Harvard Journal of Law & Technology
Volume 24, Number 2 Spring 2011

DISCOVERING FACEBOOK: SOCIAL NETWORK SUBPOENAS AND THE STORED COMMUNICATIONS ACT

*Ryan A. Ward**

TABLE OF CONTENTS

I. INTRODUCTION

For many people, online social networks have become an important part of everyday life. A recent study showed that Americans spend over 20% of their online time on social networks and blogs.[1] Although these networks began as sites where users could simply find

* Harvard Law School, Candidate for J.D., 2011. I would like to thank Tracie Bryant and the editors of the *Harvard Journal of Law & Technology* for their tireless work on this Note. Thanks also to Professor Frederic Bloom for his helpful comments on early drafts and his guidance throughout law school.

[1] *What Americans Do Online: Social Media and Games Dominate Activity*, NIELSEN WIRE (Aug. 2, 2010), http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-social-media-and-games-dominate-activity.

friends and view their contact information, they have grown increasingly complex. Modern social networking sites allow users to upload photographs and videos, post status updates, comment on friends' posts, play games, and send messages to other users. As the functionality of these sites has expanded, there has been a dramatic increase in both the number of users and the amount of content shared on social networks. Facebook, for example, currently has over five-hundred million active users, and the "[a]verage user creates 90 pieces of content each month."[2]

As Americans share more personal information on their social networking pages, lawyers have increasingly looked to these social networks as litigation resources.[3] Information from these sites is useful because "users of social network sites often 'let their hair down' in a way that surpasses even the thoughtless statements that all too often appear in email."[4] However, the best method for obtaining this information remains unclear. Lawyers can request social network information directly from users, but there may be problems with information access and formatting. Because social network users do not have access to the native format, they are only able to produce screenshots of their social network pages.[5] Additionally, it is impossible to know whether users have included all relevant information, because they may not have access to all of it.[6] For these reasons, many lawyers have found it easier to request social network information directly from social networks using civil subpoenas.[7] Social networks, like Facebook and Myspace,[8] have resisted these

[2] *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited May 6, 2011). According to Facebook, "50% of our active users log on to Facebook in any given day." *Id.*

[3] *See, e.g.*, Benjamin Rolf et al., *The Usefulness of Social Networking Websites to a Resourceful Defense Team*, STRICTLY SPEAKING (DRI, Chicago, Ill.), Feb. 11, 2008, at 1, *available at* http://www.dri.org/ContentDirectory/Public/Newsletters/0200/2008 Product Liability Committee Strictly Speaking Winter.pdf.

[4] James Parton, *Obtaining Records from Facebook, LinkedIn, Google and Other Social Networking Websites and Internet Service Providers*, DRI TODAY (May 24, 2010, 9:40 AM), http://forthedefense.org/post/Obtaining-Records-From-Facebook-LinkedIn-Google-and-Other-Social-Networking-Websites-and-Internet-Service-Providers.aspx.

[5] *See* Correy Stephenson, *Social Networking Sites Complicate Litigation*, NEW ORLEANS CITY BUS. (July 9, 2010, 8:16 AM), http://neworleanscitybusiness.com/blog/2010/07/09/social-networking-site-complicate-litigation/.

[6] The most obvious example is information that has been deleted by the user. In that case, only the social network will have access to this information, if it still exists on its servers.

[7] Facebook receives so many of these requests that it currently dedicates a section of its Help Center to answering questions about civil subpoenas. *See Law Enforcement and Third-Party Matters*, FACEBOOK, http://www.facebook.com/help/?page=1057 (last visited May 6, 2011).

[8] Myspace, previously "MySpace," rebranded the website and introduced a new suite of products on October 27, 2010. *See Meet the New Myspace*, MYSPACE, http://www.myspace.com/pressroom/2010/10/meet-the-new-myspace/ (last visited May 6, 2011).

subpoenas, however, by invoking the protection of the Stored Communications Act ("SCA").[9]

Since the adoption of the SCA in 1986, courts have used the Act to protect the privacy of Internet users.[10] This is consistent with Congress's intention to "protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs."[11] From the text of the SCA, it is uncertain whether this protection extends to information on social networks, as Facebook and Myspace claim. Without the SCA, however, there is little to protect users from aggressive litigants and government prosecutors who wish to access their social network information.[12]

This Note explores the challenges related to discovery of online social network information. Part II explores what protections, if any, the SCA provides against discovery of information on online social networks. Part III analyzes the U.S. District Court for the Central District of California's decision in *Crispin v. Christian Audigier, Inc.*,[13] the first case to hold that social networks are protected from disclosing some information by the SCA. Part IV critiques recent decisions that have allowed broad discovery of social network information, arguing that the discovery requests in these cases violated Federal Rule of Civil Procedure 26(b)(1) and that the requested information should have qualified for SCA protection. Part V assumes that litigants will continue requesting social network information through discovery requests and subpoenas, and attempts to determine the proper scope of this discovery by looking at recent cases and the Federal Rules of Civil Procedure. Part VI concludes.

II. THE STORED COMMUNICATIONS ACT

A. SCA Background

The SCA was enacted as Title II of the Electronic Communications Privacy Act ("ECPA").[14] Congress adopted the

[9] *See, e.g.*, *Law Enforcement and Third-Party Matters: May I Obtain Contents of a User's Account from Facebook Using a Civil Subpoena?*, FACEBOOK, http://www.facebook.com/help/?faq=17158 ("[T]he 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.").

[10] *See, e.g.*, William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1196 (2010) ("The resulting task of adapting the Act's language to modern technology has fallen largely upon the courts.").

[11] S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

[12] *See* Nathaniel Gleicher, Comment, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1945 (2009).

[13] 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[14] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

statute, in part, to address privacy concerns created by the rise of new technologies such as the Internet that the Fourth Amendment could not adequately address.[15] In enacting the SCA, Congress hoped to "protect privacy interests in personal and proprietary information" that may be stored on the Internet.[16] It is worth noting that Congress's conception of the Internet in 1986 was quite different from the Internet as it exists today. The World Wide Web had not been developed, and cloud computing services and online social networks would not exist for nearly a decade.[17] Internet users in 1986 could essentially do three things: (1) download and send e-mail; (2) post messages to online bulletin boards; and (3) upload and store information that they could access on other computers.[18] The definitions and prohibitions listed in the SCA align with these three functions as they existed in 1986. Because Congress has not updated the statute, courts have struggled to apply the SCA in light of the explosive growth of the World Wide Web.[19]

B. What Does the SCA Do?

Broadly speaking, the SCA "regulat[es] the relationship between government investigators and [network] service producers in possession of users' private information," limiting the government's ability to compel disclosure of this information from third parties.[20] This Note examines the SCA by looking at two questions: First, which service providers are protected by the SCA? And second, what does the SCA prevent these service providers from doing?

[15] *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, 1210–12 (2004). The Fourth Amendment does not apply to information revealed to third parties or information held by private parties, which would allow many Internet providers to disclose their users' content without violating existing protections.

[16] S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3557.

[17] Tim Berners-Lee invented the World Wide Web in 1989. *See Tim Berners-Lee*, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/People/Berners-Lee/ (last visited May 6, 2011). SixDegrees.com, the first online social network, launched in 1997. *See* danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, J. COMPUTER-MEDIATED COMM., Oct. 2007, *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

[18] *See* S. REP. NO. 99-541, at 8–9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3562–63 (describing "some of the new telecommunications and computer technologies referred to in the [ECPA]").

[19] *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.").

