Washington and Lee Law Review

Volume 69 | Issue 2 Article 19

Spring 3-1-2012

Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites

Rudolph J. Burshnic

Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites

Rudolph J. Burshnic*

Table of Contents

* Candidate for J.D., Washington and Lee University School of Law, May 2012. I thank Professor Brian Murchison for his insightful and invaluable feedback on earlier drafts of this Note. I also thank my fellow law review members for their comments and exemplary editing. Any remaining errors are my own.

I. Introduction

Larry sued Ten Pin Lanes for personal injuries stemming from an unfortunate bowling accident. Vanessa, Ten Pin's attorney, suspects Larry is malingering. Her diligent research digs up a gem—Larry has been posting all over Facebook about his latest Aspen ski trip, and this evidence would deal deathly blows to Larry's claim of physical impairment. But because Vanessa expects a long and expensive discovery battle if she requests the Facebook information from Larry directly, Vanessa decides to subpoena Facebook for Larry's profile content (including any personal information, photos, videos, messages, wall posts, and status updates).

Vanessa will soon find out that the Stored Communications Act (SCA)[1] governs her request.[2] But the application of the SCA to social networking sites like Facebook is only a recent phenomenon.[3] Various interpretative difficulties arise when applying the SCA in this context, and the relevant case law has provoked more questions than answers.

This Note explores the application of the SCA in civil litigation to aspects of social networking sites unexplored by the courts. This Note then proposes legislative reforms to update the SCA with respect to social networking sites in the civil litigation context. Part II summarizes the SCA. Part III analyzes *Crispin v. Christian Audigier, Inc.*,[4] a landmark case applying the SCA to social networking sites.

---

1. Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2006).

2. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (applying the SCA to subpoenas directed to Facebook, MySpace, and Media Temple).

3. *See id.* at 977 ("Although some courts have considered the SCA's application to certain types of providers, none appears to have addressed whether social networking sites fall within the ambit of the statute.").

4. *See id. at* 991 (holding that private messages sent over social networking sites are protected from subpoena by the SCA, and remanding the issue of whether the plaintiff's Facebook wall posts and MySpace comments could be subpoenaed after a determination of the plaintiff's privacy settings).

Part IV discusses how the SCA's application to social networking sites relates to general civil discovery rules. Part V addresses the questions left unanswered by *Crispin* and applies the decision to the parts of a Facebook profile unexplored by the court. Finally, Part VI proposes legislative reform.

II. The Stored Communications Act

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA),[5] part of which is a statute known as the Stored Communications Act (SCA).[6] Generally, the ECPA was enacted to update the federal privacy law in light of new changes in communication technology.[7] These "new" communications included "large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing."[8]

More specifically, the SCA portion of the ECPA governs the privacy of stored Internet communications in the United States.[9] The SCA has been used to address gaps in the Fourth Amendment due to the advent of the Internet.[10] The SCA "creates a set of Fourth

---

5. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

6. 18 U.S.C. §§ 2701–2711 (2006).

7. *See* S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555 (explaining that the bill amends the federal wiretap law "to protect against the unauthorized interception of electronic communications" and "to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies"); *id.* at 5, 3559 (noting the SCA seeks to establish "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement").

8. *Id.* at 2, 3556.

9. *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, 1208 (2004) (describing the purpose of the SCA); Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 569 (2007) ("[The SCA] represents Congress' attempt to strike a fair balance between the privacy rights of individuals who have entrusted the contents of their electronic communications to internet service providers and the government's legitimate interest in gaining access to such communications when investigating crimes.").

10. *See* Kerr, *supra* note 9, at 1209–13 (discussing the implications of the Internet and Fourth Amendment privacy protection).

Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information."[11]

Notably, the SCA imposes requirements that the government must meet to compel disclosure of users' electronic communications.[12] The SCA also provides limits on voluntary disclosure by service providers of the same type of information to the government.[13] Depending on how content is classified, the SCA has a layered protection scheme for electronic communications, ranging from a search warrant requirement, to a § 2703(d) court order, to a mere subpoena with prior notice.[14]

Whether and how the SCA protects the privacy of a communication depends on the classification of the provider. The SCA only protects communications stored by the two statutory categories of providers; otherwise, only Fourth Amendment protections apply.[15] In essence, the SCA provides "Fourth Amendment plus" protection to electronic communication stored by a statutorily defined provider.[16]

The first statutory category is an "electronic communication service" (ECS), defined as "any service which provides to users thereof

---

11. *Id.* at 1212.

12. *See* 18 U.S.C. § 2703 (2006) (providing the requirements of required disclosure of customer communications and records when such information is sought by a government entity); *see also* Kerr, *supra* note 9, at 1213 ("[The SCA] creates limits on the government's ability to compel providers to disclose information in their possession about their customers and subscribers.").

13. *See* 18 U.S.C. § 2702 (2006) (providing the limits on voluntary disclosure of customer communications or records by a provider of remote computing service or electronic communication service); *see also* Kerr, *supra* note 9, at 1213 ("[The SCA] places limits on the ability of [Internet service providers] to voluntarily disclose information about their customers and subscribers to the government.").

14. *See* 18 U.S.C. §§ 2702–2703 (2006) (providing restrictions on compelled and voluntary disclosure of various content covered by the SCA).

15. *See* Kerr, *supra* note 9, at 1213 ("If the provider fits within [the ECS or RCS definitions], the SCA protects the communication; otherwise, only Fourth Amendment protections apply.").

16. *See id.* ("Although the private search doctrine of the Fourth Amendment allows private providers to make such disclosures, the SCA imposes limitations on the circumstances in which such a disclosure can occur."); Zwillinger & Genetski, *supra* note 9, at 576 (noting that the Fourth Amendment alone does not prevent Internet service providers (ISP) from disclosing user communication to anyone, including the government (under the private search and voluntary disclosure doctrines), and explaining how the SCA provides limitations on such disclosure).

the ability to send and receive wire or electronic communications."[17] An ECS provider is only prohibited from divulging "the contents of a communication while in electronic storage by that service."[18] "Electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" or alternatively "any storage of such communication by an [ECS] for purposes of backup protection of such communication."[19]

The second category is a "remote computing service" (RCS), defined as an entity that provides the public "computer storage or processing services by means of an electronic communications system."[20] "Electronic communications system" is defined as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[21] RCS providers are prohibited from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service."[22]

A provider can be a RCS, an ECS, both, or neither depending upon what function the provider is performing.[23] For example, a provider can hold a file in temporary, intermediate "electronic storage," and that content is protected by ECS rules,[24] while other files held for long-term storage are governed by RCS rules.[25]

---

17. 18 U.S.C. § 2510(15) (2006); *see, e.g.*, Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (concluding that providers of basic e-mail services are ECS providers under the SCA); Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (concluding that the provider of e-mail services in the case was an ECS).

18. 18 U.S.C. § 2702(a)(1) (2006).

19. *Id.* § 2510(17).

20. *Id.* § 2711(2); *see, e.g.*, Viacom Int'l Inc. v. YouTube, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (holding YouTube to be a RCS with respect to its storage of user videos).

21. 18 U.S.C. § 2510(14) (2006).

22. *Id.* § 2702(a)(2).

23. *See* Kerr, *supra* note 9, at 1215–16 ("A provider can act as an RCS with respect to some communications, an ECS with respect to other communications, and neither an RCS nor an ECS with respect to other communications.").

24. *See* 18 U.S.C. §§ 2702(a)(1), 2703(a) (2006) (providing the rules governing an ECS).

25. *See id.* §§ 2702(a)(2), 2703(b) (providing the rules governing a RCS).

Despite vast technological advancement since the SCA's passage, Congress has yet to update the SCA to conform to modern day innovations related to e-mail and cell phones, among other things.[26] As a result, courts have difficulty applying the SCA to new technologies. The *Crispin* decision is a prime example.

III. Crispin v. Christian Audigier

The SCA is notoriously complicated and confusing,[27] and its application to social networking sites has only further muddied the waters. In May 2010, a federal district court applied the SCA to determine whether the defendants could subpoena the plaintiff's electronic communications from Facebook, Media Temple, and MySpace.[28] This case appears to be the first to apply the SCA to data on social networking sites.[29] Plaintiff, an artist named Buckley Crispin, filed an action against defendants Christian Audigier, Christian Audigier, Inc., and their various sublicensees, alleging that the defendants used Crispin's art in violation of the alleged oral agreement between the parties.[30] Defendants served subpoenas *duces tecum* on the three social networking websites (Facebook, Medial Temple, and MySpace) in their capacity as third-party businesses.[31]

---

26. *See* Mark Sidoti et al., *How Private Is Facebook Under the SCA?*, 8 INTERNET L. & STRATEGY, Nov. 2010, at 1, 4 ("Congress has not amended the SCA to keep pace with changing technology. Rather, courts have had to lead the charge in applying the decades-old statute to modern Internet technology and electronic communication disclosure issues.").

