It affords some level of privacy protections for electronic communications akin to Fourth Amendment protections for physical spaces.[11] Courts have reached different conclusions in applying the SCA to ever-evolving social network websites, but some identifiable

---

2009) (discussing student threats posted to Facebook groups as basis of discrimination action); Doe v. Cal. Lutheran High Sch. Ass'n, 88 Cal. Rptr. 3d 475, 478 (Cal. Ct. App. 2009) (examining discrimination claim based on sexual orientation listed on MySpace).

[5] *See* Thomas et al., *supra* note 3 (discussing various beneficial uses of social network sites in litigation, including witness impeachment); *see also* Christopher R. Drake, *Digging up Dirt on Facebook*, CONN. L. TRIB., Feb. 1, 2010, at 1, 1, *available at* http://www.murthalaw.com/files/digging_up_dirt_on_facebook_drake_2110_copy3.pdf ("Personal injury attorneys claim to have successfully defended exaggerated injury claims using pictures that plaintiffs themselves posted on Facebook. Likewise, employment lawyers can verify disability claims; divorce lawyers can see who is cheating on whom; and litigators of all sorts can find out if the opposing party is talking about the case."); Eric B. Meyer, *Social Networking Sites Provide Litigation Treasure Trove*, TEX. LAW., Sept. 6, 2010 (discussing ways to utilize social media in litigation). Meyer describes the potentially enormous value of users' unfiltered communications on social networks to litigants. *See* Meyer, *supra*.

[6] *See* Bass *ex rel.* Bass v. Miss Porter's Sch., Civil No. 3:08cv1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009) (party lost access to Facebook account prior to start of suit); Jeremy Byellin, *Facebook and the Stored Communications Act: What's Protected? (Part 1)*, WESTLAW INSIDER (Sept. 6, 2011), http://westlawinsider.com/social-media-law/facebook-and-the-stored-communications-act-whats-protected-part-1/ (describing risk party may delete relevant content before discovery).

[7] *See* Caroline H. Mankey, *'But My Lawyer Told Me to Delete the Facebook Posts!'*, L.A. DAILY J., Mar. 6, 2012, *available at* http://cypressllp.com/wp-content/uploads/2011/10/DailyJournal3.6.121.pdf (describing instances where litigants removed damaging Facebook content).

[8] *See* Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 657 (Sup. Ct. 2010) (ordering disclosure of social media records by Facebook and MySpace).

[9] 18 U.S.C. §§ 2701-2712 (2006).

[10] *Id.* §§ 2702-2703 (setting forth protections provided for different types of communications).

[11] *See* 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, 1212 (2004) (describing SCA as set of Fourth Amendment-like statutory privacy protections).

trends are emerging.[12]

This Note provides members of the legal profession insight into the types of challenges the SCA may present in attempting to compel disclosure of a party's Facebook account contents, as well as arguments that practitioners can make both for and against such disclosure. Part II examines the text of the SCA and the policy justifications for enacting the statute.[13] Part III discusses the application of the SCA to communication services analogous to the services provided by Facebook, including electronic bulletin board systems, text messages, and e-mail.[14] Part III also details courts' analyses in the few cases that have applied the SCA to communications residing on Facebook users' accounts.[15] The content of those accounts is playing an increasingly important role in litigation and settlement negotiations as more and more people become members of social network websites.[16] Therefore, Part IV sets forth issues practitioners are likely to encounter in seeking to obtain or prevent disclosure of Facebook account holders' information in both civil and criminal matters.[17]

II. THE STORED COMMUNICATIONS ACT

Congress wished to extend Fourth Amendment protections to new forms of communications when it passed the SCA in 1986.[18] The Fourth Amendment prohibits searches where individuals have an actual, subjective expectation of privacy that is objectively reasonable.[19] For instance,

---

[12] *Compare* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (finding private messages and certain other Facebook communications protected by SCA), *with* Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010) (ordering party to give written consent to opposing party for social media account access), *and* Largent v. Reed, No. 2009-1823, 2011 WL 5632688 (Pa. Ct. Com. Pl. Nov. 8, 2011) ("[T]he SCA regulates only ISPs . . . ."), *and* McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285 (Pa. Ct. Com. Pl. Sept. 9, 2010) ("Where there is an indication that a person's social network sites contain information relevant to the prosecution or defense of a lawsuit . . . access to those sites should be freely granted.").

[13] *See infra* Part II (detailing privacy concerns of electronic communications and different classifications of such communications under SCA).

[14] *See infra* Part III.A (highlighting treatment of technologies similar to Facebook under SCA).

[15] *See infra* Part III.B (comparing different approaches to applying SCA to social network sites).

[16] *See* Evan E. North, Note, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1286 (2010) (referring to social networking sites as potential "gold mines" of information).

[17] *See infra* Part IV (identifying obstacles to obtaining users' account contents).

[18] *See* S. REP. NO. 99-541, at 1-2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-57 (setting forth purpose of SCA).

[19] *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (setting forth requirements of Fourth

individuals' physical homes receive strong protections from unreasonable searches due to their inherently private nature.[20] However, applying Fourth Amendment jurisprudence to intangible communications, such as internet communications, proved difficult for courts prior to enactment of the SCA.[21] Furthermore, even if the Fourth Amendment were to protect internet communications, government agents would be able to issue grand jury subpoenas to compel the disclosure of information without probable cause, despite a Fourth Amendment reasonable expectation of privacy.[22] Additionally, the Fourth Amendment places no restrictions on searches or seizures of internet users' communications by internet service providers ("ISPs") because most ISPs are private companies, to which the Fourth Amendment is inapplicable.[23] The SCA overcomes these Fourth Amendment privacy concerns by affording ISP customers statutory privacy rights.[24] The SCA limits the government's ability to compel providers to disclose information in their possession about their subscribers.[25] It also limits the ability of ISPs to voluntarily disclose information about their customers and subscribers to the government.[26]

Amendment protection).

[20] *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) (noting unconstitutionality of warrantless searches of private homes, with few exceptions); *see also* Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

[21] *See* S. REP. NO. 99-541, at 1-2 (1986), *reprinted in* 1986 U.S.C.C.A.N. at 3555-57 (describing difficulty courts faced in applying Fourth Amendment to telephone conversations). The Framers of the Constitution aimed to prevent arbitrary government surveillance, so they "limited methods of intrusion into the 'houses, papers, and effects'" of citizens. *Id.*, *reprinted in* 1986 U.S.C.C.A.N. at 3555 (quoting U.S. CONST. amend. IV). Technological advances, such as the telephone, allowed surveillance without physically entering homes or other private places protected by the Fourth Amendment. *See id.* Such difficulty was a motivating factor in passing the SCA. *See id.* at 2-3, *reprinted in* 1986 U.S.C.C.A.N. at 3556-57.

[22] *See* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (describing Fourth Amendment's protection against searches where individual has reasonable expectation of privacy); *In re* Subpoena Duces Tecum, 228 F.3d 341, 346-49 (4th Cir. 2000) (differentiating between standards for issuing warrants and subpoenas). Probable cause must exist in order for warrants to issue, whereas the government may issue subpoenas as long as they are "reasonable." *In re Subpoena Duces Tecum*, 228 F.3d at 347-48 (explaining immediate and substantial invasion of privacy resulting from warrant issuance).

[23] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (emphasizing Fourth Amendment applies only to government action). The Fourth Amendment "is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'" *Id.* (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)).

[24] *See generally* Kerr, *supra* note 11, at 1212-13 (describing "Fourth Amendment-like privacy protections" created by SCA).

[25] *See* 18 U.S.C. § 2703 (2006) (outlining process necessary to require ISP to disclose communications).

[26] *See id.* § 2702 (prohibiting voluntary disclosure of customer communications or records).