[20] Kerr, *supra* note 15, at 1212; *see also* 18 U.S.C. § 2703 (2006 & Supp. III 2009).

1. Parties Covered by the SCA

The SCA applies to communications stored on the Internet by third-party providers; an individual cannot use the SCA to avoid a court order requiring her to disclose online information herself.[21] The SCA protects communications stored by two different types of online services: electronic communication service ("ECS") providers and remote computing service ("RCS") providers.[22] Each service has different statutory requirements, but it is possible for the same provider to act as an ECS provider for some content and an RCS provider for other content.[23] If a third party is neither an ECS nor an RCS provider, it can disclose any electronic communication it has obtained from electronic storage, even if this information was obtained illegally.[24]

The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[25] Electronic communications include any form of communication "transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system that affects interstate commerce."[26] The statute's definition of ECS providers was intended to cover providers of services, such as e-mail, which required third-party providers to copy and temporarily store electronic communications.[27]

An RCS provider, on the other hand, provides "computer storage or processing services [to the public] by means of an electronic communications system."[28] Although there is debate about the meaning of "processing services,"[29] Orin Kerr claims the statute's definition of RCS providers was intended to cover companies that outsourced computing tasks, which was a common use of third-party network service providers when the SCA was adopted.[30]

[21] *See* 18 U.S.C. § 2703.

[22] *Id.*

[23] *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 986–87 (C.D. Cal. 2010).

[24] *See* Wesley Coll. v. Pitts, 974 F. Supp. 375, 389 (D. Del. 1997) ("[A] person who does not provide an electronic communication service . . . can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage.").

[25] 18 U.S.C. § 2510(15) (2006).

[26] *Id.* § 2510(12). The statute includes four minor exceptions to this definition, which are not relevant to this Note.

[27] *See* Kerr, *supra* note 15, at 1213.

[28] 18 U.S.C. § 2711(2) (2010).

[29] Kerr, *supra* note 15, at 1230. Kerr believes the SCA's "legislative history indicates that 'processing services' refer to outsourcing functions," although he recognizes that a literal reading of the statute could include any provider that "processes information sent to it." *Id.*

[30] *Id.* at 1213–14. According to Kerr, "[t]his 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.

Additionally, the SCA only protects ECS and RCS providers that make their services available "to the public at large, whether for a fee or without cost."[31] If users need a special relationship to get access to a service, the service is nonpublic and can disclose users' electronic communications voluntarily.[32]

2. Protections and Restrictions on ECS and RCS Providers

The SCA generally prevents ECS and RCS providers from disclosing their users' electronic communications to the government or a third party — either voluntarily or under compulsion — without a search warrant.[33] There are some statutory exceptions that allow ECS and RCS providers to disclose information, but these rarely arise in practice.[34] Unless one of these exceptions applies, the government cannot obtain content information from public ECS or RCS providers without a search warrant.[35]

Additionally, the SCA only applies to *content* information contained in electronic communications held by ECS and RCS providers.[36] Content is described as "any information concerning the substance, purport, or meaning of that communication."[37] The content of an e-mail, for example, would include the subject and body text of that e-mail, but would not include any logs or subscriber information related to the sending.[38] In the social networking context, therefore, the SCA would likely not prohibit ECS and RCS providers from disclosing a subscriber's user name or a list of times she logged into the website.

[31] *Id.* at 1226; *see also* 18 U.S.C. § 2702(a) (2006) (restricting only ECS and RCS providers who offer their services "to the public").

[32] Kerr, *supra* note 15, at 1226. Services that are only available to employees or students are examples of nonpublic services. Kerr speculates that the SCA distinguishes between public and nonpublic services for two reasons. First, users expect more privacy on services that are open to the public. Second, as compared to public providers, corporations that provide non-public accounts have less of an incentive to protect users' privacy. Thus, the law forces them to provide this protection. *Id.* at 1226–27.

[33] *See* 18 U.S.C. §§ 2702–03 (2006 & Supp. III 2009). The line between voluntary and compelled disclosure can be difficult to classify, but this responsibility is left to the courts. *See* Kerr, *supra* note 15, at 1225.

[34] *See generally* 18 U.S.C. §§ 2702(b), 2703(d). Information can be voluntarily disclosed, for example, "with the lawful consent of the originator or an addressee or intended recipient." *Id.* § 2702(b)(3).

[35] *See id.* § 2703(a)–(c). *See also* Kerr, *supra* note 15, at 1223. Kerr includes a helpful chart that details the requirements for a party to obtain different types of content from ECS or RCS providers. Civil discovery subpoenas may be insufficient to obtain even basic subscriber information. *See* Fed. Trade Comm'n 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 . . . .").

[36] *See* 18 U.S.C. §§ 2702(b), 2703(a)–(b).

[37] 18 U.S.C. § 2510(8) (2006).

[38] *See* Kerr, *supra* note 15, at 1228.

Finally, the SCA only prohibits ECS and RCS providers from disclosing content information that is held for specific purposes enumerated in the statute. ECS providers, for example, are prevented from knowingly disclosing the contents of an electronic communication "while in electronic storage by that service."[39] Electronic storage is given two definitions in the statute. First, electronic storage is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[40] The statute does not give examples of storage incidental to transmission, although courts have applied this section to prohibit disclosure of communications such as unread e-mails.[41] Second, the statute defines electronic storage as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[42] Neither the text of the statute nor the legislative history indicates Congress's intended meaning of "backup protection."[43] For this reason, courts must supply their own definition of "backup protection" to determine whether an electronic storage is protected under the SCA.[44]

RCS providers, on the other hand, cannot knowingly divulge the contents of any electronic communication "carried or maintained on that service . . . solely for the purpose of providing storage or computer processing services" to any person or entity.[45] Once again, the meaning of "storage or computer processing services" is not defined in the statute or its legislative history.[46] If a court looks at the common understanding of the phrase in 1986, it would likely limit the SCA's coverage to anachronistic number-crunching services that are performed today by modern software.[47] If a court applies a literal reading of the term, it will likely encompass the majority of modern Internet providers since nearly every service offers some storage or processing features.

[39] 18 U.S.C. § 2702(a)(1).

[40] *Id.* § 2510(17)(A).

[41] *See, e.g.*, United States v. Councilman, 418 F.3d 67, 81 (1st Cir. 2005) (en banc) ("The first category, which is relevant here, refers to temporary storage, such as when a message sits in an e-mail user's mailbox after transmission but before the user has retrieved the message from the mail server."); Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) ("Several courts have held that subsection (A) covers e-mail messages stored on an ISP's server pending delivery to the recipient.").

[42] 18 U.S.C. § 2510(17)(B).

[43] Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003).

[44] *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010) (holding that some postings to social networks are stored for backup purposes).

[45] 18 U.S.C. § 2702(a)(2)(B) (2006 & Supp. II 2008). This prohibition does not apply if the RCS provider is "authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." *Id.*

[46] *See* boyd & Ellison, *supra* note 17.

[47] *See* Kerr, *supra* note 15 at 1213–14 (explaining that spreadsheet programs and other basic software can perform basic number-crunching services that the SCA was intended to cover).

This is the framework that courts must use to protect social networks from disclosing their users' communications. If any of these basic requirements is not satisfied, social networks will not be exempt from compulsory disclosure. The next Part examines a recent opinion from the U.S. District Court for the Central District of California that was the first to extend SCA protection to social networks.