27. *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (acknowledging the difficulty in interpreting the Act because "the ECPA was written prior to the advent of the Internet and the World Wide Web"); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (describing the ECPA, and its subpart, the SCA, as "a complex, often convoluted area of law"); Kerr, *supra* note 9, at 1208 ("Despite [the SCA's] obvious importance, the statute remains poorly understood. Courts, legislators, and even legal scholars have had a hard time making sense of the SCA.").

28. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 971 (C.D. Cal. 2010) (applying the SCA to subpoenas directed to Facebook, MySpace, and Media Temple).

29. *See id.* at 977 ("Although some courts have considered the SCA's application to certain types of providers, none appears to have addressed whether social-networking sites fall within the ambit of the statute.").

30. *Id.* at 968.

31. *Id.* at 968–69.

The subpoenas sought Crispin's basic subscriber information, all communications between Crispin and a tattoo artist named Bryan Callan, and all communication that referred or related to Audigier, Christian Audigier, Inc., the Ed Hardy brand, or any of the sublicensee defendants.[32] Crispin moved to quash the subpoenas. He argued, among other things, that the subpoenas sought electronic communications that third-party Internet service providers are prohibited from disclosing under the SCA.[33] The magistrate judge rejected Crispin's motion to quash on SCA grounds and held that the social networking sites were not subject to the SCA.[34] Crispin then filed a motion to reconsider in the Central District of California.[35]

As an initial matter, the court had to decide whether Crispin had standing to challenge the subpoenas directed at the social networking sites.[36] Ordinarily a party does not have standing to quash a subpoena issued to a nonparty unless that party can claim a personal right or privilege to the information that is requested from the nonparty.[37] In this context, "an individual has a personal right in information in his or her profile and inbox on a social networking site and his or her webmail inbox in the same way that an individual has a personal right in employment and bank records."[38] As a result, Crispin had standing to bring the motion to quash.[39]

Next, the court had to determine how the SCA applied to the third-party social networking sites. In deciding whether SCA protection covered the content on Facebook, Media Temple, and MySpace, the court had to determine whether those services were

---

32. *Id.* at 969.

33. *Id.*

34. *Id.* at 969–70.

35. *Id.* at 970.

36. *See id.* at 973 ("Defendants [argue] that Crispin cannot assert the rights of Media Temple, Facebook, and MySpace, none of whom moved to quash the subpoenas directed to them.").

37. *See id.* ("'Ordinarily a party has no standing to seek to quash a subpoena issued to someone who is not party to the action, unless the objecting party claims some personal right or privilege with regard to the documents sought.'" (quoting 9A CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 2459 (3d ed. 2008))).

38. *Id.* at 974.

39. *See id.* ("As with bank and employment records, this personal right is sufficient to confer standing to move to quash a subpoena seeking such information.").

ECS or RCS under the SCA, depending upon what function the services were performing.[40] Again, an ECS is defined as "any service which provides to users thereof the ability to send and receive wire or electronic communications."[41] Various courts have found that providers of e-mail services are ECS providers.[42] The *Crispin* court analogized the private messaging services that Media Temple, Facebook, and MySpace provide with these types of e-mail services and held that the three sites at issue in the case are generally ECS providers.[43]

As additional support for this conclusion, the court noted the authority on private electronic bulletin board services (BBS)[44]: "Court precedent and legislative history establish that the SCA's definition of an ECS provider was intended to reach a private BBS."[45] But SCA protection "require[s] that the BBS be restricted in some fashion; a completely public BBS does not merit protection under the SCA."[46] Because Facebook and MySpace restrict viewing of wall postings and comments to those with access to the user's profile, "there is no basis for distinguishing between a restricted-access BBS and a user's Facebook wall or MySpace comments."[47]

Next, the court had to determine whether content sought by the subpoenas constituted "electronic storage" within the meaning of the

---

40. *Id.* at 976.

41. 18 U.S.C. § 2510(15) (2006).

42. *See, e.g.*, Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (concluding that providers of basic e-mail services are ECS providers under the SCA); Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (concluding that the provider of e-mail services in the case was an ECS).

43. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010) ("Recognizing that all three sites provide private messaging or email services, the court is compelled to apply the voluminous case law cited above that establishes that such services constitute ECS."). Later, the court noted that "[t]here . . . is no basis for distinguishing between Media Temple's webmail and Facebook's and MySpace's private messaging, on the one hand, and traditional web-based email on the other." *Id.* at 981–82.

44. *See id.* at 980 (noting that Facebook wall postings and MySpace comments "are accessible only to those users plaintiff selects" and finding the authority on private electronic bulletin board services "relevant, if not controlling").

45. *Id.* at 981.

46. *See id.* (citing case law and SCA legislative history).

47. *Id.*

Act.[48] As mentioned above, an ECS provider is prohibited from divulging only "the contents of a communication while in electronic storage by that service."[49] There are two definitions of "electronic storage" in the Act. "Electronic storage" is first defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,"[50] and second, as "any storage of such communication by an [ECS] for purposes of backup protection of such communication."[51] The court held that the "private" *unopened* messages were protected because the entities were acting as ECS providers and holding the unopened messages in "temporary, intermediate" electronic storage.[52]

With respect to the *opened* and retained messages, the entities were held to be RCS providers providing electronic storage, and the messages were held to be protected.[53] Again, RCS is defined as an entity that provides the public "computer storage or processing services by means of an electronic communications system."[54] The court applied case law holding that when e-mail messages were opened, the entity ceased to be an ECS and instead became a RCS providing remote storage for the e-mail.[55] The court quashed the subpoenas seeking the private messages, opened or unopened, because both were held to be protected under the SCA.[56]

---

48. *Id.* at 982.

49. 18 U.S.C. § 2702(a)(1) (2006).

50. *Id.* § 2510(17)(A).

51. *Id.* § 2510(17)(B).

52. *See Crispin*, 717 F. Supp. 2d at 987 ("As respects messages that have not yet been opened, those entities operate as ECS providers and the messages in are electronic storage because they fall within the definition of 'temporary, intermediate storage' under § 2510(17)(A)."). The court relied on precedent applying the SCA to e-mail messages stored on an Internet service provider's server for this conclusion. *See id.* at 982 (noting case law holding that unopened e-mail messages are covered under the "electronic storage" definition in 18 U.S.C. § 2510(17)(A) as "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"). The court then analogized the e-mails in this context to unopened messages in Media Temple's webmail service and Facebook's and MySpace's private messaging. *Id.*

53. *See id.* at 987 ("As respects messages that have been opened and retained by Crispin, under the reasoning of *Weaver* and *Flagg*, and the dicta in *Theofel*, the three entities operate as RCS providers providing storage under § 2702(a)(2).").

54. 18 U.S.C. § 2711(2) (2006).

55. *See Crispin*, 717 F. Supp. 2d at 987 (discussing *Weaver*).

56. *See id.* at 991 (reversing the lower court order to the extent that it

Facebook wall postings and MySpace comments, on the other hand, presented "a distinct and more difficult question."[57] Wall postings and comments do not have a "temporary, intermediate step" similar to the e-mail process[58] and thus could not be protected as temporary, intermediate storage.[59] Instead, the court found that Facebook and MySpace are ECS providers with respect to wall postings and comments and that the content is in electronic storage for "backup purposes."[60] This part of the decision relied heavily on a Ninth Circuit decision, *Konop v. Hawaiian Airlines, Inc.*[61] *Konop*

---

subpoenaed any "private" messaging).

57. *Id.* at 988.

58. *See id.* at 989 ("Unlike an email, there is no step whereby a Facebook wall posting must be opened, at which point it is deemed received.").

59. *See id.* ("[A] Facebook wall posting or MySpace comment is not protectable as a form of temporary, intermediate storage.").

60. *See id.* (holding that "Facebook and MySpace are ECS providers as respects wall postings and comments and that such communications are in electronic storage" for backup purposes).

61. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002) (holding, among other things, that the district court improperly granted summary judgment to Hawaiian Airlines on Konop's SCA claim). This court had to decide whether the district court properly dismissed Konop's SCA claim against Hawaiian Airlines, Inc. (Hawaiian). Robert Konop, a pilot for Hawaiian, alleged that Hawaiian viewed his website without authorization, disclosed the contents of the site, and took other actions in violation of, among other things, the SCA. *Id.* at 872. Konop's website contained a bulletin where he posted comments critical of his employer, its officers, and his current airline union. *Id.* Access to the website was controlled by requiring visitors to log in with a user name and password. *Id.* Anyone accessing the site had to agree to terms and conditions that prohibited any member of Hawaiian's management from viewing the website and prohibited disclosure of the website's contents to anyone else. *Id.* at 872–73. The Hawaiian vice president, James Davis, accessed the site by using the usernames of two of Konop's fellow Hawaiian pilots. *Id.* at 873. Konop argued on appeal that Davis accessed a stored communication without the proper authorization under the SCA. *Id.* at 879. The parties stipulated that the website was an "electronic communications service" and that the website was in "electric storage." *Id.* The court assumed, without deciding, that Davis's conduct constituted "access without authorization" to "a facility through which an electronic communication service is provided." *Id.* at 879–80. The court noted that "the plain language of § 2701(c)(2) [of the SCA] indicates that only a 'user' of the service can authorize a third party's access to the communication." *Id.* at 880. "User" is defined as "one who 1) *uses* the service and 2) is duly authorized to do so." *Id.* The court found that neither pilot who allowed Davis to access the site could be found to be a "user" when they authorized Davis to access it. *Id.* Thus, the court reversed the district court's grant of summary judgment to Hawaiian on the SCA claim. *Id.*

addressed the application of the SCA to a secure website containing a bulletin board.[62] The *Konop* court concluded that the private bulletin board at issue was in fact covered by the SCA.[63] The parties agreed that the website containing the bulletin board was an ECS provider and the communication it stored was electronic storage under § 2510(17).[64] The *Konop* court did not, however, indicate whether the electronic storage was held for temporary and immediate storage or for backup.[65] The *Crispin* court reasoned that the bulletin postings in *Konop* could not be considered to be in temporary, intermediate storage.[66] Because the *Konop* court found the postings to be within "electronic storage," the only other option under the SCA is for the postings to be stored for "backup purposes."[67] Thus, "it appears that the passive action of failing to delete a BBS post, which is in all material ways analogous to a Facebook wall posting or a MySpace comment, also results in that post being stored for backup purposes."[68]

The court, however, hedged its reasoning and alternatively held Facebook and MySpace to be RCS providers with respect to wall postings and comments.[69] The court found persuasive *Viacom International Inc. v. YouTube*,[70] which held YouTube to be a RCS

---

62. *Id.* at 872.

63. *See id.* at 875 (noting that the legislative history of the ECPA suggests Congress wanted to protect private communications like e-mail and private electronic bulletin boards).

64. *See id.* at 879 ("The parties agree that the relevant 'electronic communications service' is Konop's website, and that the website was in 'electronic storage.'").

65. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 988 (C.D. Cal. 2010) (noting that the *Konop* court "did not indicate whether the electronic storage was temporary and intermediate or for backup purposes").

66. *See id.* at 989 ("Because Facebook wall postings and MySpace comments, on the one hand, and bulletin postings on a website such as Konop's, on the other, cannot be considered to be in temporary, intermediate storage, the court interprets *Konop* as holding that the postings, once made, are stored for backup purposes.").

67. *See id.* ("This reading of *Konop* is consistent with *Theofel* and *Quon*, which held that email messages and pager text-messages, respectively, were held for backup purposes once read.").

68. *Id.*

69. *See id.* at 990 ("In the alternative, the court holds that Facebook and MySpace are RCS providers as respects the wall postings and comments.").

70. *See* Viacom Int'l Inc. v. YouTube, 253 F.R.D. 256, 265 (S.D.N.Y. 2008) (holding, among other things, that plaintiffs cannot compel YouTube to produce

provider because "it provided storage services for the user . . . it stored the video on a web page for the benefit of the user and those the user designates."[71] Like the wall postings and comments, the private videos sought in the *Viacom* case "are accessible to a limited set of users selected by the poster and are stored on a page provided by the website."[72]

The subpoenas for the Facebook wall postings and MySpace comments were remanded to the magistrate judge for further findings of fact.[73] Whether this information could be subpoenaed

---

"private" user videos because YouTube is prohibited from doing so under the ECPA). The various plaintiffs in this case brought copyright infringement claims against YouTube and Google. In one motion, plaintiffs sought to compel defendant YouTube to produce copies of various "private" videos "which can only be viewed by others authorized by the user who posted each of them, as well as specified data related to them." *Id.* at 264. The court found that YouTube, as a "remote computing service," could not produce the videos under SCA § 2702 because that statute does not allow a RCS to divulge "any electronic communications stored on behalf of their subscribers." *Id.* Also, the statute contains "no exception for disclosure of such communications pursuant to civil discovery requests." *Id.* The court noted that this prohibition only applies when the provider "'is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing,'" but that defendants had satisfied this condition. *Id.* at 264 n.8 (quoting SCA § 2702(a)(2)(B)).

The plaintiffs claimed that the users authorized disclosure of the contents of the private videos, which would allow YouTube to divulge such information under SCA § 2702(b)(3), by consenting to YouTube's Use and Privacy Policy. *Id.* But the court found that none of the clauses in the Policy could be construed as a "grant of permission from users to reveal to plaintiffs the videos that they have designated as private and chosen to share only with specified recipients." *Id.* at 265. Thus, the motion to compel production of the private video content was denied. *Id.*

The plaintiffs also requested "non-content data" (for example, a video's view count) about the videos. *Id.* They argued that "such data are relevant to show whether videos designated as private are in fact shared with numerous members of the public and therefore not protected by the ECPA, and then to obtain discovery on their claim . . . that users abuse YouTube's privacy feature" to share videos but evade detection by the video's owners. *Id.* The court granted this request, finding that the plaintiffs "need the requested non-content data so that they can properly argue their construction of the ECPA on the merits and have an opportunity to obtain discovery of allegedly infringing private videos claimed to be public." *Id.*

71. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 990 (C.D. Cal. 2010).

72. *Id.*

73. *Id.* at 991.

under the SCA depended upon whether the user's wall was open to the public or restricted in some manner: as the court noted, a "review of the plaintiff's privacy settings would definitively settle the question."[74]

The *Crispin* decision is important because it provided insight into how the SCA can be interpreted in the social networking site context, and it highlighted the difficulties in doing so. At the same time, *Crispin* raised many new questions: How restricted must a user's content be to be subject to subpoena? Are status updates and profile information subject to SCA protection? Can a user's list of "friends" be subject to subpoena under the SCA? Is content private because one must be a site subscriber to access the profile or does access have to be limited to a user's friends? If the user changes his privacy settings in the middle of litigation, before the subpoena is granted, is discovery precluded?

IV. The Stored Communications Act's Relationship to General Civil Discovery of Social Networking Site Information

Before discussing the implications of *Crispin*, this Part addresses the important parallel issue of general civil discovery between parties and how it relates to the subpoena of a third-party social networking site. The defendants in *Crispin* (and Vanessa, our hypothetical defendant's lawyer) chose to pursue the plaintiff's information by serving a subpoena on social networking websites. In federal courts, subpoenas in civil litigation are governed generally by Federal Rule of Civil Procedure 45.[75] But a litigant's Facebook profile or MySpace messages are also subject to general civil discovery and the accompanying rules.[76]

---

74. *Id.*

75. *See* FED. R. CIV. P. 45 (providing requirements for issuing a subpoena, among other things).

76. *See* Tonn Petersen, *Redefining "Privacy" in the Era of Social-Networking*, ADVOCATE, Sept. 2010, at 27, 27 (noting that the defendant in *Crispin* "could still seek information directly from the plaintiff in the case"); Sidoti et al., *supra* note 26, at 5 ("[A] litigant seeking to obtain another party's private online communications may be able to avoid application of the SCA altogether by simply serving a Rule 34 document request directly on the party whose communications are sought.").

Federal discovery requests in civil cases are governed generally by Federal Rule of Civil Procedure 26.[77] The scope of a discovery request is broad: parties may request discovery "regarding any nonprivileged matter that is relevant to any party's claim or defense."[78] Federal Rule of Civil Procedure 26(b)(2) provides some limitations on this otherwise broad scope of permissible civil discovery.[79] Federal Rule of Civil Procedure 34 provides more specific rules regarding the discovery of "electronically stored information" or ESI.[80] While this Note's main focus will not be the issue of civil discovery in the social networking context, it is helpful to compare this method of information gathering with the civil subpoena and the rules for parties and nonparties to civil litigation. This merits a brief discussion of the recent case law regarding the discovery of social networking account information—a relatively new legal issue.[81]

A. Discovery Cases

Mackelprang v. Fidelity National Title Agency of Nevada, Inc.[82] involved a sexual harassment suit based on allegations stemming from the plaintiff's time as an employee at Fidelity.[83] During

77. *See* FED. R. CIV. P. 26 (providing duty to disclose discovery, and the relevant general provisions regarding discovery).