The level of protection afforded to a communication depends upon whether the SCA classifies the provider of the communication as an electronic communication service ("ECS") or remote computing service ("RCS") in relation to the communication at issue.[27] The SCA defines ECS providers as those that provide "service[s] which provide[] to users thereof the ability to send or receive . . . electronic communications."[28] RCS providers are those that provide the public "computer storage or processing services by means of an electronic communications system."[29] The distinction between ECS and RCS providers arose in part due to businesses outsourcing their data processing and data storage needs.[30] A single provider may be a provider of ECS in some instances and a provider of RCS in other instances.[31] A provider may also provide both ECS and RCS with respect to the same communication.[32] For example, when a person sends an e-mail, that e-mail awaits the recipient's retrieval, and the e-mail provider acts as a provider of ECS.[33] If the recipient retrieves the e-mail and chooses to keep the e-mail on the provider's server, the provider may act thereafter as a provider of RCS.[34]

The SCA first prohibits ECS and RCS providers from revealing contents of electronic communications that they store or maintain.[35] It next

---

[27] *See id.* §§ 2702-2703 (setting forth different treatment of ECS and RCS providers under SCA); *see also* Kerr, *supra* note 11, at 1215 n.48 (stressing importance of analyzing individual communications as opposed to abstract status of provider); *infra* notes 35-50 and accompanying text (describing voluntary and compelled disclosure by ECS and RCS providers).

[28] 18 U.S.C. § 2510(15) (defining ECS).

[29] *Id.* § 2711(2) (defining RCS).

[30] *See* S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556-57 (detailing purpose of SCA). Large companies that specialized in computer processing and storage offered businesses convenience and sophistication that may not have otherwise been available in-house. *See id.* at 10-11, *reprinted in* 1986 U.S.C.C.A.N. at 3565-66 (describing rise of remote computer services). The distinctions also arose in the context of early e-mail in 1986, which was transmitted through multiple computer servers that each temporarily stored the e-mail until it reached its final destination. *See id.* at 7, *reprinted in* 1986 U.S.C.C.A.N. at 3562 (summarizing electronic mail transmission technology). At its final destination, the message was stored in the e-mail provider's computer mailbox until retrieved by the subscriber via dial-up modem. *See id.* (describing 1986 e-mail retrieval technology).

[31] *See* Kerr, *supra* note 11, at 1215-16 (characterizing most providers as multifunctional). Additionally, the same provider may act as neither an ECS nor RCS provider in other instances. *See id.* (emphasizing classification is context specific and not in the "abstract").

[32] *See id.* at 1216 (clarifying classification of multifunctional providers).

[33] *See id.* (providing example communications in which same provider provides both ECS and RCS).

[34] *See id.* (continuing example of e-mail communication).

[35] *See* 18 U.S.C. § 2702(a)(1)-(2) (2006) (proscribing divulging communication contents). ECS providers may not knowingly disclose "the contents of a communication while in electronic storage," and RCS providers may not knowingly disclose "the contents of any communication which is carried or maintained on that service." *Id.*

describes the instances in which providers may voluntarily disclose electronic communications.[36] Under the SCA, ECS providers may voluntarily disclose electronic communications in eight situations.[37] Four situations—set forth in exceptions (1), (2), (4), and (5)—are a part of providing the communication service, including to the addressee of the communication, as well as to employees of the service provider.[38] Exceptions (3), (6), (7), and (8) set forth other specific instances in which providers may disclose communications.[39] More specifically, the third exception allows disclosure if the sender or intended recipient consents to disclosure; the sixth allows disclosure in certain instances of child abuse; and the eighth allows disclosure to a governmental entity if the provider believes an emergency involving death or serious bodily injury requires disclosure.[40] Finally, the seventh exception allows disclosure to a law enforcement agency if a provider inadvertently obtains a communication that appears relevant to the commission of a crime.[41] Similarly, RCS providers may voluntarily disclose electronic communications in the same eight situations, as well as when the subscriber consents to the disclosure.[42]

The SCA next sets forth the methods in which the government may compel a provider to disclose communications.[43] To compel disclosure of ECS communications, the contents at issue must be held "in electronic storage in an electronic communications system."[44] The SCA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[45] If the ECS provider has held the communication for 180 days or less, the government must obtain a search warrant.[46] To compel an ECS provider who has held a communication for more than 180 days, the government may obtain a warrant, use an administrative or trial

---

[36] *See* § 2702(b) (listing exceptions for disclosure).

[37] *See id.* (outlining disclosure exceptions for ECS providers).

[38] *See id.* (describing exceptions for disclosure incidental to rendition of communication services).

[39] *See id.*

[40] *See id.* (setting forth ECS provider voluntary disclosure exceptions).

[41] *See* § 2702(b).

[42] *See* § 2702(b)(3) (allowing RCS provider to disclose contents of communication if originator, addressee, recipient or subscriber consents).

[43] *See id.* § 2703 (addressing methods for both ECS and RCS providers).

[44] § 2703(a) (articulating ECS disclosure process).

[45] *Id.* § 2510(17)(A)-(B).

[46] *See* § 2703(a) (limiting disclosure to instances where warrant is issued pursuant to governing rules of criminal procedure).

subpoena with prior notice to the subscriber, or obtain a court order with prior notice to the subscriber.[47] The procedure for compelling an RCS provider to disclose communications is identical to the procedure for compelling ECS providers who have held a communication for more than 180 days, i.e., the government may obtain a warrant, obtain an administrative or trial subpoena with prior notice to the subscriber, or obtain a court order with prior notice to the subscriber.[48] Thus, the heightened compelled disclosure requirements are only applicable to ECS providers who have held a communication for 180 days or less.[49]

The SCA contains no exception—for either ECS or RCS providers—for disclosure of communications pursuant to civil discovery subpoenas.[50] Compelling disclosure using a "trial subpoena" does not encompass a discovery subpoena duces tecum.[51] Trial subpoenas—subpoenas "for attendance at a . . . trial"—must issue from the court where the trial is to be held.[52] Discovery subpoenas—subpoenas "for production or inspection" of documents or electronically stored information—must issue from the court where the production or inspection is to be made.[53] Congress could have included discovery subpoenas as a method for compelling disclosure if it had intended that result.[54]

Major technology companies and privacy groups have pressured legislators to reform the SCA to address some of these confusing issues

---

[47] *See* § 2703(a)-(b) (setting forth requirements for communications held by ECS providers for more than 180 days). To compel disclosure by means of a court order, the government must offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." § 2703(d) (defining standard for court to issue order).

[48] *See* § 2703(b) (setting forth requirements for compelling RCS disclosure).

[49] *Compare* § 2703(a) (requiring warrant for ECS communications held for 180 days or less), *with* § 2703(b) (setting forth compelled disclosure for RCS and ECS communications held longer than 180 days).

[50] *See* § 2703 (describing exceptions allowing disclosure); *see also* Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (holding providers may not divulge contents of any electronic communication stored on behalf of subscribers); *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008) (finding SCA did not include exception allowing disclosure in civil discovery requests).

[51] *See* FED. R. CIV. P. 45(a)(2) (distinguishing from which court trial subpoenas and discovery subpoenas must issue).

[52] FED. R. CIV. P. 45(a)(2)(A).

[53] FED. R. CIV. P. 45(a)(2)(C).