III. APPLYING THE SCA TO SOCIAL NETWORKS: *CRISPIN V. CHRISTIAN AUDIGIER, INC.*

A. Case Background

In December 2009, Buckley Crispin filed an action against Christian Audigier and Christian Audigier, Inc. ("CAI"), claiming five causes of action including breach of contract and copyright infringement.[48] Crispin alleged that he granted the defendants an oral license to use fifteen of his copyrighted works.[49] In the course of discovery, the defendants served civil subpoenas on Facebook, Media Temple, Inc., and MySpace, Inc., seeking discovery of "Crispin's basic subscriber information" and various communications made by Crispin.[50]

Crispin attempted to quash the subpoenas by arguing, among other things, that they sought electronic communications that the companies could not disclose under the SCA.[51] Magistrate Judge John E. McDermott rejected this argument, holding that the SCA did not apply for three reasons. First, the SCA only protects ECS providers, and "businesses providing products or services on or through the internet are not ECS providers."[52] Second, the SCA only prohibits voluntary disclosure of electronic communications, not disclosure compelled by subpoena.[53] Third, Judge McDermott held that "the SCA only prohibits an ECS from voluntarily disclosing electronic communications 'while in electronic storage by that service,'" and the communications at issue were "not in 'electronic storage,' as that term is defined by the statute."[54]

Crispin moved for reconsideration on the issue of whether Media Temple, Facebook, and MySpace were protected from disclosure

[48] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 968 (C.D. Cal. 2010).

[49] *Id.* at 968 n.3.

[50] *Id.* at 968–69. The defendants' request included "Crispin's basic subscriber information, as well as all communications between Crispin and tattoo artist Bryan Callan, and all communications that referred or related to Audigier, CAI, the Ed Hardy brand, or any of the sublicensee defendants." *Id.* at 969.

[51] *Id.* at 969.

[52] Order re Plaintiff's Motion to Quash Defendant's Third Party Subpoenas at 7, *Crispin*, 717 F. Supp. 2d 965 (No. 2:09-CV-09509).

[53] *Id.* at 8.

[54] *Id.* (quoting Judge McDermott).

under the SCA.[55] Judge Margaret Morrow of the U.S. District Court for the Central District of California reviewed the Order, reversing Judge McDermott and finding that the three companies were subject to the SCA.

The court found that Judge McDermott fundamentally misunderstood how these services operated by concluding that they "engaged in public messaging only."[56] Judge Morrow recognized that all three services offer a variety of other electronic communication services. Media Temple, for example, provides "webmail," which allows "users to view email messages."[57] Facebook and MySpace also offer "private messaging services" as well as "Facebook wall postings and the MySpace comments [that] are not strictly 'public.'"[58] These differences affect the providers' classifications under the SCA as well as the level of protection they receive.

B. The Court's Analysis

After presenting background on the SCA, Judge Morrow addressed the primary issue of whether the subpoenas should be quashed under the SCA. Recognizing that no court "appears to have addressed whether social-networking sites fall within the ambit of the [SCA],"[59] the court took a two-step approach. First, the court determined whether Media Temple, Facebook, and MySpace qualified as ECS providers under existing case law. Second, the court asked whether the specific content on these services met the definition of "electronic communications." Ultimately, it concluded that the services operate as ECS and RCS providers at different times, depending on the content at issue.[60]

1. Private Messages

Judge Morrow differentiated between read and unread private messages, holding that they are protected in different ways under the SCA. Traditionally, e-mail services have been protected as ECS

[55] *Crispin*, 717 F. Supp. 2d at 970.

[56] *Id.* at 980.

[57] *Id.*

[58] *Id.*

[59] *Id.* at 977.

[60] In a footnote, the *Crispin* court notes that the parties disagree about whether the companies are providers or users of "the ability to send or receive electronic communications." Defendants cited three cases that found that services with the goal of buying and selling books, gold, and travel services were not providers, but rather "merely use[d] the internet to sell goods or services." *Id.* at 982 n.35 (quoting Inventory Locator Serv., LLC v. Partsbase, Inc., No. 02-2695 MA/V, 2005 WL 2179185, at *24 (W.D. Tenn. Sept. 6, 2005)). The court rejected this argument for social networks, noting that the goal of these services is to enable and "provide an electronic venue to communicate." *Id.*

providers because they provided "a conduit for the transmission of electronic communications from one user to another, and stored those communications 'as a "backup" for the user.'"[61] This reasoning applied to e-mail services as they existed throughout the 1980s and 1990s, when users would "download emails from an ISP's server to their own computers" and the ECS provider would retain copies of these e-mails in case the downloaded version was lost or deleted.[62] Like e-mails, private messages on online social networks can only be viewed by the sender and the recipient of the message. Although the private messaging services on Media Temple, Facebook, and MySpace differ from traditional e-mail services in some ways, they both allow users to send messages to individual recipients. As a result, the court found "no basis for distinguishing" between e-mails and private messages on social networks.[63] The court then looked at what information ECS providers could protect from disclosure and concluded that the storage of *unread* private messages was "incidental" to the original transmission within the meaning of the SCA.[64] Media Temple, Facebook, and MySpace were therefore operating as ECS providers for "messages that have not yet been opened," and these private messages were protected by the SCA.[65]

Judge Morrow took a different approach for private messages that have been opened or read, determining that the services were operating as RCS providers for this content.[66] The court relied heavily on *United States v. Weaver*, an Illinois case that applied the SCA to Microsoft's Hotmail e-mail service, finding that it was "web-based" and "remote."[67] Under the SCA, an ECS provider is protected from disclosure if it stores opened messages for "backup purposes" and not for purposes incidental to transmission.[68] The *Weaver* court noted that Hotmail's default setting was for *all* e-mails to be stored on Microsoft's servers and that "Microsoft [was] not storing that user's opened messages for backup purposes."[69] The *Weaver* court therefore held that once an e-mail was read, Hotmail stopped being an ECS provider and "became an RCS provider, providing remote storage

[61] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902 (9th Cir. 2008) (quoting Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004)), *rev'd on other grounds*, City of Ontario, Cal. v. Quon, 130 S.Ct. 2619 (2010).

[62] United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009).

[63] *Crispin*, 717 F. Supp. 2d at 981–82.

[64] *Id.* at 983 ("The Ninth Circuit agrees that 'subsection (A) applies only to messages in "temporary, intermediate storage,"' and has 'limited that subsection's coverage' to messages not yet delivered to their intended recipient." (citing *Theofel*, 359 F.3d at 1075)). *See generally* 18 U.S.C. § 2510(17)(A) (2006).

[65] *Crispin*, 717 F. Supp. 2d at 987.

[66] *Id.* at 985–86.

[67] *See id.* at 985 (citing *Weaver*, 636 F. Supp. 2d at 772).

[68] 18 U.S.C. § 2510(17)(B).

[69] *Crispin*, 717 F. Supp. 2d at 985 (quoting *Weaver*, 636 F. Supp. 2d at 772).

service for the email."[70] Adopting the reasoning of this opinion and dicta from *Theofel v. Farey-Jones*,[71] the *Crispin* court held that once a private message was read, Media Temple, Facebook, and MySpace operated "as RCS providers providing storage services under § 2702(a)(2)."[72] Judge Morrow noted that this shifting system was consistent with Ninth Circuit precedent,[73] case law in other jurisdictions,[74] and legal scholarship.[75]

Although services like Facebook and MySpace fit the definition of RCS providers for private messages that have been opened or read, these messages might have also been protected from disclosure if the court had considered Facebook and MySpace to be ECS providers.[76] The Crispin court may have avoided this route because of dicta in *Theofel v. Farey-Jones*, noting that "[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."[77] Other courts are free to ignore this reasoning and could instead adopt a commonsense definition of "backup purposes" that would include cloud-based private messaging systems.