78. *Id.* 26(b)(1).

79. *See id.* 26(b)(2)(C) (allowing the court to limit frequency or extent of discovery based on various factors).

80. *See id.* 34 (providing for discovery of electronically stored information, but within the scope of Rule 26(b)).

81. *See* EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D 430, 434 (S.D. Ind. 2010) (discussing the principles applicable to the discovery of social networking sites: "[D]espite the popularity of [social networking sites] and the frequency with which this issue might be expected to arise, remarkably few published decisions provide guidance on the issues presented here"); *see also* Evan E. North, Note, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1290–93 (2010) (discussing recent developments in this area).

82. *See* Mackelprang v. Fidelity Nat'l Title Agency of Nev., Inc., No. 2:06-CV-00788-JCM-GWF, 2007 WL 119149, at *6 (D. Nev. Jan. 9, 2007) (holding that because the defendants "have failed to demonstrate a relevant basis for obtaining production of Plaintiff's Myspace.com private email messages based on Defendants' suspicion that they may contain sexually explicit or sexually promiscuous content[,]" the defendant's motion to compel plaintiff's consent to produce these messages must be denied).

83. *See id.* at *1 (noting various claims by the plaintiff).

discovery, defendant Fidelity first attempted to subpoena MySpace for all the records of the plaintiff's two accounts on the site, including her private e-mail communications.[84] MySpace produced certain "public" information about the accounts, but "refused to produce private email messages on either account in the absence of a search warrant or letter of consent to production by the owner of the account."[85] Subsequently, plaintiff Mackelprang refused defendant's request for her consent to the release of the private messages, on the grounds that the information is "irrelevant and improperly invades" her privacy.[86]

Fidelity then moved to compel production of Mackelprang's private e-mails on MySpace.[87] The court denied this request, in part because of factors relating to evidence rules governing admissibility of sexual behavior, which in turn are relevant to whether such information is discoverable.[88] But the court did not imply that the MySpace e-mails were not discoverable, and instead stated the opposite: "The proper method for obtaining such information, however, is to serve upon Plaintiff limited requests for production of relevant [MySpace] email communications."[89]

Equal Employment Opportunity Commission v. Simply Storage Management, LLC[90] also involved discovery of social networking sites in a sexual harassment suit.[91] The Equal Employment Opportunity Commission (EEOC) requested a discovery conference to determine whether the two claimants in this case had to produce their "profiles"[92] and other communication from their Facebook and

---

84. *See id.* at *2 ("Defendant Fidelity thereafter served a subpoena on Myspace.com . . . to produce all records for these accounts, including private email communications exchanged between Plaintiff and others.").

85. *Id.*

86. *Id.*

87. *Id.*

88. *See id.* at *6 ("[T]he probative value of such evidence does not substantially outweigh its unfair prejudicial effect to Plaintiff.").

89. *Id.* at *8.

90. *See* EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 435 (S.D. Ind. 2010) (holding that social networking site discovery was proper, but the scope of such discovery must be limited by relevancy).

91. *See id.* at 432 (describing the EEOC sexual harassment suit on behalf of two claimants, and the ensuing discovery dispute over the scope of social networking site information).

92. *See id.* at 432 n.1 (interpreting "profile" to mean "any content—

MySpace accounts.[93] The parties disagreed about the proper scope of discovery involving the various requests.[94] The EEOC, representing the two claimants, objected to the requests as overly broad and irrelevant.[95] The EEOC also objected on the grounds that the requests were unduly burdensome because they infringed on the claimants' privacy, in addition to being harassing and embarrassing.[96]

The court then determined the proper scope of the discovery requests in light of the emotional distress claims at issue. As a preliminary matter, the court determined that social networking site content is not barred from discovery because it is made "private" by the user.[97] Next, while the court agreed that social networking site discovery was appropriate, the court found that its scope had to be limited to the circumstances (in other words, relevant within Rule 26).[98] "[T]he appropriate scope of relevance is any profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) and [social networking site] applications . . . that reveal, refer, or relate to any emotion, feeling, or mental state" and also "communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state."[99] The same test would

---

including postings, pictures, blogs, messages, personal information, lists of 'friends' or causes joined—that the user has placed or created online by using her user account").

93. *Id.* at 432.

94. *See id.* (noting disputed discovery requests over photographs, videos, and electronic copies of profile pages from Facebook and MySpace). The requests for electronic copies of the profile pages included "all status updates, messages, wall comments, causes joined, groups joined, activity streams, blog entries, detail, blurbs, comments, and applications." *Id.*

95. *Id.*

96. *See id.* ("The EEOC objects to production of all SNS content (and to similar deposition questioning) on the grounds that the requests are overbroad, not relevant, unduly burdensome because they improperly infringe on claimants' privacy, and will harass and embarrass the claimants.").

97. *See id.* at 434 ("[A] person's expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery.").

98. *See id.* at 435 ("It is reasonable to expect severe emotional or mental injury to manifest itself in some SNS content, and an examination of that content might reveal whether onset occurred, when, and the degree of distress.").

99. *Id.* at 436.

apply to photographs and videos.[100] Third-party communications had to be produced if the claimants' own communications put them in "context."[101]

In *Romano v. Steelcase, Inc.*,[102] Romano brought a personal injury action against Steelcase. Steelcase sought an order giving access to Romano's Facebook and MySpace accounts, believing it could find information that would discredit Romano's claims regarding her injuries.[103] The court mentioned reviewing the SCA but did not offer any related analysis.[104] Presumably, the court did not find that it governed the case. Under the New York state civil discovery standard of "material and necessary," the court found that Romano's Facebook and MySpace accounts were both material and necessary to Steelcase's defense, and that the account information could lead to admissible evidence.[105]

B. Relevance to the Stored Communications Act

As the prior discussion shows, parties in civil litigation are subject to discovery procedures (including requests for production and subpoenas), but nonparties can also be compelled to produce information by order of a subpoena.[106] A party may attempt to

---

100. *See id.* ("The same test set forth above can be used to determine whether particular pictures should be produced.").

101. *See id.* ("Third-party communications to [claimants] must be produced if they place these claimants' own communications in context.").

102. *See* Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 654 (N.Y. Sup. Ct. 2010) (holding information from Romano's Facebook and MySpace accounts discoverable).

103. *See id.* at 653 ("Steelcase contends that a review of the public portions of [Romano's] Facebook and MySpace pages reveals that she has an active lifestyle and has traveled to Florida and Pennsylvania during the time period she claims that her injuries prohibited such activity."). After looking at the public portions of her profile, Steelcase sought to question Romano at her deposition and sought a request for authorization to access her Facebook and MySpace accounts. *Id.* Romano did not cooperate with either request. *Id.*

104. *See id.* at 651–52 ("The Court has reviewed . . . the applicable federal statutory law, specifically the Stored Communications Act . . . .").

105. *See id.* at 654 ("[T]here is a reasonable likelihood that the private portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action.").

106. *See* FED. R. CIV. P. 45 (providing the rule for civil subpoenas).

subpoena a nonparty's information through a Rule 45 request, but this request cannot overcome the protections provided in the SCA.[107] There are exceptions to these SCA protections, but "the exceptions enumerated in § 2702(b) do not include civil discovery subpoenas."[108] The lack of an exception in the SCA for civil discovery subpoenas explains why the SCA, rather than the civil procedure rules, governed the *Crispin* decision.[109]

On the other hand, a court may force a *party* in the course of civil discovery to "consent" to produce electronically stored information within its "control" under Rule 34, thus avoiding the SCA issue.[110]

---

107. *See, e.g.*, *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 609 (E.D.V.A. 2008) (upholding a magistrate judge's order quashing a subpoena requesting a nonparty's e-mails from AOL because there is no exception in the SCA for such disclosure).

108. *Id.* at 611; *see also* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 975 (C.D. Cal. 2010) ("The [SCA] does not mention service of a civil subpoena duces tecum."); Timothy G. Ackermann, *Consent and Discovery Under the Stored Communications Act*, 56 FED. LAW. 42, 43 (Dec. 2009) ("[Section] 2702 of the SCA does not provide a general exception for complying with civil discovery."); Zwillinger & Genetski, *supra* note 9, at 587 ("[T]he SCA contains no exception for civil discovery . . . .").

109. *See Crispin*, 717 F. Supp. 2d at 971 (applying the SCA to subpoena requests to nonparty social networking sites). This Note, in Part VI.B., argues that the SCA should include a civil litigant exception that it now lacks.