[54] *See generally* FTC v. Netscape Commc'ns Corp., 196 F.R.D. 559, 561 (N.D. Cal. 2000) ("The court cannot believe that Congress intended the phrase 'trial subpoena' to apply to discovery subpoenas in civil cases, thus permitting government entities to make an end-run around the statute's protections through the use of a Rule 45 subpoena.").

pertaining to disclosure.[55] The difficulty in applying the SCA to modern technology is also well documented in academia.[56] There have been several amendments to the SCA in the past, but none has updated the Act to better apply to modern communications.[57] As of the publishing of this Note, there is no proposed legislation amending the SCA to address the SCA's applicability to social media.[58]

III. APPLICATION OF THE SCA

A. The SCA Applied to Similar Technologies

Although the SCA did not contemplate how communications such as social network sites might be handled, the Senate Report provides some insight as to how the SCA would be applied to electronic bulletin boards.[59]

---

[55] *See About the Issue*, DIGITAL DUE PROCESS, http://digitaldueprocess.org (last visited May 29, 2012) (calling SCA "patchwork of confusing standards that have been interpreted inconsistently"). Digital Due Process is a coalition of major companies, including Amazon, AOL, Apple, AT&T, eBay, Facebook, Google, HP, IBM, and Microsoft. *See Who We Are*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited May 29, 2012) (listing corporations, privacy advocates, think tanks, and individuals associated with Digital Due Process). These corporations have sponsored events to try to raise awareness of the need to reform the SCA. *See* Declan McCullagh, *Google, Facebook Go Retro in Push to Update 1986 Privacy Law*, CNET NEWS (Oct. 21, 2011, 8:56 AM), http://news.cnet.com/8301-31921_3-20123710-281/google-facebook-go-retro-in-push-to-update-1986-privacy-law/ (describing 1980s-themed Capitol Hill event to "woo congressional staff" to update SCA).

[56] *See* Simon M. Baker, Article, *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, 109 (2011) (stating SCA "is simply not designed to deal with modern technology"); Sara E. Brown, Student Work, *An Illusory Expectation of Privacy: The ECPA Is Insufficient to Provide Meaningful Protection for Advanced Communication Tools*, 114 W. VA. L. REV. 277, 296 (2011) ("Many courts addressing privacy issues in light of advanced communication tools get caught up in the futile distinctions in the [SCA] between an RCS and an ECS. Because the [SCA] provides privacy protection only for temporarily stored electronic communications, the distinction is important to analysis, but futile in the context of advanced communications.").

[57] *See, e.g.*, Protect Our Children Act of 2010, H.R. 6027, 111th Cong. § 2 (requiring providers maintain certain subscriber information to aid investigation of child sexual exploitation); USA Patriot Amendments Act of 2009, H.R. 3845, 111th Cong. § 109 (giving provider right to judicial review of compelled disclosure by subpoena, order, or warrant); Foreign Evidence Request Efficiency Act of 2009, S. 1289, 111th Cong. § 2(1), 123 Stat. 2086 (modifying statutory language to allow warrants to issue from any court of competent jurisdiction).

[58] *See* Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. § 3 (proposing elimination of 180-day rule but not addressing SCA's application to modern communication technologies).

[59] *See* S. REP. NO. 99-541, at 8-9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562-63 (discussing electronic bulletin boards). The report considered electronic bulletin boards

Electronic bulletin boards, a predecessor to social media, resemble traditional cork-and-pin bulletin boards in allowing users to read, post, and delete messages on the board.[60] The report makes it clear that Congress did not intend the SCA to hinder the use of electronic bulletin boards that do not require a password or warn users that the information on the board is not private.[61] The majority of courts have interpreted the SCA similarly, finding that an electronic bulletin board that has unrestricted public access will not merit protection under the SCA.[62] Instead, there must be some registration process controlling who may access the information contained on the bulletin board.[63]

Furthermore, the SCA does not criminalize or create civil liability for individuals who access "communications that are otherwise readily accessible by the general public."[64] So as long as the communications residing on the bulletin board cannot be easily viewed by anyone desiring to see them, the vast majority of courts have found them within the SCA.[65]

---

consisting of communications networks used to transfer information among users and computers. *See id.* (defining purpose of electronic bulletin board systems). The report further provides that a bulletin board system "may require special 'passwords' which restrict entry to the system. These bulletin boards may be public or semi-public in nature, depending on the degree of privacy sought by users, operators or organizers of such systems." *Id.* at 9, *reprinted in* 1986 U.S.C.C.A.N. at 3563 (expanding on electronic bulletin board definition).

[60] *See* United States v. Riggs, 739 F. Supp. 414, 417 n.4 (N.D. Ill. 1990) (describing operation of electronic bulletin boards).

[61] *See* S. REP. NO. 99-541, at 36, *reprinted in* 1986 U.S.C.C.A.N. at 3590 ("To access a communication in such a public system is not a violation of the Act, since the general public has been 'authorized' to do so by the facility provider.").

[62] *See* Snow v. DirecTV, Inc., 450 F.3d 1314, 1321-22 (11th Cir. 2006) (refusing to provide SCA protection to posts on bulletin board freely accessible to public); Kaufman v. Nest Seekers, LLC, No. 05 CV 6782(GBD), 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006) ("Only electronic bulletin boards which are not readily accessible to the public are protected under the Act.").

[63] *See Snow*, 450 F.3d at 1321 ("Given the Web's ubiquitous and public nature, it becomes increasingly important in cases concerning electronic communications available through the Web for a plaintiff to demonstrate that those communications are not readily accessible."). A user could gain access to the electronic bulletin board in *Snow* merely by registering, creating a password, and accepting the terms of use. *See id.* (reciting facts of complaint). However, so few requirements do not keep the postings from being readily accessible. *See id.* at 1322 (explaining holding of court).

[64] *Id.* at 1320-21 (interpreting language of SCA).

[65] *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) ("Thus, the SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system (BBS)."); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002) ("The legislative history of the [SCA] suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards."); Becker v. Toca, No. 07-7202, 2008 WL 4443050, at *4 (E.D. La. Sept. 26, 2008) ("Courts have interpreted the statute to apply primarily to telephone companies, internet or e-mail service providers, and bulletin board services."); Inventory Locator

However, courts are split as to whether an electronic bulletin board provider is an ECS or RCS provider.[66]

The importance of classifying a communication as either ECS or RCS is also illustrated in courts' analyses of e-mail under the SCA.[67] Although courts have not reached the same conclusion as to the classification of e-mail providers, the variation can be explained in part due to the way different e-mail technology functions.[68] Currently, there are two general types of e-mail services: web-based e-mail and non-web-based e-mail.[69] Web-based e-mail services, such as Gmail, Yahoo!, and Hotmail, do not require their users to download messages to their hard drive in order to read the messages.[70] Users may access their account—and any messages stored thereon—on any computer via the internet, and the e-mail stays on the provider's servers; there is no other copy downloaded to a user's computer.[71] In contrast, in non-web-based e-mail platforms, such as

---

Serv., LLC v. Partsbase, Inc., No. 02-2695 MA/V, 2005 WL 2179185, at *24 (W.D. Tenn. Sept. 6, 2005) (finding SCA applied to password-protected website containing an electronic bulletin board).

[66] *Compare Kaufman*, 2006 WL 2807177, at *5 ("An electronic bulletin board fits within the definition of an [ECS] provider."), *with* Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 443 (W.D. Tex. 1993) (holding bulletin board service at issue was an RCS), *aff'd*, 36 F.3d 457 (5th Cir. 1994). The *Jackson* court reasoned that the electronic bulletin board provided a service that allowed its users to store public and private communications, which fit within the definition of an RCS provider. *See Jackson*, 816 F. Supp. at 442-43 (explaining operation of electronic bulletin board). The *Kaufman* court issued its opinion on a motion to dismiss and only cited authority regarding the SCA's applicability to electronic bulletin boards; the court did not provide any authority for its finding that an electronic bulletin board is an ECS provider under the SCA. *See Kaufman*, 2006 WL 2807177, at *5 (referencing courts that found electronic bulletin boards to fall within SCA).

[67] *See supra* notes 46-49 and accompanying text (discussing greater protection afforded ECS communications stored for 180 days or less); *see also* United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009) ("Thus, for emails less than 181 days old, the question of whether a warrant is necessary turns on whether the emails are 'in electronic storage' or are 'held or maintained . . . solely for the purpose of providing storage or computer processing services to [the] subscriber or customer.'" (quoting 18 U.S.C. § 2703(b)(2))).

[68] *Compare* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (holding opened, non-web-based e-mails were ECS communications), *with Weaver*, 636 F. Supp. 2d at 773 (holding opened, web-based e-mails were RCS communications).

[69] *See Weaver*, 636 F. Supp. 2d at 772 (distinguishing web-based e-mail from traditional non-web-based e-mail that requires downloading of messages).