2. Wall Posts, Comments, etc.

Next, the court considered whether Facebook Wall posts or MySpace Comments are protected under the SCA by analogizing to private electronic bulletin board services ("BBS").[78] The legislative

[70] *Id.*

[71] Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

[72] *Crispin*, 717 F. Supp. 2d at 987.

[73] *See Theofel*, 359 F.3d at 1076 (noting that "remote computing services and electronic communications services are 'often the same entities'").

[74] *See* Flagg v. City of Detroit, 252 F.R.D. 346, 362–63 (E.D. Mich. 2008).

[75] *See, e.g.*, Kerr, *supra* note 15, at 1216 ("If Jane chooses to store the e-mail with the ISP, the ISP now acts as a provider of RCS (and not ECS) with respect to that copy of the e-mail so long as the ISP is available to the public.").

[76] *See* Matthew A. Goldberg, Comment, *The Googling of Online Privacy: Gmail, Search-Engine Histories and the New Frontier of Protecting Private Information on the Web*, 9 LEWIS & CLARK L. REV. 249, 268 (2005) (noting that web-based e-mail providers seem to qualify as ECS providers).

[77] *Theofel*, 359 F.3d at 1077. It is unclear whether *Theofel* is still controlling after *Quon v. Arch Wireless Operating Co., Inc.*, which held that messages which were archived by an ECS provider were not "permanent storage" and therefore met the definition of "backup protection" under 18 U.S.C. § 2510(17)(B). *See Crispin*, 717 F. Supp. 2d at 984 (citing Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 902–03 (9th Cir. 2008), *rev'd on other grounds*, City of Ontario, Cal. v. Quon, 130 S.Ct. 2619 (2010)). This is especially true for services (like Facebook) that allow users to download their content, including private messages. *See* Paul Boutin, *Facebook Now Lets You Take Your Data With You*, GADGETWISE (Oct. 6, 2010, 6:19 PM), http://gadgetwise.blogs.nytimes.com/2010/10/06/facebook-now-lets-you-take-your-data-with-you.

[78] *See Crispin*, 717 F. Supp. 2d at 985. Although the court focused on Facebook Wall posts and Myspace Comments, the same logic could be applied to all non-private content on social networks, including uploaded photographs and status updates.

history of the SCA suggests that Congress expected private BBS to be protected from disclosure, and the text of the statute is not inconsistent with this goal.[79] It is unclear, however, whether Facebook and MySpace are operating as ECS or RCS providers for this content. The court did not resolve this issue, holding that the social networks qualify for protection either way.[80]

Judge Morrow first explains that "Facebook and MySpace are ECS providers as respects wall postings and comments and that such communications are in electronic storage."[81] At least two cases, including the Ninth Circuit's decision in *Konop v. Hawaiian Airlines, Inc.*, have held that a private BBS qualifies as an ECS provider under the SCA.[82] In *Konop*, the Ninth Circuit considered an invitation-only BBS located on a secure website to be an ECS provider and held, without detail, that the communications on the BBS were in electronic storage.[83] The *Crispin* court analogized to this case, declaring that a BBS post was "in all material ways analogous to a Facebook wall posting or a MySpace comment"[84] and that "there is no basis for distinguishing between a restricted-access BBS and a user's Facebook wall or MySpace comments."[85]

Regarding Facebook Wall posts and MySpace Comments, the court did not distinguish between read and unread content, adopting the reasoning of an earlier BBS case that recognized there is no intermediate storage for this kind of content because the "website is the final destination for the information."[86] In order for these posts to be in electronic storage, therefore, the *Konop* court must have concluded that they were stored for "backup purposes."[87]

Judge Morrow seemed to recognize the unusual nature of this claim, which requires adopting a broad definition of "backup purposes." The court explained that this is consistent with Ninth Circuit precedent, which has "implicitly held that although a user may have other purposes for . . . leaving a post on his or her Facebook

[79] *See* 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 . . . .").

[80] *Crispin*, 717 F. Supp. 2d at 989–90.

[81] *Id.* at 989.

[82] *See* 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."); Kaufman v. Nest Seekers, LLC, No. 05 CV 6782(GBD), 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006) ("An electronic bulletin board fits within the definition of an electronic communication service provider.").

[83] *Konop*, 302 F.3d at 879.

[84] *Crispin*, 717 F. Supp. 2d at 989.

[85] *Id.* at 981.

[86] *Id.* at 988 (quoting Snow v. DIRECTV, Inc., No. 2:04-CV-515FTM33SPC, 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005)).

[87] *See* 18 U.S.C. § 2510(17)(B) (2006).

wall, rather than . . . deleting the Facebook wall posting after the information has become stale, one of the multiple purposes may be for backup storage."[88] This interpretation is consistent with the text of the statute and is likely "more coherent and more consistent with Congressional intent" than categorizing Facebook Wall posts and MySpace Comments as intermediate storage, which is unprotected by the SCA.[89]

Next, the *Crispin* court held that Facebook and MySpace were also protected as RCS providers with respect to Wall posts and Comments.[90] The court analogized to *Viacom International Inc. v. YouTube Inc.*, which held that YouTube is an RCS provider "because their authorization to access and delete potentially infringing private videos is granted in connection with defendants' provision of alleged storage services."[91] Similarly, Facebook and MySpace store a wide range of content for their users, from pictures and videos to Wall posts and Comments.[92] The court rejected the defendants' claim that Facebook and MySpace could not be RCS providers because some communications were maintained for display purposes and not "'solely' for the purpose of storage" as used in section 2702(a)(2)(B).[93] Judge Morrow held that "a storage service necessarily requires a retrieval mechanism to be useful," and noted that the defendants' argument was inconsistent with the *YouTube* decision.[94]

Regardless of whether Facebook and MySpace are ECS or RCS providers, the *Crispin* court cautioned that "a completely public BBS does not merit protection under the SCA."[95] In order to be protected from disclosure, therefore, Facebook Wall posts and MySpace Comments must not be "completely public." Judge Morrow distinguished Facebook and MySpace from "completely public" BBS by noting that the users of both websites can limit public access via privacy settings.[96] Nevertheless, it was unclear whether Crispin had

[88] *Crispin*, 717 F. Supp. 2d at 989 n.50.

[89] *Id.* (quoting Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 887 (9th Cir. 2002) (Reinhardt, J., concurring) (noting that Congress intended that read e-mail messages be protected as backup copies)).

[90] *Id.* at 990.

[91] Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 n.8 (S.D.N.Y. 2008).

[92] *Crispin*, 717 F. Supp. 2d at 990.

[93] *Id.*

[94] *Id.*

[95] *See id.* at 981 (citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002)).

[96] *See id.* YouTube users can mark their videos as private so they "can only be viewed by others authorized by the user who posted . . . them." *YouTube*, 253 F.R.D. at 264. Facebook users can restrict their profiles, thereby controlling what kind of information is made available to different Facebook Friends and the public at large. *See Facebook's Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last updated Dec. 22, 2010).

employed these privacy settings, so the court vacated and remanded to Judge McDermott to determine "plaintiff's privacy settings and the extent of access allowed to his Facebook wall and MySpace comments."[97]

C. Result

The *Crispin* court properly followed Ninth Circuit precedent and furthered the SCA's stated purpose by protecting the privacy of social network users. Judge Morrow recognized that social networks are both ECS and RCS providers, and that determining "which protections apply is a [sic] governed by the type of storage involved."[98] The court was wise to carefully deconstruct the different types of content on social networks and explain how that content satisfied the statute's requirements for ECS or RCS providers.