110. *See* Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (holding that the SCA does not prevent Defendant from giving consent to a third-party to release text messages relevant to discovery). The Court stated:

> Defendant City is both able and obligated to give its consent, as subscriber, to SkyTel's retrieval of text messages so that the City may comply with a Rule 34 request for their production . . . . [A] party has an obligation under Rule 34 to produce materials within its control, and this obligation carries with it the attendant duty to take the steps necessary to exercise this control and retrieve the requested documents . . . . [A] party's disinclination to exercise this control is immaterial, just as it is immaterial whether a party might prefer not to produce documents in its possession or custody.

Id.; *see also* Ackermann, *supra* note 108, at 43 ("Section 2702(b)(3) of the SCA does, however, create an exception based on lawful consent that applies to civil discovery."); Steve C. Bennett, *Civil Discovery of Social Networking Information*, 39 SW. L. REV. 413, 423 (2010) ("[A litigant] may be required to provide consent for access to social networking sites that contain [relevant] information . . . . [I]f the litigant has the ability to obtain 'control' over such information by providing consent to the ISP, then the litigant must provide such consent as part of its discovery obligations."). But there is at least one authority to the contrary. *See* J.T. Shannon Lumber Co. v. Gilco Lumber Inc., No. 2:07-CV-119-SA-SAA, 2008 WL 4755370, at *1 (N.D. Miss. Oct. 29, 2008) (denying plaintiff's motion to compel defendant's consent for information held by ISPs). The court reasoned

Consequently, in the context of civil litigation, the SCA is most relevant to requests for electronically stored information of *nonparties*, or for parties who forgo the discovery route and subpoena a nonparty ECS or RCS for the opposing party's information. Thus, this Note focuses on the SCA's application to civil subpoenas served on social networking sites outside of the normal discovery context between parties.

Nevertheless, the availability of discovery procedures does not undermine the importance of the application of the SCA in the social networking context. Again, the SCA still protects nonparties who are not subject to the discovery process.[111] Also, litigants have incentives to retrieve information directly from a social networking site because this tactic is easier than obtaining the information from the opposing parties themselves.[112] Accordingly, it is still important that there be clear standards for what the SCA does and does not protect when litigants subpoena social networking sites for information.

V. Applying Crispin v. Christian Audigier

Crispin provided two important answers. First, social networking site information is subject to protection under the SCA. The court determined that the SCA protects information on Facebook, MySpace, and Media Temple because, depending on what function they are serving, the sites are either ECS or RCS.[113] Second,

---

that this request would allow an "end run around the [SCA]," which implies that the court believed the SCA should still preclude the request. *Id.* In any event, "the plaintiff has other means of obtaining any discoverable information at its disposal, which would not be contrary to the Stored Communications Act." *Id.*

111. *See, e.g.*, *In re Subpoena Duces Tecum*, 550 F. Supp. 2d at 609 (upholding a magistrate judge's order quashing a subpoena requesting a nonparty's e-mails from AOL because there is no exception in the SCA for such disclosure).

112. *See* Derek S. Witte, *Your Opponent Does Not Need a Friend Request to See Your Page: Social Networking Sites and Electronic Discovery*, 41 MCGEORGE L. REV. 891, 897 (2010) ("Because an individual Facebook [user] does not have direct access to the servers upon which his or her pages are stored [or access to archived information] . . . the best way to discover this potentially rich ESI . . . is by requesting it directly from the sites themselves.").

113. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010) (holding that the social networking sites are ECS when they hold private unopened private messages but RCS regarding opened and retained private messages). When Facebook or MySpace holds a wall post or comment,

privacy settings matter. Crispin's privacy settings on his Facebook and MySpace accounts would "definitively settle the question" whether the defendants could subpoena Crispin's wall posts and comments.[114] Private messages, on the other hand, were analogized to e-mails and were held to be protected.[115]

But even with the guidance of *Crispin*, social networking sites fail to find a good fit within the statutory framework of the SCA. *Crispin* left important questions unanswered, particularly regarding the issue of privacy settings.[116] This Part addresses the issue of what should be sufficiently "private" for protection under the SCA,[117] applies *Crispin* to the various Facebook profile parts that the court did not address,[118] and addresses the question of when, in the course of litigation, a user's privacy settings are relevant.[119]

A. Privacy Settings Should Not Be Determinative of Whether a User's Profile Is "Private" Under the Stored Communications Act

How private must a user's information be to be protected? Generally, the SCA prohibits voluntary disclosure from a public provider of electronic communications[120] but does not protect electronic communications "readily accessible to the general public."[121]

---

they operate as ECS or RCS. *See id.* at 989–90 (holding that the sites are ECS in this regard, but alternatively holding that they are RCS).

114. *Id.* at 991.

115. *See id.* (quashing a subpoena for webmail and private messages because they are "inherently private" and "not readily accessible to the general public").

116. *See, e.g.*, Alan Klein et al., *Social Networking Sites: Subject to Discovery?*, THE NAT'L L.J., Aug. 23, 2010, at 15, 19 ("Is content private if one must be a subscriber to access it, or must access be limited to a user's 'friends,' which on Facebook may number in the thousands?"); Petersen, *supra* note 76, at 27–28 ("Does the definition of privacy merely turn on whether a user chooses a public or private setting by the click of a mouse? If so, can a user involved in litigation make critical information inaccessible simply by changing privacy settings on his or her Facebook or MySpace pages?").

117. *Infra* Part V.A.

118. *Infra* Part V.B.

119. *Infra* Part V.C.

120. *See* 18 U.S.C. § 2702 (2006) (providing the voluntary disclosure rules and exceptions).

121. *See id.* § 2511(2)(g) ("It shall not be unlawful under [the SCA] for any

Crispin implicitly rejected the argument that signing up for a Facebook account to access another user's profile is a sufficient privacy bar: "[E]ither the general public had access to plaintiff's Facebook wall and MySpace comments, or access was limited to a few."[122] The general public would necessarily have to sign up for Facebook to access the profile.[123] Apparently, the court viewed this registration step as irrelevant to the privacy determination.

Also, according to the court, a user with numerous "friends" on a social networking site would still have "private" wall posts, so long as the proper privacy settings were in place.[124] To base a rule on the number of friends would result in "arbitrary line-drawing" and would lead to "anomalous result[s]."[125] While the court's concerns are legitimate, one could imagine a Facebook profile that can only be viewed by a user's friends but still falls within the statutory language of "readily accessible to the general public."[126] For example, celebrity Facebook profiles are relatively common. A celebrity could restrict her profile only to her "friends," yet her "friends" could be indiscriminately "accepted" without regard to who they might be. In practical terms, this hypothetical Facebook profile would be "readily accessible to the general public." Simply because a user's profile is set to "private" should not foreclose the possibility that the profile still

---

person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.").

122. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

123. *See* Facebook, *Sign Up for Facebook*, http://www.facebook.com/r.php (last visited Apr. 10, 2012) (requiring a first and last name, e-mail address, password, gender, and birthday to create a Facebook account) (on file with the Washington and Lee Law Review). *Crispin* also covered MySpace, but this Note only focuses on Facebook because Facebook is today's preeminent social networking site and because the discussion of a single social networking site, as opposed to multiple, is preferable for the sake of clarity.

124. *See Crispin*, 717 F. Supp. 2d at 990 (noting that the number of plaintiff's Facebook friends who can view a wall post "has no legal significance").

125. *See id.* ("[B]asing 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."). While this discussion was within the court's discussion of the sites as RCS, the court presumably would apply the same logic to the ECS context.

126. 18 U.S.C. § 2511(2)(g) (2006).

may be readily accessible to the general public and thus unprotected by the SCA.

B. Extending Crispin *to the Rest of a User's Facebook Profile*

While *Crispin* only addressed private messages and wall posts or comments in the social networking context, there is a plethora of other information that a litigant could seek. Facebook allows a user to update his status, post videos and photos, and to include various profile information.[127] As with wall posts, Facebook allows a user to restrict the previously mentioned information to either all, some (including, for example, an option for only friends in your network), or none of his friends.[128] Or, a user can leave this information open to any Facebook user.[129] This subpart applies the logic of *Crispin* to Facebook profile content that the court did not address. First, it addresses whether certain profile content is "electronic communication" under the SCA. Second, it determines whether Facebook acts as either an ECS or RCS with respect to that profile content.

1. Facebook Profile Content Is Electronic Communication Under the Stored Communications Act

There is a preliminary question: what content can be properly deemed "communication"?[130] The SCA only protects "electronic

127. *See* EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 432 n.1 (S.D. Ind. 2010) (interpreting "profile" to mean "any content—including postings, pictures, blogs, messages, personal information, lists of 'friends' or causes joined—that the user has placed or created online by using her user account").