[70] *See id.* (citing James X. Dempsey, *Digital Search & Seizure: Standards for Government Access to Communications and Associated Data*, *in* 970 PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK 687, 707 (Practising Law Inst. 2009), *available at* Westlaw PLI-PAT). "[A]ll of a subscriber's messages—sent, received, opened, unopened, unsent drafts—are kept on third party servers." Dempsey, *supra*, at 722.

[71] *See Weaver*, 636 F. Supp. 2d at 772 (explaining web-based e-mail users typically do not download messages, but rather access online only). "[I]f Hotmail users save a message, they generally leave it on the Hotmail server and return to Hotmail via the web to access it on subsequent occasions." *Id.*

Microsoft Exchange Server, accounts are often configured to download messages to a user's local drive, with a copy remaining on the Exchange server.[72]

An e-mail will only receive the greater protections of ECS classification if it is held in "electronic storage," which includes two types of communications: temporary storage incidental to transmission and storage for backup protection.[73] Courts agree that the first type—temporary storage that is incidental to transmission—covers unopened e-mails waiting to be read by the recipient.[74] Where the e-mail has been opened, courts disagree on the classification.[75] For an opened e-mail to continue to be classified as an ECS communication, it must be held "for purposes of backup protection" since the first definition of electronic storage—temporary storage incidental to transmission—is no longer applicable.[76]

"Backup protection" in the context of e-mail messages has been interpreted in two very different ways.[77] The first interpretation as applied to e-mail takes the account user's perspective: "backup" involves customers leaving opened e-mail on the provider's server.[78] In contrast, the second interpretation takes the provider's perspective: "backup" refers to

---

[72] *See Weaver*, 636 F. Supp. 2d at 772 (discussing non-web-based e-mail systems that download messages from ISP's server to local drive); *see also Leave E-mail Messages on Your E-mail Server*, MICROSOFT OFFICE, http://office.microsoft.com/en-us/outlook-help/leave-e-mail-messages-on-your-e-mail-server-HA001150793.aspx (last visited May 29, 2012) (explaining functionality of Exchange Server). Exchange Server accounts can be configured to keep a copy of e-mail messages in a data file on a user's local drive, as well as on the e-mail server. *See Leave E-mail Messages on Your E-mail Server*, *supra*.

[73] *See supra* text accompanying notes 44-45 (defining ECS provider).

[74] *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) ("[T]he section is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission—for example, when an email service stores a message until the addressee downloads it."); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part, vacated in part*, 352 F.3d 107 (3d Cir. 2003) ("[Intermediate storage] covers a message that is stored . . . after the message is sent by the sender, but before it is retrieved by the intended recipient.").

[75] *See In re* U.S., 665 F. Supp. 2d 1210, 1214 n.1 (D. Or. 2009) ("The distinction [between ECS and RCS] can be difficult to draw."); *infra* notes 76-82 (describing courts' disparate classifications of opened e-mail messages).

[76] *See* 18 U.S.C. § 2510(17) (2006) (defining "electronic storage"); *supra* notes 44-45 and accompanying text (defining ECS provider).

[77] *See* WAYNE R. LAFAVE ET AL., 2 CRIMINAL PROCEDURE § 4.8(d) (3d ed.), *available at* Westlaw CRIMPROC (setting forth various interpretations of "backup protection"). *Compare* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (holding opened e-mails stored on server were stored for "backup protection"), *with Weaver*, 636 F. Supp. 2d at 773 (finding opened e-mails stored for users were not stored for "backup protection").

[78] *See* LAFAVE, *supra* note 77, § 4.8(d) (describing e-mail backup storage as keeping copy on provider's server).

copies of e-mails that providers make in case of system failure.[79] Under the first interpretation, opened e-mails remain in "electronic storage" and receive the heightened protections of ECS communications.[80] Under the second interpretation, however, opened e-mails are no longer held for "backup protection," thus removing them from the ECS classification and its corresponding heightened protection.[81] The SCA's legislative history lends support to this interpretation, and the *Theofel* court, in dicta, suggested it would make a similar finding regarding web-based e-mail providers.[82]

Another technology to which courts have applied the SCA is text messaging.[83] Courts have analyzed text messaging service on a case-by-

---

[79] *See id.* (setting forth alternate interpretation of backup storage). LaFave gives an example of this interpretation where an ISP makes backup copies of its entire server every night. *Id.* The day after an e-mail arrives and is read, the ISP will have two copies of the opened e-mail: it will have the original copy residing in the user's account and the backup copy. *Id.* The backup copy is a permanent copy made in case of system failure, and section 2510(17)(B) assures that the backup copy and original are both classified as ECS. *Id.*

[80] *See Theofel*, 359 F.3d at 1076 (refusing to distinguish between intermediate and post-transmission storage of e-mail in defining ECS). The user in *Theofel* had to download a copy of each e-mail message to his hard drive in order to read it, and another copy remained on the ISP's server. *See id.* at 1075 (framing court's analysis in context of messages downloaded from ISP server to user's computer). The *Theofel* court argued that an e-mail message, whether delivered or not, is ECS and not RCS because it is not "a message stored by a remote computing service 'solely for the purpose of providing storage or computer processing services to [the] subscriber.'" *Id.* at 1070 (quoting 18 U.S.C. §§ 2702(a)(2)(B), 2703(b)(2)(B)). A handful of other courts have followed the *Theofel* court's reasoning. *See* Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (adopting similar reasoning); Jennings v. Jennings, 697 S.E.2d 671, 677-78 (S.C. Ct. App. 2010) ("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.").

[81] *See Weaver*, 636 F. Supp. 2d at 770-71 (finding previously opened e-mail not stored for backup protection). The e-mail at issue in *Weaver* resided on Hotmail, a web-based e-mail account. *Id.* at 772. The court reasoned that because web-based e-mail users often do not download their messages, their online account is the only place where opened messages reside. *Id.* Subsequent to a user opening a message, the provider is "maintaining the messages 'solely for the purpose of providing storage or computer processing services to such subscriber or customer.'" *Id.* (quoting 18 U.S.C. § 2703(b)(2)). The *Theofel* court itself recognized when such an instance might arise: "A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes." *Theofel*, 359 F.3d at 1070.

[82] *See* H.R. REP. NO. 99-647, at 65 (1986) ("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 [the RCS provisions of] section 2702(a)(2).").

[83] *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th Cir. 2008) (determining provider classification for pager text messaging service), *rev'd in part on other grounds sub nom.* City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010); Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (analyzing classification of text message archival).

case basis, thus sometimes reaching different conclusions as to the provider's classification.[84] Regardless of the ultimate classification, the proper test is to determine the type of service being provided with respect to the communication at issue.[85]

Courts have also differentiated between services that *provide* users with the ability to send or receive electronic communications and services that merely *utilize* the ability to send or receive electronic communications.[86] Internet-based services that allow consumers to send or receive electronic communications incidental to some other primary purpose are not considered providers of electronic communications services under the SCA.[87]

B. The SCA Applied to Social Networking

1. How Facebook Works

Social network sites allow users to "(1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[88] Of the popular

---

[84] *Compare Quon*, 529 F.3d at 900 (holding text messaging service to be ECS), *with Flagg*, 252 F.R.D. at 363 (finding provider's storage of *archived* text messages to be RCS). The court described the text messaging service in *Quon* as "a 'service' that enabled Quon and the other Appellants to 'send or receive . . . electronic communications,' i.e., text messages." *Quon*, 529 F.3d at 901 (quoting definition of ECS as found at 18 U.S.C. § 2510(15)). Conversely, the provider in *Flagg* was no longer providing text messaging service. *See Flagg*, 252 F.R.D. at 347-48 (giving background facts of case). Therefore, the court found the provider was an RCS provider at that point in time because "any archive of text messages that SkyTel continues to maintain . . . constitutes the *only* available record of these communications, and cannot possibly serve as a 'backup' copy of communications stored elsewhere." *Id.* at 363.