Assuming other courts follow the approach laid out in *Crispin*, there are still many open questions about the SCA's applicability to social network content that is not inherently private. Most obviously, the *Crispin* court fails to give any real guidance on the precise requirements for SCA protection of Wall posts and other non-private message content. Must content be limited to a certain number of friends? Does content still fall under the SCA if your friends' friends can view it? For a proposed solution to this question, see *infra* Part V.

IV. CASES THAT HAVE IGNORED THE SCA

Although *Crispin* was the first case to hold that the SCA protects some social network information from subpoenas, other cases have addressed discovery of social network information more broadly. Most of these cases have concluded that social network information is admissible so long as it is relevant to the case, thus forcing parties to turn over access to users' social networks. In addition to allowing overbroad discovery requests, these cases fail to explain why the SCA does not protect at least some of the information contained in the discovery request.

A. Ledbetter v. Wal-Mart Stores, Inc.

In *Ledbetter v. Wal-Mart Stores, Inc.*, plaintiffs and repairmen Joel Ledbetter and Heath Powell alleged that they "suffered permanent physical and psychological injuries" resulting from an

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

[98] *Id.* at 987.

electrical accident at a Wal-Mart located in Aurora, Colorado.[99] Heath Powell's wife, Disa Powell, also brought a claim for loss of right of consortium.[100] Wal-Mart issued subpoenas to Facebook, MySpace, and Meetup.com for "[a]ny and all internet usage activity" related to the plaintiffs' accounts.[101] The Facebook subpoenas requested "private messages for user account, private blog entries of user account, and ip log [sic] of user account."[102] Similarly, subpoenas issued to MySpace and Meetup.com asked for "IP logs, date profile was created; email address of user; friend requests; private messages; private blog entries; photographs; bulletins; and any additional information."[103] The plaintiffs responded by arguing that the subpoenas were "overly broad and amount[ed] to a fishing expedition,"[104] and asked the court to grant a protective order that would require production of all responsive documents "directly to the Court for an *in camera* review."[105] In a brief order, the court denied this request and found that the subpoenas were "reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues in this case."[106]

There are two problems with the *Ledbetter* court's holding. First, the court did not consider whether the SCA prevented the social networks from disclosing the plaintiff's content.[107] Because the subpoenas specifically requested private messages, private blog entries, and other information that was not accessible by the general public, the court's failure to address the SCA was an error. Indeed, all three social networks later refused to comply with Wal-Mart's subpoena, claiming the SCA prevented them from complying with the court order.[108] Second, the court granted the defendant's subpoena

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

[100] *Id.*

[101] Plaintiffs' Motion for Protective Order Pursuant to Fed. R. Civ. P. 26(c) Regarding Subpoenas Issued to Facebook, My Space, Inc. and Meetup.com at 5, *Ledbetter*, 2009 WL 1067018 (No. 01-958).

[102] *Id.* An "IP log" stores data on requests made from an IP address. If the social network maintains an IP log, "[i]t is . . . possible to track and correlate all the web searches originating from a single IP address." Article 29 Data Protection Working Group, *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, 6, 00737/EN WP 148 (April 4, 2008).

[103] Plaintiffs' Motion for Protective Order Pursuant to Fed. R. Civ. P. 26(c) Regarding Subpoenas Issued to Facebook, My Space, Inc. and Meetup.com, *supra* note 101, at 5–6.

[104] *Id.* at 8.

[105] *Id.* at 12.

[106] *Ledbetter*, 2009 WL 1067018, at *2.

[107] Because the plaintiffs did not raise the SCA as a defense to the defendant's subpoena, the court would have had to raise the issue *sui sponte*. *See generally* Plaintiffs' Motion for Protective Order Pursuant to Fed. R. Civ. P. 26(c) Regarding Subpoenas Issued to Facebook, My Space, Inc. and Meetup.com, *supra* note 101.

[108] Defendant Wal-Mart Stores, Inc.'s Motion to Compel Production of Content of Social Networking Sites at ¶ 8, *Ledbetter*, 2009 WL 1067018 (No. 106CV01958), 2009 WL 3061763.

despite the fact that it sought *all* information on the plaintiffs' social network accounts, regardless of whether it was related to the injuries at issue in the lawsuit.[109] Such broad discovery violates the Federal Rules of Civil Procedure, which require that the discovery be "relevant to any party's claim or defense" or "reasonably calculated to lead to the discovery of admissible evidence."[110]

B. Romano v. Steelcase Inc.

Similarly, in *Romano v. Steelcase Inc.*,[111] the plaintiff claimed she suffered permanent injuries when she fell from a defective chair manufactured by the defendant.[112] The defendant believed that the plaintiff's social network accounts contained photographs that were inconsistent with these claims and sought a court order granting "access to Plaintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information."[113] Judge Spinner began his opinion by briefly noting that he had reviewed the applicable federal law, including the SCA.[114] This was the only time the court mentioned the SCA and Judge Spinner never explained why it did not apply to the requested information. Instead, the court's opinion focused on whether the defendant's request fell within the scope of permissible discovery under New York evidence law and whether production of these documents would violate the plaintiff's right to privacy.

Judge Spinner first analyzed the state's liberal discovery standard, which requires disclosure of information that is "material and necessary to the defense or prosecution of an action"[115] or "may lead to the disclosure of admissible proof."[116] The information requested from the plaintiff's Facebook and MySpace pages satisfied both of these standards. First, the information was "material and necessary to the defense of this action" because the plaintiff's public Facebook

[109] *See* Plaintiffs' Motion for Protective Order Pursuant to Fed. R. Civ. P. 26(c) Regarding Subpoenas Issued to Facebook, MySpace, Inc. and Meetup.com, *supra* note 101, at 5.

[110] FED. R. CIV. P. 26(b)(1).

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

[112] *See* Brian Grow, *In U.S. Courts, Facebook Posts Become Less Private*, REUTERS (Jan. 27, 2011, 2:40 PM), http://www.reuters.com/article/2011/01/27/us-facebook-privacy-idUSTRE70Q7EG20110127.

[113] *Romano*, 907 N.Y.S.2d at 657.

[114] *Id.* at 651–52.

[115] *Id.* at 652. New York trial courts are given broad discretion to decide whether requested information is "material or necessary." *Id.*

[116] *Id.* (quoting Twenty Four Hour Fuel Oil Corp. v. Hunter Ambulance Inc., 640 N.Y.S.2d 114, 114 (App. Div. 1996)). Requested information need not be directly admissible at trial to be discoverable. *Id.* This is similar to the federal rule. *Cf.* FED R. CIV. P. 26(b)(1) ("Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.").

picture showed her smiling happily outside of her home, contradicting her claim that she was "largely confined to her house and bed."[117] Second, and most importantly, the plaintiff's profile picture led the court to conclude "there [was] a reasonable likelihood that the private portions of her site may contain further evidence . . . with regard to her activities and enjoyment of life" that would be admissible in court.[118] The court recognized that "there is no New York case law directly addressing [discovery of social network information]," but referenced *Ledbetter* and five Canadian cases that allowed broad discovery of social network pages by defendants in personal injury lawsuits.[119] Reasoning from these cases, Judge Spinner held that denying the defendant's requested court order "would go against the liberal discovery policies of New York favoring pre-trial disclosure . . . [and] condone Plaintiff's attempt to hide relevant information behind self-regulated privacy settings."[120]

Next, the court considered whether the plaintiff had an expectation of privacy in her Facebook and MySpace pages. Although no court had addressed this issue in New York, the court mentioned a Second Circuit case that found no expectation of privacy for "transmissions over the Internet or e-mail that have already arrived at the recipient."[121] Additionally, Judge Spinner cited three cases that found no expectation of privacy for MySpace writings that were "shared with others."[122] The court did not rely on the reasoning of these cases. Instead, Judge Spinner held that the plaintiff had no reasonable expectation of privacy on her social networks because "neither Facebook nor MySpace guarantee complete privacy."[123] The court looked to the privacy policies of both companies, which warn users that their information may become publicly available.[124] Because of this warning, Judge Spinner held that "when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings."[125]

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

[118] *Id.*

[119] *Id.* at 654–55.

