Note

Status Update: Adapting the Stored Communications Act to a Modern World

*Jake Vandelist**

The sheer number of electronic communications users is astounding. There were an estimated 2.9 billion email accounts in 2010, and this is expected to rise to 3.8 billion by 2014.[1] In 2012, there were 950 million worldwide active users of Facebook[2] and over 500 million worldwide Twitter users.[3] As a result of the increased number of email and social networking users, the amount of case law involving civil discovery has exploded. In the first six months of 2012, over three hundred published civil opinions substantively involved social media.[4] This number almost certainly understates the volume of cases

* J.D. Candidate 2014, University of Minnesota Law School; B.A. 2011, University of Wisconsin-Madison. Thank you to Professor Bradley Clary, for help in developing this topic; Ed Stockmeyer, Morgan Helme, and Grace Fleming for their insightful edits and advice on this Note; Professor Kristin Hickman for her support of the journal throughout the year; and the board and staff of the *Minnesota Law Review*, for their help in editing this piece and for all of their hard work throughout the year on Volume 98. Many thanks also to my family and friends who have always provided me with unending support.

1. THE RADICATI GRP., INC., EMAIL STATISTICS REPORT, 2010, at 2 (Sara Radicati ed., 2010), *available at* http://www.radicati.com/wp/wp-content/uploads/2010/04/Email-Statistics-Report-2010-2014-Executive-Summary2.pdf.

2. Associated Press, *Number of Active Users at Facebook over the Years*, YAHOO FINANCE (Oct. 23, 2012, 6:04 PM), http://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html.

3. *Twitter Reaches Half a Billion Accounts More than 140 Million in the U.S.*, SEMIOCAST, http://semiocast.com/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US (last visited Feb. 4, 2014).

4. *Published Cases: Involving Social Media Evidence (First Half 2012)*, X1 DISCOVERY, http://www.x1discovery.com/social_media_cases.html (last visited Mar. 10, 2014). These numbers were gleaned from searching "online legal databases of state and federal court decisions across the United States." John Patzakis, *Mid-Year Report: Legal Cases Involving Social Media Rapidly Increasing*, X1 DISCOVERY (July 23, 2012, 3:20 PM), http://blog.x1discovery.com/2012/07/23/mid-year-report-legal-cases-involving-social-media-rapidly-increasing/.

involving social media because only about one percent of all filed cases result in a published decision and many of the published decisions involve fact patterns from as far back as 2008.[5] Accordingly, just as electronic communications have become an important part of everyday life, these communications have also become essential to civil litigation.

The discovery of these electronic communications in civil litigation is governed by, among other things, the Stored Communications Act of 1986 (SCA).[6] The current interpretation of the SCA prevents email and social networking websites from disclosing a user's private messages in civil discovery.[7] This approach limits the amount of available information in civil litigation.[8] As a result, some commentators have advocated for a civil discovery exception to the SCA, allowing email and social networking sites to fully disclose a user's private messages in civil discovery.[9] This approach is consistent with the liberal discovery approach taken by the Federal Rules of Civil Procedure.[10] However, allowing broad discovery of electronic information comes at a cost to both the court and to Internet service providers.[11] Therefore, in considering possible amendments to

5. Patzakis, *supra* note 4.

6. *See generally,* 18 U.S.C. §§ 2701–2712 (2006).

7. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (holding the SCA prohibits civil discovery of any email from an email service provider).

8. *See* Ryan A. Ward, Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J.L. & TECH. 563, 564 (2011) (explaining that users do not have access to all potentially relevant information regarding their social media accounts, however social media sites do have access to this information).

9. *See, e.g.*, Rudolph J. Burshnic, Note, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 WASH. & LEE L. REV. 1259, 1289–93 (2012).