[85] *See Flagg*, 252 F.R.D. at 362 ("[T]he prohibitions against disclosure . . . focus on the specific type of service being provided (an ECS or an RCS) with regard to a particular communication, and do not turn upon the classification of the service provider or on broad notions of the service that this entity generally or predominantly provides.").

[86] *See* United States v. Standefer, No. 06-CR-2674-H, 2007 WL 2301760, at *4 (S.D. Cal. Aug. 8, 2007) (applying SCA to website that facilitated gold exchange between users); Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (discussing communications between Amazon.com and its customers).

[87] *See Standefer*, 2007 WL 2301760, at *4 ("The Court concludes that e-gold is not a service which *provides* users the ability to send or receive electronic communications, rather e-gold is a service which *utilizes* the ability to send or receive electronic communications to permit the instant transfer of gold ownership between its users."); *see also Crowley*, 166 F. Supp. 2d at 1270 (finding Amazon "is an online merchant, not an electronic communication service provider").

[88] Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, J. COMPUTER-MEDIATED COMM. (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (defining "social network sites").

social network websites, Facebook currently has the most number of users.[89] The site allows users to stay in touch with their friends, upload photos, share website links and videos, and meet new people.[90] Individuals can also share content with a broad audience via a status update, with a small group of friends using the Groups feature, or with just a single individual via a wall post or private message.[91] When a user logs in to Facebook, he is taken to the home page, where a "news feed" shows a constantly updating list of friends' activity.[92] Users may request notifications via e-mail when they receive new messages, wall posts, comments, etc.[93] Also, smartphone users may download the Facebook application, which provides notifications for similar Facebook activities,

---

[89] *See Facebook and Twitter Post Large Year over Year Gains in Unique Users*, NIELSEN COMPANY (May 4, 2010), http://blog.nielsen.com/nielsenwire/global/facebook-and-twitter-post-large-year-over-year-gains-in-unique-users (comparing number of users on Facebook, MySpace, Twitter, LinkedIn, and Classmates Online).

[90] *See Facebook - Résumé*, FACEBOOK, http://www.facebook.com/facebook?sk=info (last visited May 29, 2012) (summarizing purpose of Facebook).

[91] *See How Do I Share a Status or Other Content on Facebook?*, FACEBOOK, http://www.facebook.com/help/?faq=132371443506290 (last visited May 29, 2012) (describing different ways to share content). A wall is a space on a person's profile that allows the user and his friends to post and share comments, pictures, website links, and other content. *See What Can I Do on the Wall (Timeline)?*, FACEBOOK, http://www.facebook.com/help/?faq=224964477515963 (last visited May 29, 2012) (describing purpose of "wall"). Posts to a person's wall may be viewed by everyone, friends only, friends of friends, or some other custom group of people, depending upon a user's privacy settings. *See When I Share Something, How Do I Choose Who Can See It?*, FACEBOOK, http://www.facebook.com/help/?faq=120939471321735#When-I-share-something,-how-do-I-choose-who-can-see-it? (last visited May 29, 2012) (detailing privacy settings for user's wall); *infra* notes 95-101 and accompanying text (describing default and customized privacy settings available to users). Users can also send private messages, which function similarly to web-based e-mail services like Gmail or Hotmail and are viewable only by the recipient or recipients. *See Who on Facebook Can See My Messages?*, FACEBOOK, http://www.facebook.com/help/?faq=212388195458335 (last visited May 23, 2012) ("You and the people you're messaging with can view the contents and history of your conversation.").

[92] *See What Is News Feed?*, FACEBOOK, http://www.facebook.com/help/?faq=210346402339221 (last visited May 24, 2012) (explaining purpose of news feed).

[93] *See Notifications*, FACEBOOK, http://www.facebook.com/help/notifications (last visited May 29, 2012) (explaining how to control notifications received by e-mail). Since 2007, e-mail notifications for new Facebook messages include the full text of the message and leave the actual message in the user's Facebook inbox. *See* Justin Smith, *Facebook Message Email Notifications Now Include the Actual Message*, INSIDE FACEBOOK (Dec. 6, 2007), http://www.insidefacebook.com/2007/12/06/facebook-message-email-notifications-now-include-the-actual-message (praising new Facebook message notifications that include message body). When a user receives a notification about a comment, post, or picture on his wall, the actual comment, post, or picture stays on his wall. *See Notifications*, *supra* (describing how notifications work); *What Can I Do on the Wall (Timeline)?*, *supra* note 91 (discussing ways to share content using wall feature).

including the full text of private messages the user receives.[94]

Facebook provides a multitude of privacy settings to allow users to control how information is shared on the website.[95] Facebook's privacy policy sets forth its terms of use, including how Facebook uses and shares individuals' information.[96] Users can select from a variety of privacy settings for each type of content they post; one such setting is called "Public."[97] Information set to "Public" may be accessed by everyone on the internet, including people not logged into Facebook.[98] Once a user deletes such information, the content is removed from Facebook, but it may have already been used, saved, or downloaded outside of Facebook.[99] Users can change the privacy settings for their content on Facebook.[100] In addition to the "Public" setting, users can choose to share content with "Friends of Friends," "Friends," or some other custom group of people.[101]

2. Application of the SCA to Social Network Sites

The first court to issue a decisive and in-depth opinion on Facebook's provider status under the SCA was *Crispin v. Christian Audigier, Inc.*[102] In *Crispin*, a copyright infringement case, the defendants

---

[94] *See Facebook for Android*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.facebook.katana (last visited May 25, 2012) (describing ways to use Facebook application on Android phones); *Free Facebook*, BLACKBERYY APP WORLD, http://appworld.blackberry.com/webstore/content/680/?lang=en (last visited May 25, 2012); *Facebook for iPhone App*, FACEBOOK, http://www.facebook.com/help/mobile/iphone (last visited May 25, 2012) (providing answers to frequently asked questions regarding application). For smartphone application users, messages are delivered to their handset, and a copy remains on their Facebook account as well. *See id.*

[95] *See Data Use Policy*, FACEBOOK, http://www.facebook.com/full_data_use_policy (last updated Sept. 23, 2011) (providing privacy policy background).

[96] *See id.* (discussing various information that users may share and how Facebook uses that information).

[97] *See id.* (describing ways to share information); *see also What Audiences Can I Choose from When I Share?*, FACEBOOK, http://www.facebook.com/help/?faq=211513702214269 (last visited May 29, 2012) (explaining privacy settings).

[98] *See What Audiences Can I Choose from When I Share?*, *supra* note 97 (explaining privacy settings).

[99] *See Data Use Policy*, *supra* note 95 ("[I]nformation you share on Facebook can be copied or re-shared by anyone who can see it.").

[100] *See When I Share Something, How Do I Choose Who Can See It?*, *supra* note 91 (explaining fundamental privacy settings).

[101] *See id.* (highlighting privacy setting categories). "Friends of Friends" is a special privacy setting available for minors and includes people who are friends with a user's friends. *See What Does the "Friends of Friends" Privacy Setting Mean?*, FACEBOOK, http://www.facebook.com/help/?faq=168814273179270 (last visited May 24, 2012) (expanding on privacy settings features).

[102] 717 F. Supp. 2d 965 (C.D. Cal. 2010).

served subpoenas on third-party businesses, including Facebook.[103] The defendants demanded Facebook turn over communications between the plaintiff and another individual.[104] As to private messages, the court followed precedent regarding e-mail messages and accordingly held that Facebook was an ECS provider with respect to unopened messages and an RCS provider with respect to messages that were opened and retained on Facebook by the user.[105] The court further explained that posts on users' walls were analogous to electronic bulletin boards, and thus were a form of ECS under established precedent.[106]

Nevertheless, case law on the SCA's applicability to users' Facebook account communications remains scant, in part because some courts make a finding on the validity of a subpoena without discussing the SCA.[107] For example, the defendant in *Ledbetter v. Wal-Mart Stores, Inc.*[108] sought production of the contents of the plaintiffs' social network sites in an attempt to contradict the plaintiffs' claims of permanent physical and psychological injuries.[109] The plaintiffs moved for a protective order regarding the social network contents, but the court held that the information sought by the subpoenas was "reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues in this

---

[103] *See id.* at 968-69 (explaining background of case). Crispin alleged that he granted Audigier a license to use Crispin's works of art for a specified sum of money. *See id.* at 968. Audigier purportedly used Crispin's works in various applications outside of the scope of the license agreement. *See id.* The defendants claimed that the social network communications were relevant in determining the exact terms of the licensing agreement between Crispin and Audigier. *See id.*

[104] *See id.* at 968-69 (describing nature of communications sought).