128. *See* Facebook, *Facebook's Privacy Policy* (Dec. 22, 2010), http://www.facebook.com/policy.php (last visited Apr. 10, 2012) (explaining Facebook's privacy policy) (on file with the Washington and Lee Law Review).

129. *Id.*

130. *See* Witte, *supra* note 112, at 900 ("[I]t is possible that the Stored Communications Act, which only protects communications from disclosure, may prohibit these [social networking] websites from divulging the other contents of someone's page, such as photos, the individual's 'wall,' . . . 'friends,' or other data displayed on the page."). Witte also notes that he "could find no case addressing the issue of whether social networking sites fall within the scope of the Stored Communications Act." *Id.* Witte's article was published just prior to the *Crispin* decision.

communication" from disclosure.[131] The statute defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system."[132] The *Crispin* court held that sufficiently private wall posts and comments and private messages are protected under the SCA as electronic communication.[133] The *Viacom* court held that YouTube videos were protected and, if only implicitly, deemed the videos "communication."[134]

Given the broad definition of electronic communication in § 2510(12), it is likely that all profile content of a Facebook page would be protected by the SCA as "electronic communication."[135] A user's status updates and profile information are all "written" and thus within § 2510(12).[136] It seems relevant that the *Crispin* court did not even find it necessary to address whether the wall posts and comments were electronic communications.[137]

Photos would be covered by the term "images." While videos are not explicitly mentioned, this is in all likelihood not an intentional omission but instead indicative of the technology in 1986, when

---

131. *See* 18 U.S.C. § 2702(a)(1) (2006) ("[An ECS] shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."); *id.* § 2702(a)(2) ("[An RCS] shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service.").

132. *Id.* § 2510(12).

133. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (holding plaintiff's private messages protected under the SCA and remanding the wall posts and comments issue for a determination of privacy settings). The court did not specifically address whether the messages were electronic communication, but this determination was indeed necessary to reach the holding.

134. *See* Viacom Int'l Inc. v. YouTube, 253 F.R.D. 256, 265 (S.D.N.Y. 2008) (holding that plaintiffs cannot compel YouTube to produce "private" user videos because YouTube is prohibited from doing so under the ECPA).

135. *See* 18 U.S.C. § 2510(12) (2006) (defining "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system").

136. *Id.*

137. *See Crispin*, 717 F. Supp. 2d at 988–91 (applying the SCA to the subpoena requests for plaintiff's Facebook wall posts and MySpace comments but neglecting to address whether such information was "electronic communication" within the Act).

Congress enacted the ECPA. The *Viacom* court has already held that the SCA protects videos (without discussing the threshold "electronic communications" issue),[138] and § 2510(12) covers videos without straining the statutory text.[139] It would be rather anomalous for the SCA to protect "images" and not videos.

Whether a user's list of "friends" is covered by § 2510(12) presents a slightly more difficult problem. One could argue that because a user's friend is represented as a picture, it is within the definition of an "image." Names of friends, of course, are in "writing," and this could be another ground. A list of friends could arguably even be deemed "data." In any event, it is unlikely that a court would hold that a user's list of friends falls outside the electronic communication definition in § 2510(12). In conclusion, despite the peculiarities of Facebook profile content, all of it should be covered by the SCA definition of "electronic communication."

2. Facebook Acts as Both a RCS and an ECS

Next, it must be determined whether Facebook acts as a RCS or an ECS with respect to profile content. The distinction is pertinent because, under the SCA, disclosure protection levels differ based on how content is classified.[140] How the content is classified then determines whether an entity is acting as a RCS or an ECS.[141] If Facebook is neither an ECS or a RCS with respect to this profile content, then SCA protection is unavailable and only Fourth Amendment protections apply.[142]

---

138. *See Viacom*, 253 F.R.D. at 265 (holding that YouTube videos protected by the SCA, but not discussing whether those videos are "electronic communication" within the Act).

139. *See* 18 U.S.C. § 2510(12) (2006) (defining "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system").

140. *See id.* §§ 2702–2703 (providing voluntary and required disclosure rules for the various content covered by the SCA); *see also* Kerr, *supra* note 9, at 1222–23 (explaining the basic disclosure rules of the SCA).

141. *See* 18 U.S.C. §§ 2702–2703 (2006) (providing the disclosure rules governing RCS and ECS).

142. *See* Kerr, *supra* note 9, at 1213 ("If the provider fits within [the ECS or RCS definitions], the SCA protects the communication; otherwise, only Fourth Amendment protections apply.").

The *Crispin* court, in an alternative holding, held Facebook and MySpace to be RCS providers supplying remote storage for the wall posts and comments.[143] In *Viacom* the court found that YouTube was acting as a RCS because it "stored the video on a web page for the benefit of the user and those the user designates," and the private videos sought were "accessible to a limited set of users selected by the poster and . . . stored on a page provided by the website."[144] Like in *Viacom*, the wall postings and comments in *Crispin* were stored on Facebook's website for the user, subject to the user's privacy settings.[145]

Applying the *Crispin* and *Viacom* logic, Facebook acts as a RCS regarding personal profile information (relationship status, religious views, birth date, contact information, etc.) on a user profile.[146] Personal profile information, like the wall posts and comments in *Crispin* and the videos in *Viacom*, is stored on Facebook's website, and access is limited as selected by the user.[147] Accordingly, these different aspects of a user's profile content should be subject to the same analysis that the *Crispin* court applied to wall posts and comments. That is, the user's privacy settings determine whether the requested information could be subpoenaed under the SCA under the "readily available to the general public" standard.[148]

There is a counterargument that Facebook is acting as an ECS rather than a RCS. Indeed, the *Crispin* court first held that Facebook and MySpace were acting as ECSs with respect to the wall posts and

---

143. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 990 (C.D. Cal. 2010) (holding, in the alternative, that Facebook and MySpace are RCS providers with respect to wall postings and comments).

144. *Id.*

145. *See id.* ("The private videos whose production plaintiff sought to compel [in *Viacom*] are thus analogous to the Facebook wall postings and MySpace comments defendants seek here, in that both are accessible to a limited set of users selected by the poster and are stored on a page provided by the website.").

146. *Id.*

147. *See* Facebook, *Controlling How You Share*, http://www.facebook.com/privacy/explanation.php (last visited Apr. 10, 2012) (discussing various types of personal profile information a user can add and how the user can restrict viewing access to such content) (on file with the Washington and Lee Law Review).

148. *See Crispin*, 717 F. Supp. 2d at 991 (remanding for a determination of privacy settings to decide whether the plaintiff's wall posts and comments could be subpoenaed).

comments[149] and only alternatively held that the entities were acting as RCSs.[150] But under *Crispin* and *Konop*, the ECS argument is less persuasive for personal profile information. Personal profile information is closer to the RCS distinction in *Viacom* than the ECS distinction in *Konop*.[151] Unlike the private electronic bulletin board in *Konop*, only the user can post his personal information to his profile page.[152] The bulletin board in *Konop*, in contrast, allowed for multiple users to post information.[153] A user's posting of personal profile information is therefore more similar to the YouTube user in *Viacom* who posts videos to his account; both users are solely in control of how and what content is posted, and accordingly, a social networking site acts as a RCS with respect to storage of this information.

The ECS argument is more persuasive when analyzing an outside user's post on the user's Facebook wall. The *Crispin* court analogized the wall posts and comments to the secure website containing an electronic bulletin board in *Konop* and found that Facebook and MySpace were ECS providers providing electronic storage for backup purposes.[154] The *Crispin* court reasoned that the passive action of failing to delete a bulletin board post in *Konop*, which resulted in the post being stored for backup purposes, was analogous to the storage of wall postings and comments.[155] Like the

149. *See id.* at 989 (holding that "Facebook and MySpace are ECS providers as respects wall postings and comments and that such communications are in electronic storage" for backup purposes).

150. *See id.* at 990 ("In the alternative, the court holds that Facebook and MySpace are RCS providers as respects wall postings and comments.").

151. *Compare* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002) (holding that a website providing a private electronic bulletin board is acting as an ECS), *with* Viacom Int'l Inc. v. YouTube, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (holding YouTube to be a RCS with respect to its storage of videos for a user).

152. Facebook, *Controlling How You Share*, http://www.facebook.com/privacy/explanation.php (last visited Apr. 10, 2012) (on file with the Washington and Lee Law Review).

153. *See Konop*, 302 F.3d at 872 (describing how access to the electronic bulletin board was limited to users made eligible by Konop).

154. *See Crispin*, 717 F. Supp. 2d at 989 (holding that "Facebook and MySpace are ECS providers as respects wall postings and comments and that such communications are in electronic storage" for backup purposes); *id.* ("This reading of *Konop* is consistent with *Theofel* and *Quon*, which held that email messages and pager text-messages, were held for backup purposes once read.").