10. The Supreme Court has indicated that FED. R. CIV. P. 26(b)(1), the general discovery provision of the federal rules, "*has been construed broadly* to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 (1978) (emphasis added). Further, since *Oppenheimer* was decided, the federal rules have been broadened to allow discovery regarding any matter "relevant to any party's claim or defense" instead of limiting discovery "relevant to the subject matter involved in the pending action." *Compare* FED. R. CIV. P. 26(b)(1), *with Oppenheimer*, 437 U.S. at 350.

11. See generally, Patzakis, *supra* note 4 and accompanying text for the amount of cases involving social media content. Allowing third party subpoenas in every single one of these cases would place a burden on these Internet service providers and the courts administering these requests.

the SCA legislators must be weigh the importance of broad discovery against the efficiency of obtaining that information.

This Note offers a solution to reconcile the competing values of efficiency and liberal discovery engendered by the SCA.[12] Part I introduces the SCA and its application to private Internet messages. Part II examines the different solutions for addressing the problems posed by the SCA in civil discovery. Finally, Part III recommends legislative reform to promote efficiency in the discovery of private Internet messages. Specifically, this Note proposes that Congress amend the SCA to provide a clearer and more flexible definition for what constitutes protected information and explicitly protect Internet service providers from being required to respond to third party subpoenas in civil suits, but allow such information to be acquired directly through the user.

I. THE STORED COMMUNICATIONS ACT'S APPLICATION TO MODERN CIVIL DISCOVERY

This Part sets out an overview of the SCA and its application to civil discovery. First, this Part will introduce the SCA with a particular focus on the statutory provisions relevant to civil discovery. Next, it will briefly introduce the civil discovery provisions at issue and discuss the application of the SCA to email, social networking sites, and cloud computing services. Then, this Part outlines some judicially created alternatives to obtaining electronic communications in civil discovery. Finally, this Part sets out a framework from which to analyze discovery policy proposals.

A. THE STORED COMMUNICATIONS ACT

The SCA was enacted as Title II of the Electronic Communications Privacy Act (ECPA) of 1986.[13] The purpose of the ECPA was to extend the codification of Fourth Amendment protections to the world of electronic communication and re-

12. Privacy concerns are present during the process of electronic discovery as well. This Note's focus, however, is on the mechanisms of civil discovery and how they affect the information flow of litigation. Volumes have been written about user privacy as it relates to electronic discovery, for example, Rory Bahadur, *Electronic Discovery, Informational Privacy, Facebook and Utopian Civil Justice*, 79 MISS. L.J. 317 (2009), which is outside the scope of this Note.

13. Pub. L. No. 99-508, §§ 201–202, 100 Stat. 1848, 1860–68 (1986) (codified as amended at 18 U.S.C. §§ 2701–2712 (2006)).

mote computing.[14] Congress saw a potential gap in Fourth Amendment protection for information that would traditionally be protected but for it being sent or stored on the Internet or on a third party's computers.[15] Thus, in general, the SCA sought to both limit third party Internet service providers' ability to disclose a user's' information voluntarily[16] and limit the power of government investigators searching for electronic information.[17]

Congress drafted the SCA to reflect the technological landscape of 1986.[18] At this time, Internet users were primarily only able to send and receive electronic mail[19] and upload comments to electronic bulletin boards.[20] Further, some businesses contracted out remote computing for data processing.[21] Accordingly, only two types of Internet service providers are covered by the SCA: electronic communications service (ECS) providers

14. *See* H.R. REP. NO. 99-647, at 16–19 (1986) (describing the purpose of the ECPA as the codification of Fourth Amendment protections for emerging technologies like electronic messaging); S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (identifying the potential lack of Fourth Amendment protections typically provided for personal and business information simply because that information is shared on computers).

15. S. REP. NO. 99-541, at 3 (noting that if electronic information "is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection"). Generally, information sent with or stored on a third party Internet service provider is likely not covered by the Fourth Amendment. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . ."); 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, 1209–10 (2004) (indicating that because an Internet user's communications come into contact with other third party computers the Fourth Amendment does not protect such information).