[105] *See id.* at 987 (differentiating between private messages and wall posts).

[106] *See id.* at 980 ("Facebook wall postings . . . are not strictly 'public,' but are accessible only to those users plaintiff selects. The court therefore finds relevant, if not controlling, the authority regarding private electronic bulletin board services ('BBS')."). The court further explained that a Facebook profile page and the wall postings contained thereon function similarly to restricted-access electronic bulletin boards, and thus "there is no basis for distinguishing between a restricted-access BBS and a user's Facebook wall." *Id.* at 981. Legislative history had already made it clear that restricted-access electronic bulletin boards were ECS providers. *See id.* (referencing SCA Senate Report). Finally, the court concluded that Facebook *provides* electronic communications as opposed to merely *utilizing* such communications. *See id.* at 982 n.35 ("[T]he definition of an ECS provider 'does not encompass entities that merely use the internet to sell goods or services.' The goal of Facebook . . . is not to buy or sell books, gold, or travel services. . . . Facebook and MySpace provide an electronic venue to communicate, either one-to-one by private messaging or with a large group of friends through wall postings and comments.").

[107] *See* Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009) (denying motion for protective order regarding subpoena issued to Facebook without discussing SCA).

[108] No. 06-cv-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009).

[109] *Id.* at *1 (describing case background).

case," without discussing SCA implications.[110] Courts have avoided analyzing the SCA's applicability to Facebook in some creative ways; one court went so far as to recommend that an individual "friend" the judge on Facebook in order to avoid analysis of the SCA.[111] In another case, the court ordered the plaintiff to produce his Facebook user name and password so as to allow the defendant access to all communications on the plaintiff's user account.[112] The plaintiff did not raise the SCA as a defense, and the court did not discuss the SCA.[113] However, in some instances where a party fails to object to disclosure of social media contents, Facebook objects, citing the SCA.[114] In fact, Facebook's website cites the SCA in answering a frequently asked question about law enforcement and third-party matters:

> Federal law prohibits Facebook from disclosing user content (such as messages, Wall (timeline) posts, photos, etc.) in response to a civil subpoena. Specifically, the Stored Communications Act, 18 U.S.C. §2701 et seq., prohibits Facebook from disclosing the contents of an account to any non-governmental entity pursuant to a subpoena or court order.[115]

---

[110] *Id.* at *2.

[111] *See* Barnes v. CUS Nashville, LLC, No. 3:09-CV-00764, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010) ("If [the individuals] will accept the Magistrate Judge as a 'friend' on Facebook for the sole purpose of reviewing photographs and related comments *in camera*, he will promptly review and disseminate any relevant information to the parties."); *see also* Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387, 388 n.1 (E.D. Mich. 2012) ("I do not here address the question of whether . . . a direct subpoena for such material to Facebook could be challenged under the Stored Communications Act . . . ."); Barnes v. CUS Nashville, LLC, No. 3:09-0764, 2010 WL 2196591, at *1 (M.D. Tenn. May 27, 2010) (noting Facebook's objection to disclosure of user content under SCA).

[112] *See* McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010) ("[W]hatever relational harm may be realized by social network computer site users is undoubtedly outweighed by the benefit of correctly disposing of litigation."); *see also* Gallion v. Gallion, No. FA114116955S, 2011 WL 4953451, at *1 (Conn. Super. Ct. Sept. 30, 2011) (ordering counsel for parties to exchange clients' Facebook passwords).

[113] *See McMillen*, 2010 WL 4403285.

[114] *See* Juror No. One v. California, No. CIV. 2:11-397 WBS JFM, 2011 WL 567356, at *1 (E.D. Cal. Feb. 14, 2011) (describing Facebook's moving to quash subpoena for profile content based on SCA grounds); *Barnes*, 2010 WL 2196591, at *1 (acknowledging Facebook's objection to disclosure based on SCA).

[115] *May I Obtain Contents of a User's Account from Facebook Using a Civil Subpoena?*, FACEBOOK, http://www.facebook.com/help/?faq=133221086752707 (last visited May 25, 2012).

IV. ANALYSIS

Whether, and to what extent, the SCA protects disclosure of social network communications is increasingly important to litigants.[116] The classification of communications is also important to communication providers such as Facebook, as it sets forth the requirements for compelling providers to disclose their users' communications.[117] Because there is no pending effort to amend the SCA to better address social networking or to enact legislation to otherwise protect such communications, the existing case law applying the SCA to similar technologies will be most determinative in the near future in ascertaining what types of social network content—if any—will be protected.[118] In order for civil litigants to compel Facebook to disclose communications, Facebook must not be a provider of either ECS or RCS communications.[119] If it provides *either* service, it is governed by the SCA, and a party may not compel disclosure because the SCA provides no exception for civil discovery requests or subpoenas for either ECS or RCS providers.[120] Whether the government may compel Facebook to disclose communications in criminal cases will depend upon the classification of the type of communication at issue.[121] The government will argue that Facebook communications are governed by the less restrictive RCS requirements, and defendants will argue the communications are governed by the more restrictive ECS requirements.[122]

One commentator has suggested that all social media content should be classified into two categories: content that is set to the "Everyone" privacy setting and content that is set to any other privacy setting, including "Friends of Friends," "Friends Only," or "Other."[123]

---

[116] *See supra* note 5 and accompanying text (providing instances in which social network communications can be central to outcome of litigation).

[117] *See supra* notes 43-50 and accompanying text (discussing separate standards for compelling ECS and RCS providers to disclose user content).

[118] *See supra* note 55-58 and accompanying text (describing recent proposed legislation's failure to address modern forms of communication). Despite pressure from large corporations to update the SCA, it has remained largely unchanged, and courts are forced to apply precedent from other older technologies to social network communications. *See supra* notes 102-106 and accompanying text (setting forth precedent applied to Facebook in *Crispin*).

[119] *See* sources cited *supra* note 50 (stressing lack of exception for compelled disclosure of ECS and RCS communications in civil litigation).

[120] *See supra* note 50 and accompanying text (noting absence of exception).

[121] *See supra* notes 43-48 and accompanying text (comparing procedure for compelling ECS communications to procedure for compelling RCS communications).

[122] *See supra* notes 43-49 and accompanying text (emphasizing that heightened requirement applies for compelling ECS communications held for 180 days or less).

[123] *See* Ryan A. Ward, Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J.L. & TECH. 563, 585 (2011). Although the exact names

Content governed by the "Everyone" setting would be treated as "public" information that is not protected by the SCA; the remaining content would be subject to the SCA.[124] Social networks would be ECS providers for unread private messages and RCS providers for opened private messages.[125] They would be ECS providers for content that is "generally visible to other people on the social network," including wall posts, photographs, and status updates.[126] This approach would provide bright-line rules for courts in applying the SCA to social media.[127]

However, the convenience gained under this approach would be at odds with the SCA's communication-specific analysis.[128] Content that is generally available to other people on the social network can vary greatly; that content could be viewable by all 901 million people on Facebook, or it could be available to just a handful of close friends.[129] A person's reasonable expectation of privacy is very different in those two extremes, and the SCA requires that they be treated accordingly.[130] Although it may be argued that courts should "avoid drawing arbitrary lines related to the number of people who can view something," courts are very capable of making such factual determinations.[131] Furthermore, the types of communications on Facebook are constantly changing, and courts should establish general guiding principles rather than bright-line rules based on the terminology and technology currently in use.[132] Because the proper analysis is communication-specific, practitioners will be left to make arguments based on established precedent; a few of those arguments are

---

of the privacy settings have changed since the publication of this commentator's piece, the author uses this commentator's names for the reader's convenience. *See When I Share Something, How Do I Choose Who Can See It?*, *supra* note 91 (listing new settings as "Public," "Friends of Friends," "Friends," and "Custom").