[120] *Id.* at 655.

[121] United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (cited in *Romano*, 907 N.Y.S.2d at 656).

[122] *Romano*, 907 N.Y.S.2d at 656 (citing Order Denying 65 Motion for Reconsideration, Beye v. Horizon Blue Cross Blue Shield of N.J., 568 F. Supp. 2d 556, (D.N.J. Dec. 14, 2007) (No. 06-5337)); Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125, 1130 (2009); Dexter v. Dexter, No. 2006-P-0051, 2007 WL 1532084, at *6 n.4 (Ohio Ct. App. May 25, 2007)).

[123] *Id.*

[124] *Id.* at 656–57.

[125] *Id.* at 657.

Romano has received a great deal of attention and criticism in the months since it was issued.[126] This Note argues that Judge Spinner's decision was incorrect for three reasons. First, the court's order granted the defendant overly broad access to the plaintiff's social network accounts. Instead, discovery should have been narrowly tailored to information related to the case. Not *everything* on the plaintiff's Facebook and MySpace pages was relevant to the lawsuit.[127] It is likely that the majority of information on her social network pages had no relevance to "the issue of damages and the extent of [her] injury."[128] For example, the majority of the plaintiff's daily correspondences with friends and family would be unlikely to discuss the details of her injury, but may reveal personal information that is both embarrassing and unrelated to the claims at issue. By granting the defendant such broad discovery without court oversight, Judge Spinner pushes the discovery rules to their breaking point by allowing the defendant to engage in a fishing expedition for information about the plaintiff.[129]

Second, the court never discusses the SCA or the recent *Crispin* decision, despite recognizing that the SCA prevents social networks from disclosing at least some information.[130] Instead, Judge Spinner cites five Canadian cases that did not apply American law and one District of Colorado case that also overlooked the SCA.[131] Because the court order required Facebook and MySpace to produce non-public information from the plaintiff's account, including deleted pages, it was an error for Judge Spinner to ignore the SCA.

Third, the court's conclusion that users have no reasonable expectation of privacy for content they upload to social networks is predicated on faulty reasoning. The court relies heavily on Facebook's

[126] *See, e.g.*, Kashmir Hill, *Do Your Social Networking Privacy Settings Matter If You Get Sued?*, THE NOT-SO PRIVATE PARTS (Sept. 27, 2010, 4:01 PM), http://blogs.forbes.com/kashmirhill/2010/09/27/do-your-social-networking-privacy-settings-matter-if-you-get-sued (contrasting the opinion with the *Crispin* court's holding); Venkat, Comment to *Deleted Facebook and MySpace Posts Are Discoverable — Romano v. Steelcase*, TECH. & MARKETING L. BLOG (Sept. 29, 2010, 8:46 PM), http://blog.ericgoldman.org/archives/2010/09/deleted_faceboo.htm (criticizing the court's privacy holding); Robin Wilton, *Do You Know Jeffrey Arlen Spinner?*, GARTNER (Oct. 1, 2010), http://blogs.gartner.com/robin-wilton/2010/10/01/do-you-know-jeffrey-arlen-spinner (same).

[127] *See* FED. R. CIV. PROC. 26(b)(1) ("[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense").

[128] *Romano*, 907 N.Y.S.2d at 652.

[129] If a single photograph allows defendant to access an entire social network account because it "may lead to the disclosure of admissible proof," *id.* (quoting Twenty Four Hour Fuel Oil Corp. v. Hunter Ambulance Inc., 640 N.Y.S. 2d 114, 114 (App. Div. 1996)), there is seemingly no limit to what may be discovered.

[130] *Id.* at 651–52 ("The Court has reviewed . . . the Stored Communications Act, which prohibits an entity, such as Facebook and MySpace from disclosing such information without the consent of the owner of the account.").

[131] *Id.* at 654–55.

claim that "if you disclose personal information in your profile . . . this information may become publicly available."[132] This language is simply a warning that Facebook cannot guarantee that third parties will not illegally access users' accounts, not a concession that users have no reasonable expectation of privacy.[133] By reasoning that the mere possibility of information becoming publicly available removes any reasonable expectation of privacy, Judge Spinner reads the word "reasonable" out of the legal standard for privacy. The court seems to say that if there is any chance of information becoming public, no matter how this information might be obtained, there can be no expectation of privacy. This reasoning is dangerous. For example, in the physical world, it is generally understood that houses are not entirely secure. Regardless of security measures, it is possible for burglars to break into homes, steal information, and then make that information publicly available. According to Judge Spinner's reasoning, people should not be able to claim a reasonable expectation of privacy within their homes. Surely this is wrong.[134] Privacy measures, including privacy settings, create a reasonable expectation that at least some social network information will not be publicly available. This claim is consistent with the cases cited by Judge Spinner, which only held that there is no reasonable expectation of privacy for MySpace writings that were made available to the public by the user.[135]

V. The Proper Approach to Social Network Discovery

The cases above demonstrate that courts have not adopted a uniform approach to discovery requests for social network

[132] *Id.* at 656 (quoting Facebook Privacy Policy (effective Nov. 26, 2008) (replaced by Dec. 22, 2010 Privacy Policy)).

[133] The current language in Facebook's Privacy Policy further clarifies this intent, which reads:

> We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up to date antivirus software.

Facebook's Privacy Policy, *supra* note 96.

[134] Silverman v. United States, 365 U.S. 505, 511 (1961) (a core protection of the Fourth Amendment is "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion").

[135] *See* Order, Beye v. Horizon Blue Cross Blue Shield of N.J., 568 F. Supp. 2d 556, (D.N.J. Dec. 14, 2007) (No. 06-5337)) (excluding MySpace writings that were not shared with others); Moreno v. Hanford Sentinel Inc., 172 Cal. App. 4th 1125, 1130 (2009) (no expectation of privacy for MySpace writings available to the public); Dexter v. Dexter, No. 2006-P-0051, 2007 WL 1532084, at *6 n.4 (Ohio Ct. App. May 25, 2007) (same). None of the cases cited involved writings that were only viewable by a limited number of users.

information. Because social network discovery is poised to become a common occurrence in civil cases, it is important to ask what the proper scope of this discovery should be.[136] This Note advocates a two-step approach: (1) apply the rules of civil procedure; and (2) apply the SCA.[137]

In step one, when a court is confronted with a subpoena or court order requesting social network information, it should ask whether the request is both narrowly tailored to produce relevant information and "reasonably calculated to lead to the discovery of admissible evidence."[138] Unless both requirements are met, the court should prevent discovery either by quashing the subpoena or denying the court order.