A thorough analysis of electronic communications and the Fourth Amendment is outside the scope of this Note. This sentence is merely provided to offer a glimpse into the intentions of the legislators behind the ECPA.

16. S. REP. NO. 99-541, at 3 (noting that one of the purposes of the ECPA was to prevent "wrongful use and public disclosure" of information stored electronically with third parties by "unauthorized private parties" indicating that Congress intended to extend privacy protection to the private sphere, beyond its traditional Fourth Amendment confines).

17. Ward, *supra* note 8, at 566.

18. William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1204–05 (2010) (arguing that instead of creating a flexible rule adaptable to changing technology, Congress froze the SCA in 1986).

19. S. REP. NO. 99-541, at 2 (1986).

20. H.R. REP. NO. 99-647, at 22 (1986).

21. *Id.*

and remote computing service (RCS) providers.[22] Notably, the SCA does not cover individuals or service providers that do not qualify as ECS or RCS.[23]

An email provider is a typical example of an ECS.[24] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[25] Electronic communications include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature."[26] Moreover, the only ECS communications protected by the SCA are those held in "electronic storage" by that service.[27] Storage of electronic information can mean temporary or intermediate storage of an "electronic communication incidental" to its electronic transmission or storage of such communication for "backup protection."[28]

An RCS is a provider "of computer storage or processing services by means of an electronic communications system."[29] An "electronic communications system" is facilities and equipment used to transmit electronic communications.[30] The RCS category was meant to include services that performed outsourced data processing.[31]

An ECS or RCS must offer its services to the public.[32] Therefore, while a commercial email service like AOL would be considered offered to the public and therefore able to qualify as an ECS or RCS, an employer's internal email service would not.[33]

22. 18 U.S.C. § 2702(a) (2006).

23. *See id.*; 18 U.S.C. § 2707.

24. Kerr, *supra* note 15, at 1213; Ward, *supra* note 8, at 567.

25. 18 U.S.C. § 2510(15).

26. *Id.* § 2510(12).

27. *Id.* § 2702(a)(1).

28. *Id.* § 2510(17)(A)–(B).

29. *Id.* § 2711(2).

30. *Id*. § 2510(14).

31. *See* H.R. REP. NO. 99-647, at 19, 23 (1986) (explaining the technologies covered by the ECPA, including remote computing services); S. REP. NO. 99-541, at 8, 10–11 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562, 3564–65 (describing the advent of remote computing services in order to fully define the statutory term).

32. *See* 18 U.S.C. § 2702(a)(1)–(3) (prohibiting ECS and RCS entities serving "the public" from disclosing any person's communications to any person, entity, or government).

33. Kerr, *supra* note 15, at 1226. This distinction could exist because nonpublic accounts benefit the providers more than the users or because public providers have less of an incentive to protect a user's privacy rights, however, the legislative intent is unclear as to the distinction. *See id.* at 1226–27. Ac-

If an Internet service provider qualifies as either an ECS or RCS, it may not disclose a user's electronic communications absent a search warrant.[34] Although the SCA creates some statutory exceptions to this rule, there are none that allow an ECS or RCS to disclose a user's information during the course of civil discovery.[35]

However, the SCA only protects the "content" of a user's electronic communications held by ECS and RCS providers.[36] Content is defined by the statute as "any information concerning the substance, purport, or meaning of that communication."[37] In contrast, non-content information is not protected by the SCA.[38] As an illustration, the body of an email is protected by the SCA, whereas the name of the recipient and subject line are not.[39]

Congress did not contemplate how the SCA might apply to civil discovery. The statutory language of the SCA does not mention civil discovery.[40] Similarly, the legislative history of the ECPA is bereft of references to civil discovery.[41] As a result,

cordingly, the relevant portions of the SCA do not apply to nonpublic providers.