[124] *See* Ward, *supra* note 123, at 584-85.

[125] *See id.* at 586.

[126] *Id.* at 584, 586.

[127] *See id.* at 585 (noting that approach would allow courts to avoid "drawing arbitrary lines" in determining "public" content).

[128] *See supra* note 27 and accompanying text (noting relevant analysis is based on individual communications).

[129] *See supra* notes 95-101 and accompanying text (describing different levels of privacy settings).

[130] *See supra* notes 18-22 and accompanying text (discussing constitutional protections and congressional intent to provide "reasonable expectation of privacy" for electronic communications).

[131] *See* Ward, *supra* note 123, at 585 (recommending courts avoid arbitrary line-drawing); *see also* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (remanding case for evidentiary development regarding plaintiff's privacy settings).

[132] *See generally What's New on Facebook*, FACEBOOK, http://www.facebook.com/help/whats-new-on-facebook (last visited May 29, 2012) (describing ever-changing Facebook features).

summarized below.[133]

A. Arguments That the SCA Does Not Protect Facebook Communications

The strongest argument for the government—and the only argument for civil litigants compelling disclosure—is that wall posts, status updates, and comments are not protected electronic communications under the SCA.[134] Facebook's data use policy allows certain information to be viewed by anyone—including non-Facebook users.[135] Case law has made clear that communications that are "readily accessible" by the public are not protected by the SCA.[136] Even content that is not viewable by everyone by default may be "readily accessible," because a user's comments on photos and posts on others' walls may be viewed by individuals with whom that user is not friends.[137] An example helps illustrate this concept:

> Suppose P sues D, a ski lift operator, for injuries P incurred when the lift malfunctioned. P claims he is permanently disabled as a result of the accident. P is friends with F on Facebook. After the accident, P writes on F's wall, "Can't wait to ski the fresh powder this weekend!" F posts pictures on F's Facebook profile after the ski trip, and P comments on one, "Great weekend of hitting the slopes."

F's privacy settings determine who can see P's comments on F's wall and the ski picture; if F's privacy setting for his wall is "Public," everyone—even non-Facebook members—may view P's comments on F's picture and wall.[138] P's communications may have become viewable by

---

[133] *See supra* note 27 and accompanying text (explaining SCA's communication-specific analysis); *infra* Parts IV.A-C (setting forth arguments for maximum and minimum protection of communications).

[134] *See supra* note 35 (noting protections of SCA only afforded to providers of ECS and RCS communications). The government may make alternate arguments that, if wall posts, status updates, and comments *are* protected by the SCA, then they should only be afforded minimal protections as RCS communications; this Note addresses such arguments in Part IV. *See infra* text accompanying notes 158-72 (setting forth potential arguments supporting RCS classification for Facebook communications).

[135] *See supra* notes 97-98 and accompanying text (detailing Facebook's privacy settings for user content).

[136] *See supra* notes 64-65 and accompanying text (providing history of application of SCA to electronic bulletin boards).

[137] *See supra* notes 100-01 and accompanying text (explaining how different privacy settings function).

[138] *See supra* notes 97-98 and accompanying text (detailing default privacy settings).

anyone with internet access and thus would not be protected by the SCA.[139] Both case law and the legislative history of the SCA make clear that such easily accessible information does not fall within the SCA.[140] Moreover, even if F adjusted the privacy settings pertaining to his own wall and photos to the most restrictive preset category—"Friends"—P's comments will be visible to a group of people over whom P has no control.[141] Furthermore, despite the complex and ever-changing privacy settings of Facebook, the social network's primary purpose is to allow users to share information with each other.[142]

Private messaging on Facebook functions very similarly to web-based e-mail.[143] *Crispin*, the only court to provide a comprehensive opinion on the SCA's applicability to social networks as of the publishing of this Note, discussed SCA cases involving e-mail and concluded that the reasoning in those cases was instructive in determining whether private messages fall within the SCA.[144] As a result, the *Crispin* court found that the SCA did apply to the messages.[145] Whether the messages constitute ECS or RCS communications, however, is unclear at this point, and arguments exist for both classifications.[146]

B. Arguments for Maximum Protection Under the SCA

Defendants and civil litigants resisting disclosure will argue that wall posts, comments, and status updates are ECS communications and

---

[139] *See supra* notes 97-98 and accompanying text (emphasizing internet users not logged in to Facebook may view certain content under default settings).

[140] *See supra* notes 59-61 and accompanying text (citing legislative report's exclusion of readily accessible bulletin boards from SCA); *supra* notes 62-64 and accompanying text (summarizing case law requiring electronic bulletin boards not be readily accessible to fall within SCA).

[141] *See supra* notes 100-01 and accompanying text (discussing settings for different levels of privacy). Because P's comments are on F's picture and wall, F's privacy settings determine who can view those comments. *See When I Share Something, How Do I Choose Who Can See It?*, *supra* note 91.

[142] *See* Cohen v. Facebook, Inc., 798 F. Supp. 2d 1090, 1092 (N.D. Cal. 2011) ("Facebook exists because its users *want* to share information—often about themselves—and to obtain information about others . . . .").

[143] *See supra* note 91 and accompanying text (explaining private message function).

[144] *See supra* note 105 and accompanying text (describing *Crispin* court's reliance on e-mail message precedent).

[145] *See supra* note 105 and accompanying text (discussing holding of *Crispin* with regards to private messages).

[146] *See infra* text accompanying notes 154-57 (supporting ECS classification of private messages); *infra* text accompanying notes 160-64 (supporting RCS classification of private messages).

should therefore receive the greatest protection under the SCA.[147] In the context of the purpose of the SCA and the technology that existed at the time of the SCA's enactment, wall posts, comments, and status updates are more analogous to ECS communications than to RCS communications.[148] The SCA classifications reflect businesses that outsourced their computing tasks to computing providers.[149] RCS providers consisted of businesses providing off-site electronic data storage or data processing for customers.[150] Facebook is not a company that provides remote computers to store businesses' extra files or processes large amounts of data; it is a way for people to stay in touch.[151] An ECS communication is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[152] As one court concluded about text messages, the ECS definition describes "on its face" the service Facebook provides.[153]

For users that receive e-mail notifications when they receive a message on Facebook, opened messages are analogous to e-mail messages that are downloaded from the e-mail provider's server to a user's computer.[154] For these users, there are two copies of the message.[155] Because the e-mail notification contains the text of the message, the copy of the message residing on Facebook's website is analogous to a copy of an

---

[147] *See supra* notes 44-49 and accompanying text (addressing compelled disclosure and heightened requirements for ECS communications). Civil litigants need only show that the communication is either an ECS or RCS communication because neither may be compelled in civil discovery. *See supra* note 50 and accompanying text (differentiating between government actors compelling communications and civil litigants compelling communications). In Part IV.C, this Note addresses alternate arguments that wall posts, comments, and status updates are RCS communications and, thus, still protected from compelled disclosure. *See infra* text accompanying notes 158-72 (discussing arguments for lesser protection under SCA).

[148] *See supra* note 30 and accompanying text (citing legislative history describing businesses outsourcing large computing and storage tasks to RCS providers).

[149] *See* Kerr, *supra* note 11, at 1213-14 (providing technological context for SCA enactment). The author notes, "This was in the era before spreadsheet programs, so users generally needed to outsource tasks to perform what by today's standards are simple number-crunching jobs." *Id.* at 1214.

[150] *See id.* at 1214.