155. *See id.* ("[I]t appears that the passive action of failing to delete a BBS post, which is in all material ways analogous to a Facebook wall posting or a

electronic bulletin board in *Konop*, multiple users can post to a user's profile wall, assuming the user has set privacy settings allowing other users to do so.[156] Accordingly, under the *Konop* and *Crispin* logic, when a user posts on another user's wall, the failure to delete that post makes Facebook an ECS providing backup protection with respect to the recipient user's wall posts.[157]

Unfortunately, the distinction is meaningless in the context of civil litigation. The SCA prohibits a public ECS or RCS from voluntarily disclosing the content of a user's communication, barring an exception not relevant here.[158] So, when it is determined that a user's Facebook content is protected because the site is acting as an ECS or a RCS, we get the same result: the covered content that is not readily available to the general public is protected. What matters here is that Facebook fits both the RCS or ECS definition rules so that user content is protected, assuming the content is sufficiently private. The ECS/RCS distinction is more pertinent in the criminal context, where the rules governing compelled disclosure have been widely criticized.[159]

MySpace comment, also results in that post being stored for backup purposes.").

156. *See* Facebook, *Controlling How You Share*, http://www.facebook.com/privacy/explanation.php (last visited Apr. 10, 2012) (explaining how a user can control the use of his profile wall) (on file with the Washington and Lee Law Review).

157. *See Crispin*, 717 F. Supp. 2d at 989 (explaining that, under *Konop*, "it appears that the passive action of failing to delete a BBS post, which is in all material ways analogous to a Facebook wall posting or MySpace comments, also results in that post being stored for backup purposes").

158. *See* 18 U.S.C. § 2702(b) (2006) (providing voluntary disclosure rules and exceptions). Section 2703 provides the disclosure rules for when the government compels information from an ECS or a RCS, and these can vary from a search warrant requirement to no restriction at all, based on the type of content. *Id.* § 2703. Apparently, when a civil litigant subpoenas an ECS or a RCS, the voluntary disclosure rules, not the compelled disclosure rules, apply despite the court's participation (as the "government") in the process. Also, the SCA does not prohibit voluntary disclosure by *nonpublic* providers. *Id.* § 2702.

159. *See, e.g.*, Kerr, *supra* note 9, at 1233 ("The most obvious problem with the current version of the SCA is the surprisingly weak protection the statute affords to compelled contents of communications under the traditional understanding of ECS and RCS."); Digital Due Process, *Comments to NTIA in the Matter of Information Privacy and Innovation in the Internet Economy* 1 (June 14, 2010), *available at* http://www.digitalddueprocess.org/files/NTIA_NOI_061410.pdf (arguing that "[t]he government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online"). One court has even

C. Determining at What Point in Time Privacy Settings Matter

Accompanying the privacy settings issue is the question of exactly when the settings should be taken into account.[160] The point in time a user's privacy settings matter will probably depend on the nature of each individual case. For example, using the hypothetical in the introduction, assume Larry's Facebook profile was fully public when he posted about his post-injury ski trip. Then, assume during the middle of his lawsuit, Larry privatized his profile before Vanessa subpoenaed Facebook. What is the relevant time in determining what his privacy settings are and thus whether his profile content can be subpoenaed under the SCA?

Presumably, the latest time a user's privacy settings would be relevant is at the time of a subpoena to the social networking site. On the other hand, Vanessa could argue the relevant time is the time of Larry's posts. *Crispin* did not offer the lower court any guidance on this point, and at present the answer is unclear.[161]

Social networking sites may or may not keep track of when a user changes his privacy settings. If Vanessa could prove a change in Larry's privacy settings through information from Facebook, she could then argue that the court should apply the privacy settings analysis when he posted the relevant information. Otherwise, Vanessa would have to resort to obtaining evidence of the past public or private nature of Larry's profile herself.

---

ruled some of the compelled disclosure requirements unconstitutional. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails" stored with or sent through an Internet service provider). As a result, "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause." *Id.*

160. *See* Klein et al., *supra* note 116, at 19 ("May a user avoid discovery simply by modifying his or her settings at the time of trial?"); Petersen, *supra* note 76, at 27–28 (analyzing *Crispin* and asking whether "a user involved in litigation [can] make critical information inaccessible simply by changing privacy settings on his or her Facebook or MySpace pages").

161. *See Crispin*, 717 F. Supp. 2d at 991 (noting that a "review of the plaintiff's privacy settings would definitively settle the question" of whether the plaintiff's wall posts and comments could be subpoenaed, but providing no further guidance as to what point in time the privacy settings should be taken into account).

There is an argument that a user's change in privacy settings violates a preservation obligation.[162] Parties (or future parties) generally have a duty to preserve relevant evidence once they are reasonably aware of the possibility of impending litigation.[163] A Facebook user who privatizes his Facebook profile after a lawsuit has been filed could arguably be "destroying" relevant evidence and be subject to sanction.[164] Again, on this point, the law is unclear.

VI. Proposed Legislative Reform

While the previous Part outlined how courts should approach social networking sites under the current version of the SCA, this Part proposes SCA legislative reform. ECPA (and SCA) reform is at the door of both Congressional houses.[165] The SCA should be reformed for two reasons. First, it unnecessarily distinguishes between RCS and ECS, a now irrelevant distinction that only serves to confuse the courts.[166] Second, the current SCA fails to provide an exception for civil litigants, which, if added, would lessen the burdens on service providers and courts and clarify discovery standards for civil litigants.[167]

---

162. *See* Witte, *supra* note 112, at 901 (arguing that social networking site information should be preserved when an individual believes it could be relevant to a foreseeable or ongoing lawsuit).

163. *See* FED. R. CIV. P. 37(f) advisory committee's note (describing when a preservation obligation may arise); 8B CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 2284.1 (3d ed. 2008) (describing the preservation obligation as related to electronically stored information).

164. *See* Witte, *supra* note 112, at 895 (arguing that there is a preservation obligation with respect to the contents of social networking sites).

165. *See generally The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. (2010); *Electronic Communications Privacy Act Reform: Hearing Before the H. Subcomm. on the Constitution, Civil Rights, and Civil Liberties*, 111th Cong. (2010); *ECPA Reform and the Revolution of Location Based Technologies and Services: Hearing Before the H. Subcomm. on the Constitution, Civil Rights, and Civil Liberties*, 111th Cong. (2010); *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the H. Subcomm. on the Constitution, Civil Rights, and Civil Liberties*, 111th Cong. (2010).

166. *Infra* Part VI.A.

167. *Infra* Part VI.B.

A. Collapse the ECS/RCS Distinction

First, the ECS and RCS distinction should be eliminated because it no longer provides any functional purpose and unnecessarily occupies the time of courts and litigants. This is not a new suggestion.[168] Professor Orin Kerr authored a 2004 law review article providing a "legislator's guide" to the SCA and has suggested that the SCA be rewritten so that it applies only to "network service providers."[169] While this Note generally agrees with Kerr's argument, it proposes that it should be refined to include the recent developments with respect to *Crispin* and the SCA's application to social networking sites.

Kerr's proposal would eliminate the distinction that is based on the function a provider performs and would instead "distinguish among the files a provider holds based on its function with respect to that file."[170] It is unclear whether Kerr's proposal would include social networking sites within the definition of network service providers.

The SCA should be amended to collapse the ECS/RCS distinction into the single category of "network service provider," but the "network service provider" definition should include social networking sites. In the wake of *Crispin*, we know that social networking sites are governed by the SCA, and these sites should continue to be protected under any new legislation and included within a new unifying definition.[171] This reform would retain the intent of the original statute while simplifying the text for courts.[172] It would also promote judicial economy; courts, like the one in *Crispin*, would no longer have to unnecessarily labor over the ECS/RCS distinction.[173]

---

168. *See* Kerr, *supra* note 9, at 1235 ("Congress could eliminate the confusing categories of ECS and RCS and simply incorporate these concepts into the statute directly.").

169. *See id.* ("Congress could rewrite the statute so that the SCA applied to only 'network service providers,' which could be defined using a combination of the current definitions of ECS and RCS.").

170. *Id.* Professor Kerr provides the text of proposed statutory language. *Id.* at 1235–38.

171. *See Crispin*, 717 F. Supp. 2d at 971 (applying the SCA to subpoenas directed to Facebook, MySpace, and Media Temple).

172. *See* Kerr, *supra* note 9, at 1237–38 (noting that collapsing the ECS and RCS distinction would simplify the text without losing functionality in both § 2703 and § 2702 of the SCA).