34. 18 U.S.C. § 2702(a) (prohibiting ECS and RCS providers from voluntarily disclosing users' information); 18 U.S.C. § 2702(b)–(d) (exempting certain communications from SCA protection); 18 U.S.C. § 2703(a)–(b) (providing certain exceptions for compelled disclosure of users' information held by an ECS or RCS provider).

35. *See* 18 U.S.C. §§ 2701–2711.

36. 18 U.S.C. §§ 2702(a), 2703(a)–(b).

37. 18 U.S.C. § 2510(8).

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

39. Kerr, *supra* note 15, at 1228; *see* H.R. REP. NO. 99-647, at 23 (1986) (clarifying that the records maintained by remote computing services have less protection than the contents of those communications). For a discussion on how traditional Fourth Amendment content and non-content protections apply to new technology, compare Achal Oza, Note, *Amend the ECPA: The Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1049–50 (2008), with David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, at 2229, 2233–39 (2009).

40. *See* 18 U.S.C. §§ 2701–12.

41. *See* H.R. REP. NO. 99-647; S. REP. NO. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555; *Electronic Communications Privacy Act: Hearing Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 1 (1986); *Electronic Communication Privacy: Hearing Before the Subcomm. on Patents, Copyrights, and Trademarks, S. Comm. on the Judiciary*, 99th Cong. 1006 (1985); *1984: Civil Liberties and the National Security State: Hearing Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice, H. Comm. on the Judiciary*, 98th Cong. 1 (1984); *Oversight on Communications Privacy: Hearing Before the Subcomm.*

courts are left with no guidance as to how the SCA applies to civil discovery.

B. CIVIL DISCOVERY

Before analyzing how courts have applied the SCA to civil electronic discovery disputes, it is important to introduce how these cases end up in court. Under the Federal Rules of Civil Procedure, parties can file a Rule 45 subpoena to command a non-party to produce "documents, electronically stored information, or tangible things."[42] These are commonly called subpoenas duces tecum.[43] A subpoena duces tecum is the only tool litigants have to compel nonparties to produce documents in a civil case.[44] The nonparty must produce the documents if they are in that party's "possession, custody, or control."[45] The nonparty can object to the subpoena through a motion to quash or modify the subpoena.[46]

In a typical case where the SCA is implicated in civil discovery, one of the litigants in a civil suit serves a subpoena duces tecum on a company that transmits electronic messages, such as Facebook.[47] Then either the nonparty, or the opposing party through an ex parte motion, files a motion to quash the subpoenas under, among other things, the SCA.[48] The court then applies the SCA to Rule 45 and determines whether it bans discovery of the electronically stored information.

C. APPLICATION OF THE SCA TO CIVIL DISCOVERY

Many courts have determined that the SCA bars civil discovery of a user's electronic communications from an ECS or

on Patents, Copyrights, and Trademarks, S. Comm. on the Judiciary, 98th Cong. 1266 (1984); *Surveillance, Part 2: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice, H. Comm. on the Judiciary*, 94th Cong. 1 (1975); *Surveillance, Part 1: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice, H. Comm. on the Judiciary*, 94th Cong. 675 (1975).

42. FED. R. CIV. P. 45(a)(1)(A)(iii).

43. *See* 9A CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE & PROCEDURE CIVIL § 2451 (3d ed. 2013).

44. *Id.* § 2456.

45. FED. R. CIV. P. 45(a)(1)(A)(iii).

46. *See id.* at 45(c)(3).

47. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 969 (C.D. Cal. 2010).

48. *See, e.g.*, *id.* at 969–70.