[151] *See supra* note 1 and accompanying text (defining purpose and use of Facebook as social network website).

[152] *See* 18 U.S.C. § 2510(15) (2006) (defining ECS).

[153] *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 901 (9th Cir. 2008), *rev'd in part on other grounds sub nom.* City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010); *supra* note 84 (discussing text messaging service as ECS).

[154] *See supra* note 80 and accompanying text (explaining operation of non-web-based e-mail retrieval); *supra* note 93 and accompanying text (describing two copies of messages for users who choose to receive notifications for private messages).

[155] *See supra* note 93 (noting message appears in body of notification e-mail yet stays in Facebook inbox).

e-mail left on a server, which courts have found to be an ECS communication.[156] Individuals who use the Facebook application for smartphones and elect to receive copies of messages on their phone will similarly have two copies of messages.[157]

C. Arguments for Lesser Protection Under the SCA

Civil litigants resisting disclosure may alternatively argue that wall posts, status updates, and comments are RCS communications, and thus prohibited from compelled disclosure.[158] In criminal cases, the government may rely on these same arguments as an alternate to its argument that Facebook communications are not governed by the SCA; arguing that, if Facebook communications *are* governed by the SCA, they must be RCS communications, which would allow the less restrictive RCS compelled disclosure rules to govern.[159]

Facebook is an RCS provider with regards to private messages between individual users because it is merely "providing storage . . . services" for such messages.[160] Opened messages are functionally analogous to opened e-mail messages, which the majority of courts have agreed are RCS communications.[161] Only the United States Court of Appeals for the Ninth Circuit has clearly held that opened e-mail may be ECS in certain situations.[162] However, the e-mail at issue in that case was of the type that is downloaded to a user's computer from the ISP's server,

---

[156] *See supra* notes 77-78, 80 and accompanying text (explaining one interpretation of "backup protection"). Courts have held that an e-mail left on a server is kept for "backup protection," which is one of the two definitions of "electronic storage." *See supra* notes 77-78, 80 and accompanying text (discussing various courts' definitions of "backup protection" and storage).

[157] *See supra* note 94 and accompanying text (highlighting message delivery on smartphone application).

[158] *See supra* note 35 and accompanying text (describing SCA's prohibition of compelled disclosure of either ECS or RCS communications in civil litigation).

[159] *See supra* notes 43-49 and accompanying text (describing heightened compelled disclosure requirements applicable to ECS communications held less than 180 days).

[160] 18 U.S.C. § 2702(a)(2)(A)-(B) (2006) (setting forth nature of services provided by RCS provider); *see supra* notes 29-30 and accompanying text (distinguishing ECS and RCS communications); *infra* text accompanying notes 161-64 (suggesting supporting arguments for classifying private messages as RCS communications).

[161] *See supra* notes 75-81 and accompanying text (describing courts' classifications of opened e-mail messages).

[162] *See supra* notes 75-80 and accompanying text (providing minority view of Ninth Circuit's classification of opened e-mails as ECS communications (citing Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004))).

as opposed to web-based e-mail such as Gmail, Hotmail, or Yahoo!.[163] Applying the Ninth Circuit's reasoning to web-based e-mail, those messages exist only online and are held solely for storage (an RCS function), not for "backup protection" (an ECS function).[164]

Wall posts and comments that are viewed are also comparable to opened, web-based e-mail, and therefore constitute RCS communications.[165] The recipient—the owner of the wall, picture, or status on which the user comments—has read and chosen to retain the communication.[166] Indeed, the legislative history of the SCA contemplates communications that an addressee receives and retains "for re-access at a later time."[167] Case law regarding electronic bulletin boards and text messages supports an RCS classification for these types of communications as well.[168] Courts have classified electronic bulletin boards that allow their users to store both public and private electronic communications as RCS providers.[169] Where the communication at issue is the only copy, it cannot serve as a backup copy, and, thus, cannot be an ECS communication.[170] Even when a Facebook user utilizes e-mail notifications or the Facebook

---

[163] *See Theofel*, 359 F.3d at 1075 ("An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again-if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a 'backup' for the user."); *see also* note 80 (describing facts of *Theofel*).

[164] *See supra* note 80 (setting forth facts of *Theofel* and court's reasoning). Courts that have followed *Theofel* have reached the same conclusion only as to e-mail messages that had to be downloaded to one's computer, as opposed to web-based e-mail where the only copy resides on the provider's servers. *See supra* note 80 (same).

[165] *See supra* notes 75-81 and accompanying text (describing majority classification of opened e-mails as RCS communications).

[166] *See supra* notes 90-91 and accompanying text (describing wall, status, and picture content use on Facebook). *But see* Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 361 (2011) (arguing communications are retained by default and deletion of content is rare). "[C]ontent on Facebook does not disappear unless the user actively deletes it, which, unlike e-mail, is not a standard practice. . . . Indeed, those who notice that a Facebook user has deleted a photo, message, link, or connection may assume that the user was trying to hide something." Semitsu, *supra*, at 361 & n.264.

[167] H.R. REP. NO. 99-647, at 65 (1986); *see supra* note 82 and accompanying text (providing legislative history of SCA).

[168] *See supra* note 66 (discussing *Jackson* court classification of electronic bulletin board service provider as RCS). Although the *Kaufman* court found electronic bulletin board providers to be ECS providers, the court's decision did not cite any authority for its classification. *See supra* note 66 (same).

[169] *See supra* note 66 (discussing *Jackson* holding and reasoning).

[170] *See supra* note 84 and accompanying text (discussing text messages in provider's possession as RCS where they were sole copy of messages). The *Flagg* court held that where there is only one copy of a communication, that copy cannot possibly serve as a backup copy, and thus is not an ECS communication. *See supra* note 84 (setting forth *Flagg* holding).

application on his smartphone, the copy that is subsequently accessed is likely to be online.[171] The online copy is not a "backup" copy, however, because there is no other primary copy of that communication.[172]

IV. CONCLUSION

The SCA provides important privacy protections for electronic communications, which have become a primary way in which individuals communicate on a daily basis. Because Facebook communications are often very candid and personal, they have become increasingly important to the resolution of civil and criminal cases. However, in civil cases, communications that fall within the SCA may not be compelled from the provider of the communication service. In criminal cases, such communications may be compelled only through the process described in the SCA. Compelling communications from ECS providers is more difficult than compelling communications from RCS providers. Therefore, whether Facebook communications fall within the SCA, and determining their potential classification thereunder, has become increasingly important to litigants.

Although certain Facebook communications resemble other traditional communications for which there is established SCA precedent, some Facebook communications have no traditional counterpart. Private messages that have been read are functionally similar to opened e-mails, which most courts agree are RCS communications. Status updates and wall posts to a user's profile whose privacy settings prevent public viewing resemble posts on restricted-access electronic bulletin boards. Such bulletin boards are protected under the SCA as an RCS storage service. However, where a user's privacy settings allow the general public to view such communications, it is clear that the SCA will not govern such "readily accessible" communications. Courts have not yet had the opportunity to define what constitutes "readily accessible" wall posts or status updates when a user's privacy settings allow some, but not all, Facebook users to view content posted on their profile. These quasi-public communications are precisely the type of communications that lack analogous case law.

Because the SCA's applicability depends on the particular communication at issue, courts will have to analyze the circumstances of each instance in which litigants compel Facebook to turn over the contents

---

[171] *See supra* note 93 and accompanying text (describing e-mail notifications for messages, wall posts, and comments).

[172] *See supra* note 93 and accompanying text (explaining functioning of comments, posts, and pictures on a user's wall).

of a user's profile. The user's privacy settings and the number of individuals that have access to the profile will be directly relevant in ascertaining whether a wall post, status update, comment, or some other future form of communication falls within the SCA. Making such fact-specific determinations that depend on nuanced differences in technology will require that both attorneys and judges have an extensive understanding of how different Facebook communications function, as well as a thorough understanding of SCA precedent.

Allen D. Hankins