If both requirements of step one are met, then, in step two, the court should determine whether the SCA protects the requested information from disclosure. Most courts seem to reverse these steps, addressing a party's SCA arguments before determining whether the request is overbroad or unlikely to produce admissible evidence.[139]

A. Step One: Apply the Rules of Civil Procedure

Courts should begin with issues of overbreadth and admissibility because SCA protection is irrelevant when the request violates federal or state rules governing discovery. The Federal Rules of Civil Procedure limit what evidence is discoverable by requiring that information be narrowly tailored to produce information relevant to the claims at issue in the case and "reasonably calculated to lead to the discovery of admissible evidence."[140] Just like any other kind of evidence, a discovery request for information on a social network page should be rejected as overly broad if it is unlimited in scope, or not related to an alleged injury or claim for recovery. The relevant inquiry is whether the discovery request is so broad that it amounts to

[136] This is especially true for personal injury cases. *See* Andrew S. Kaufman, *Social Networks in Personal Injury Litigation*, NEW YORK L.J. (Dec. 17, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202476307983 ("Social network profiles are a fertile source of information concerning a litigant's physical and emotional condition and recent activities.").

[137] While this framework is written with federal courts in mind, state courts can apply the same two steps by adjusting the admissibility inquiry to capture any differences in the state's evidentiary rules.

[138] FED R. CIV. P. 26(b)(1).

[139] *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 969–70 (C.D. Cal. 2010) (describing the magistrate judge's order, which dismissed plaintiff's SCA claims before addressing "overbreadth and privacy arguments"); Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (Sup. Ct. 2010) (acknowledging and then ignoring plaintiff's SCA defense before analyzing the materiality and necessity of defendant's request).

[140] FED. R. CIV. P. 26(b)(1).

a fishing expedition.[141] It would be exceedingly rare for discovery requesting all content on a social network profile to be narrowly tailored to produce relevant information when the vast majority of content on a litigant's social network site likely has nothing to do with a material issue in the case.[142] Courts should be especially mindful of this concern when the requesting party has other pending or potential lawsuits in which the requested information could be used for harassment or to prolong litigation of frivolous claims.

Two recent cases illustrate how the overbreadth inquiry should be applied. First, in *Crispin v. Christian Audigier, Inc.*, detailed in Part III, the defendants served subpoenas on Facebook and MySpace.[143] The subpoenas sought "All COMMUNICATIONS by and between CRISPIN . . . and BRYAN CALLAN," a non-party who filed a separate lawsuit against the plaintiff.[144] Magistrate Judge McDermott quashed these requests as overbroad because the defendants' complaint "does not mention Callan, and Callan's own artwork and lawsuit are unrelated to Crispin's lawsuit."[145] The court ruled that subpoena requests must be limited to communications related to defendants and their sublicensees.[146] Additionally, the court cautioned against allowing the defendants to use this lawsuit "to obtain discovery for use in Callan's suit."[147]

Second, similar issues arose in *McCann v. Harleysville Insurance Co. of New York*, a personal injury case in New York state court.[148] In that case, the defendant appealed two discovery motions that were denied by the trial court. First, the defendant sought to compel disclosure of photographs on the plaintiff's Facebook account and requested authorization to access all content on the plaintiff's Facebook account.[149] The appellate court affirmed the lower court's denial of this motion, concluding without explanation that it was overly broad.[150] Second, the defendant filed a subsequent motion that

[141] *See, e.g.*, Groom v. Standard Ins. Co., 492 F. Supp. 2d 1202, 1205 (C.D. Cal. 2007) ("discovery must be narrowly tailored and cannot be a fishing expedition").

[142] This is certainly true for the Federal Rules of Civil Procedure. THOMAS R. VAN DERVORT, AMERICAN LAW AND THE LEGAL SYSTEM: EQUAL JUSTICE UNDER THE LAW 136 (2d ed. 2000). State rules are often analogous to the federal rules but must be analyzed on a case-by-case basis

[143] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 968–69 (C.D. Cal. 2010).

[144] *See* Joint Stipulation re: Notice of Motion and Motion to Quash Defendant's Subpoenas, or in the Alternative, for a Protective Order; Declaration of Regina Y. Yeh Esq. in support thereof at 13, *Crispin,* 717 F. Supp. 2d 965 (No. 2:09-CV-09509).

[145] Order re Plaintiff's Motion to Quash Defendant's Third Party Subpoenas, *supra* note 52, at 10.

[146] *Id.*

[147] *Id.*

[148] McCann v. Harleysville Ins. Co. of N.Y., 910 N.Y.S.2d 614 (App. Div. 2010).

[149] *Id.* at 615.

[150] *See id.*

specified the type of evidence sought.[151] The appellate court also rejected this motion because the defendant failed to establish why the evidence was relevant to any of its claims.[152] The court held that the defendant's request for access to the plaintiff's Facebook account was nothing more than a "fishing expedition" in "hope of finding relevant evidence."[153]

Discovery requests that are overly broad or do not relate to one of the claims or defenses should be denied with leave to amend. If the request satisfies the relevant rules of civil procedure, courts must then determine whether the discovery request is invalid under the SCA.

B. Step Two: Apply the SCA

The *Crispin* decision offers valuable insight regarding the SCA's application, and future courts should look to its holdings for guidance. First, courts should determine whether a discovery request requires a social network to produce content from a party's account. If the discovery request does not require any action by a third party social network, the SCA does not apply.[154]

Second, courts should identify the different types of content being requested. Social network information can be separated into two categories: private messages and content that is generally visible to other people on the social network. Private messages include any communications sent to specific individuals through the social network platform that can only be viewed by those recipients. It does not matter if these communications are addressed to more than one party. On Facebook, for example, private messages include Messages and Chat. Generally-visible content is information a user posts to a social network that other users can view, even if they were not the intended audience. The *Crispin* court only considered Facebook Wall posts and MySpace Comments under this category, but this category is much broader. Generally-visible content on Facebook might also include profile information, status updates, photographs, Notes, Questions, Groups, and more.

Under the SCA, information that is "readily accessible to the general public" is not protected from disclosure.[155] Private messages

[151] *Id.*

[152] *See id.*

[153] *Id.*

[154] *See* 18 U.S.C. § 2703 (2006 & Supp. III 2009); *see generally* FED. R. CIV. P. 34 (governing discovery requests on any other party in federal cases). To obtain complete and accurate social network records, it may be necessary to request this information directly from the social network. *See* Stephenson, *supra* note 5 (noting that it is unlikely that "individuals have the technological capacity to do more than provide a paper printout from the [social network] site").

[155] *See* 18 U.S.C. § 2511(2)(g) (2006 & Supp. II 2008). The term "readily accessible to the general public" is only defined in relation to radio communication, 18 U.S.C. § 2510(16)

are, by definition, unavailable to the public and will generally be protected.[156] It is unclear when generally visible content is "readily accessible to the general public" under the SCA.[157] Should something be public when thousands of people can see it, even if these people are your social network friends? Courts should, if possible, avoid drawing arbitrary lines related to the number of people who can view something, which would result in both under-inclusive and over-inclusive application of the SCA.[158] This Note advocates a narrow definition of "readily accessible to the general public" that is limited to information that is viewable by anyone who creates an account on the social network. This definition is consistent with a literal reading of "public" to mean "accessible to or shared by all members of the community."[159] Under this framework, Facebook content that is visible to "Everyone" is public; content set to any other setting ("Friends of Friends," "Friends Only," or "Other") is private.[160] In the context of Twitter, unprotected Tweets would be "public," but protected Tweets would not be.[161] This approach is also consistent

(2006), but the *Crispin* court applied it to social networks by analogizing to BBSes. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 981–82 (C.D. Cal. 2010). If the requested content is accessible to the general public, lawyers can obtain this information either by serving a subpoena on the social network or simply obtaining the information directly. It is possible that social networks could refuse to comply with subpoenas in these cases, arguing that producing information that is publicly available on their website is an undue burden. *See* FED. R. CIV. P. 26(b)(2)(C)(i) ("[T]he court must limit the frequency or extent of discovery otherwise allowed by these rules . . . if it determines that . . . the discovery sought . . . can be obtained from some other source that is more convenient, less burdensome, or less expensive . . . ."). At the time of publication, no court had ever addressed this defense.