173. *See* Sidoti et al., *supra* note 26, at 8 ("One need look no further than the legal acrobatics that the *Crispin* court and others have employed to determine

This proposition finds further support in the civil litigation context because despite the distinction (ECS or RCS) given to a social networking site, the same protections apply.[174]

B. Include an Exception in the Stored Communications Act for Civil Litigants

Second, the statute should provide a disclosure exception for civil litigants. Currently, the SCA bans ECS and RCS from voluntarily disclosing "content" information when subpoenaed by civil litigants[175] unless such information is "readily available to the general public."[176] In our hypothetical, this means that, under current law, Vanessa could not subpoena the "content" (or substance) of Larry's messages, wall posts, status updates, videos, photos, or profile information if this content is (or was) sufficiently private. Including a disclosure exception in the SCA for civil litigants would allow parties, in certain circumstances, to subpoena content information from a service provider or social networking site. A specified disclosure exception would clarify discovery standards for both courts and litigants while lessening the burden on providers and sites subject to the SCA. This Note argues that Congress should adopt a modified version of Marc Zwillinger and Christian Genetski's proposed disclosure exception amendment discussed below.

In a 2007 article, Zwillinger and Genetski argue that the SCA creates an "uneven playing field" regarding the standards governing "[Internet service providers'] disclosure of Internet communications that turn on the nature of the information sought and the identity of the person seeking it."[177] In short, when the government seeks

---

whether . . . Facebook or MySpace is an ECS and/or RCS provider to conclude that the SCA is outdated . . . .").

174. *See supra* note 158 and accompanying text (describing how the ECS/RCS distinction is irrelevant in relation to the level of voluntary disclosure protection given to user content).

175. *See* 18 U.S.C. § 2702 (2006) (providing the requirements the government must meet to force disclosure of "content" information).

176. *See id.* § 2511(2)(g) ("It shall not be unlawful under [the SCA] for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.").

177. Zwillinger & Genetski, *supra* note 9, at 590.

information from an Internet service provider (ISP) under the SCA, the information is subject to qualified privacy protection, depending on the type of information sought.[178] In contrast, when a criminal defendant or civil litigant seeks information from an ISP under the SCA, "content" information is absolutely protected, while "non-content" information is afforded no protection at all.[179]

When the government seeks content information (for example, the substance of an e-mail) it must meet the statutory requirements.[180] A criminal defendant or civil litigant, on the other hand, cannot compel content information directly from an ISP without requesting the government to compel the information for them.[181] But noncontent information (such as "IP addresses of government informants, the buddy lists of alleged co-conspirators, or the identity of an insulting poster to a message board"[182]) is more easily accessed by the criminal defendant or civil litigant because the SCA provides exceptions to disclosure of noncontent information to "any person other than a governmental entity."[183]

In practice, Zwillinger and Genetski argue, the advantage that nongovernment entities may have in compelling noncontent information is largely gone.[184] While the SCA does not restrict ISPs

---

178. *See id.* ("If the government is the seeker, then non-content and content information are both given qualified privacy protection along a sliding scale in which the privacy of content is more closely guarded."); *see also* 18 U.S.C. §§ 2702–2703 (2006) (providing the requirements the government must meet to force disclosure of content and noncontent information).

179. *See* Zwillinger & Genetski, *supra* note 9, at 590 ("If, however, the seeker is a criminal defendant or civil litigant, then content is afforded absolute privacy protection, and non-content is afforded no protection at all."); *see also* 18 U.S.C. § 2702(c)(6) (2006) (allowing a provider to divulge noncontent information to "any person other than a governmental entity").

180. *See* 18 U.S.C. § 2702(b) (2006) (providing the requirements the government must meet to force disclosure of content information).

181. *See* Zwillinger & Genetski, *supra* note 9, at 593 ("[D]efendants may . . . ask the government to intercede and compel disclosure of the communications and then turn them over to defendants upon receipt."). Zwillinger and Genetski note the problems associated with this method: "[A]ny attempt by criminal defendants to enlist the courts to force the government's hand in issuing process raises serious separation of powers issues." *Id.*

182. *Id.* at 590.

183. 18 U.S.C. § 2702 (2006).

184. *See* Zwillinger & Genetski, *supra* note 9, at 590 ("[A]ny benefit to defendant's of the SCA's free pass for disclosures of non-content information has been more or less eroded by voluntary privacy practices of ISPs.").

from divulging noncontent information, the ISPs have self-imposed privacy policies that "promise users the ISP will not disclose their information to any third party absent legal process."[185] As a consequence, in practice, criminal defendants and civil litigants must get a subpoena or court order to get noncontent information—the same limitations imposed on the government.[186] In sum, the government is advantaged when requesting content information, and all parties are on equal footing when requesting noncontent information.

Zwillinger and Genetski propose an amendment[187] that they believe would "harmonize the interest of the criminal defendant, civil litigant, subscriber, and ISP."[188] The proposed showing would be similar to what SCA § 2703(d) requires.[189] This proposed amendment

---

185. *Id.*

186. *See id.* at 591 ("The playing field for non-content information, as a matter of ISP policy, is leveled.").

187. *See id.* at 597–98 (proposing an SCA amendment that provides an exception for civil and criminal litigants). The text of the proposed amendment is as follows:

> A non-governmental entity who is a party to pending criminal or civil litigation may petition the court in which such litigation is pending for an order requiring a service provider to disclose contents of electronic communications in electronic storage or contents of wire or electronic communications in a remote computing service and such order shall issue only if the requesting party can demonstrate that the requested information is relevant and material to the ongoing litigation and is unavailable from other sources, and both the subscriber or customer whose materials are sought and the service provider from whom the materials will be produced are provided reasonable notice and the opportunity to be heard. In the case of a State court, such a court order shall not issue if prohibited by the law of such state. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature, or compliance with such an order would cause an undue burden on such provider. In all cases, the service provider shall be entitled to cost reimbursement by the requesting party, as set forth in 18 U.S.C. § 2706.

Id.

188. *Id.* at 598.

189. *Id.* at 597; *see also* 18 U.S.C. § 2703(d) (2006) ("A court order . . . shall issue only if the governmental entity offers 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.").

has several benefits: it provides notice and an opportunity to be heard to the subscriber and service provider before disclosure, it preserves the ECPA's preference for serving a subpoena on the subscriber or customer before the ISP (or social networking site), and it protects the interests of the ISP (or social networking site) by allowing it to move to quash or modify an order and to recover reasonable costs.[190]

The proposed amendment should be modified slightly. Discovery rules can vary by jurisdiction, and the amendment should account for this. For example, it could include this phrase: "The court issuing an order under this section shall determine relevancy and materiality according to the law of its jurisdiction." Case law can also vary by jurisdiction as to what constitutes an "undue burden" on a service provider, so Congress should add a similar provision regarding the determination of an undue burden.

Returning to our hypothetical, this exception would allow Vanessa to subpoena Facebook for the content of Larry's Facebook profile if she could prove that the information was both relevant and material to her case and unavailable from other sources. Reasonable notice and opportunity to be heard would also have to be given to Larry and Facebook. Facebook would be allowed to move to quash any order that it believed would be an undue burden. Finally, Facebook could get cost reimbursement from Vanessa as the requesting party.

This disclosure exception would give courts and litigants clear standards on what governs a request for information that would otherwise be protected by the SCA. It would also require a party to exhaust other sources of the requested content,[191] thus lessening the burden on service providers. Finally, it would still preserve the privacy of nonparties who are not subject to the information sharing that is required of litigants.

VII. Conclusion

For now, courts must trudge through the 1986 version of the SCA to apply its statutory categories to modern-era social networking sites. Whether social networking sites are acting as an ECS or a RCS

190. Zwillinger & Genetski, *supra* note 9, at 598.

191. *See infra* Part IV (discussing the general discovery of social networking sites).

regarding a user's content, that content should be protected from voluntary disclosure so long as it is not "readily available to the general public."

In reforming the SCA, Congress should collapse the ECS/RCS distinction and include social networking sites within a singular entity definition. This would allow courts to avoid the unnecessary deliberation and confusion that accompanies determining whether a site like Facebook acts as an ECS or a RCS. This would also preserve the functional purposes of the SCA without undermining any of its protections.

Further, without an exception for civil litigants, the SCA has caused unnecessary confusion for courts and parties alike. Congress should include such an exception that allows parties, after exhausting other remedies, to obtain social networking site information that is relevant to the ongoing litigation. Any such exception should allow courts to conform discovery procedures to local rules. As a result, the standards governing disclosure of social networking content would be much clearer for courts and litigants while still preserving SCA privacy protections for nonparties.

Congress seems poised to revamp the SCA in the near future; the legislature would serve the legal system well to bring the SCA out of the technological Stone Age and in line with modern innovations.