[156] Of course, the social network must still meet the other requirements of the SCA. For instance, they must either be RCS or ECS providers.

[157] In *Crispin*, Judge Morrow remanded this issue to the magistrate court. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

[158] The *Crispin* court recognized the problem of over-inclusion, arguing that "basing a rule on the number of users who can access information would result in arbitrary line-drawing and likely in the anomalous result that businesses such as law firms, which may have thousands of employees who can access documents in storage, would be excluded from the statute." *Id.* at 990.

[159] MERRIAM WEBSTER ONLINE, http://www.m-w.com (last visited May 6, 2011) (defining "public").

[160] The default privacy setting for most Facebook information, including your "name, profile picture, and connections" is "everyone." *Facebook's Privacy Policy*, *supra* note 96. This information is publicly available and can "be accessed by everyone on the Internet (including people not logged into Facebook), be indexed by third party search engines, and be imported, exported, distributed, and redistributed by us and others without privacy limitations." *Id.* It is worth noting that content available to everyone in a "Facebook network" is considered private under this framework unless that information is also available to all Facebook users.

[161] Protected Tweets are only viewable by your Twitter contacts. Additionally, these Tweets cannot be shared using "Retweet," a feature that allows users to share Tweets created by other Twitter users. *See Why Can't I Retweet Certain Tweets?*, TWITTER HELP CENTER, http://support.twitter.com/entries/91886-why-can-t-i-retweet-certain-tweets (last visited May 6, 2011).

with the rationale for adopting the SCA,[162] and the reasonable expectation of privacy that comes from using privacy settings on a social network site.[163]

Finally, courts should determine whether the content is protected as ECS or RCS. Because social networks qualify as both ECS and RCS providers, courts should look at the way content is stored to determine the proper protection. While the *Crispin* court's analysis is helpful, courts must be sure to focus on the underlying rationale for the SCA and not adopt limited definitions of key terms left undefined in the text or legislative history, including "backup protection" and "processing services." If other courts adopt a strict definition of these terms, the SCA will be limited to the three Internet functions that existed in 1986.[164] This would allow the government to access billions of electronic communications held on social networks through the use of a standard civil subpoena, violently disrupting Congress's intended "fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies" established in the SCA.[165] If courts cannot use the SCA "to balance the interests of users, law enforcement, and private industry, communications will be subjected to a tug-of-war between the private companies that transmit them and the government agencies that seek to access them. . . . [and] Internet users will find themselves with little protection."[166]

With that in mind, courts should follow the reasoning in *Crispin* and find that social networks are acting as ECS providers for unread private messages on their systems.[167] Similarly, these social networks should be protected from disclosing private messages that have been opened, because they store these messages as RCS providers.[168] It is less clear how courts should protect generally-visible content. Although *Crispin* holds that social networks can be protected as either ECS or RCS providers for such content, this Note suggests that it is more textually accurate to say that they are acting as ECS providers.[169] Judge Morrow relied on *YouTube* in holding that generally-visible content was protected as RCS because the phrase "solely for the purposes of storage," as used in the SCA, included

[162] S. REP. NO. 99-541, at 35 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3589 ("This provision addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public.").

[163] *See supra* Part IV.

[164] *See supra* Part II.A.

[165] S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3359.

[166] Gleicher, *supra* note 12, at 1945.

[167] *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 979–80 (C.D. Cal. 2010).

[168] Courts should not limit RCS protections to services that existed in 1986, which did not include backup storage. *See supra* note 47 and accompanying text.

[169] *See Crispin*, 717 F. Supp. 2d at 989–90.

both storage and display functions.[170] In so holding, the *Crispin* court departed from the clear text of the SCA to achieve a sensible result. This result is unnecessary, however, because generally-visible content can be protected as ECS by broadly defining a key term in the statute, "backup protection," to be consistent with congressional intent. Protecting social networks as ECS providers is also easier for judges because it allows them to interpret the text of the SCA and does not require a technical understanding of whether display functions are inherent in storage functions.

As mentioned previously, electronic communications are protected when an ECS provider stores them for "backup protection."[171] Unlike RCS providers, ECS providers do not have to store the communications "solely" for these purposes.[172] Courts should avoid adopting a narrow definition of this term that requires two copies of a communication for one of them to serve as a "backup." Instead, because one of the purposes for leaving generally-visible content on a social network, rather than deleting it, may be to store that content for backup protection,[173] courts should protect social networks as ECS providers for generally-visible content that is not publicly available.

It is worth noting that this protective approach, which will prevent social networks from disclosing large amounts of user content, does not completely bar access to information on social networks. Parties can ask courts to issue a search warrant, which trumps the SCA and requires social networks to comply with a discovery request.[174] Additionally, parties can request that courts compel a user to give her lawful consent for disclosure.[175] Once this consent is received, social networks are free to voluntarily disclose the information. Although courts have increasingly used this approach, it raises questions about whether courts are using compelled consent as a way to avoid the strict disclosure requirements established by Congress in the SCA.[176]

[170] *See id.* at 990.

[171] 18 U.S.C. § 2510(17)(B) (2006).

[172] *Compare id. with* 18 U.S.C. § 2702(a)(2)(B) (2006 & Supp. II 2008).

[173] *See Crispin*, 717 F. Supp. 2d at 989 n.50.

[174] *See* 18 U.S.C. § 2703(a)–(b) (2006 & Supp. III 2009).

[175] *See id.* §§ 2702(b)(3), (c)(2).

[176] *See, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 657 (Sup. Ct. 2010) (requiring plaintiff to deliver "a properly executed consent and authorization" to Facebook and MySpace); Minute Order, Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009) (No. 01-958, 2009) (compelling plaintiff to execute consents); *see also* O'Grady v. Superior Court of Santa Clara Cnty., 139 Cal. App. 4th 1423, 1446 (2006) (recognizing that "[w]here a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions").

VI. CONCLUSION

The Stored Communications Act is an unnecessarily complicated statute.[177] Originally designed to protect the privacy of Internet users as the Internet existed in 1986, courts have been made to "extract[] operating principles from [the SCA's] tangled legal framework" and apply these to new Internet technologies.[178] Social networks present one of the latest challenges in this regard. Courts have taken inconsistent approaches in applying the SCA to social network information and many of these cases have obvious flaws. Even the *Crispin* decision, which represents a step in the right direction, provides incomplete guidance in determining whether social networks should be protected from disclosing certain content under the SCA. This Note attempts to fill this void by presenting a simplified two-step approach for dealing with discovery requests that require social networks to disclose their users' information. This is far from a complete solution to the problem of Internet privacy, but it honors congressional intent by serving as a roadblock for litigants who try to access private communications improperly.

[177] *Cf.* Kerr, *supra* note 15, at 1235–38 (providing recommendations to simplify the SCA).

[178] *See* Robison, *supra* note 10, at 1204–05.