RCS.[49] Most of these courts prohibit such discovery because there is no exception to the SCA allowing ECS or RCS providers to disclose a user's information pursuant to a civil discovery request and because there is no congressional intent indicating otherwise.[50] Therefore, courts are forced to classify Internet service providers within the ECS or RCS categories in order to determine whether the SCA prohibits civil discovery requests served directly upon Internet service providers. Due to the immensity of technological change since 1986, it has been no easy task applying the SCA to current technology.[51] Making this more complicated, some courts have held that a single service must be either an ECS or an RCS, but others have held that a single service can qualify as both an ECS and an RCS.[52]

The SCA traditionally has been interpreted to cover email providers. Courts have more recently applied the SCA to social networking sites. However, the new technology challenging the boundaries of SCA protection is cloud computing.

1. Email Providers

Courts agree that commercial email service providers, in general, are considered ECS providers under the SCA.[53] Specifically, it is generally understood that unopened emails are protected under the SCA.[54] This is because the email communications are in "temporary, intermediate storage" incidental to their transmission.[55] However, much disagreement exists over

49. *See, e.g.*, Bower v. Bower, 808 F. Supp. 2d 348, 349–51 (D. Mass. 2011); In re Subpoena Duces Tecum to AOL, LLC., 550 F. Supp. 2d 606, 611 (E.D. Va. 2008); O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 89 (Ct. App. 2006); Fed. Trade Comm'n v. Netscape Commc'ns Corp., 196 F.R.D. 559, 561 (N.D. Cal. 2000).

50. *See, e.g.*, *Netscape*, 196 F.R.D. at 561.

51. For example, in Crispin, the court labored over fifteen pages to determine the applicability of the ECS and RCS categories to email and social networking sites. 717 F. Supp. 2d at 976–91.

52. *Compare* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902–03 (9th Cir. 2008) (holding that a service provider can only be either an ECS or an RCS), *with* Flagg v. City of Detroit, 252 F.R.D. 346, 362 (E.D. Mich. 2008) (holding that a service provider can be both an ECS and RCS).

53. *See, e.g.*, *Quon*, 529 F.3d at 902–03 (9th Cir. 2008); United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005); Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); *Bower*, 808 F. Supp. 2d at 349 (D. Mass. 2011).

54. *See, e.g.*, *Quon*, 529 F.3d at 902–03; *Theofel*, 359 F.3d at 1077; United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009); Jennings v. Jennings, 736 S.E.2d 242, 246 (S.C. 2012).

55. *Theofel*, 359 F.3d at 1075 (quoting 18 U.S.C. § 2510(17)(A)(2012)); *accord Councilman*, 418 F.3d at 72–79 (holding, after considering the text and

whether an opened email is considered to be in "electronic storage" and thus protected from civil discovery by the SCA.[56]

Those arguing that opened emails should be considered to be held in backup storage indicate that emails left on a commercial email provider's servers, after a user downloads the message onto her computer, are left there for backup reasons.[57] The principal rebuttal to this argument is that the backup provision definition of electronic storage should be narrowly interpreted as merely closing an "end-run" loophole around ECS protections without which Internet service providers could disclose unopened backup copies created incident to transmission.[58] However, some of the courts that have held opened messages do not fit within the ECS category have suggested those same messages might constitute RCS content.[59]

2. Social Networking Sites

Crispin v. Christian Audigier, Inc. was the first published case to apply the SCA to social media sites.[60] The defendants

legislative history of the ECPA, that unread emails were meant to be protected under the SCA).

56. *Compare*, *e.g.*, *Theofel*, 359 F.3d at 1077 ("[W]e think that prior access is irrelevant to whether the messages at issue were in electronic storage."), *and* Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (holding that there is no difference between unopened and opened emails under the SCA), *with Weaver*, 636 F. Supp. 2d at 771 (noting that read emails have already been transmitted and are not stored for backup purposes, and are therefore unprotected), *and* 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, 580 (2007) ("[T]he *Theofel* court's analysis is somewhat tortured.").

57. *See, e.g.*, *Theofel*, 359 F.3d at 1075 ("An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message . . . ."); *cf. Quon*, 529 F.3d at 902–03 (holding that a text message service provider who permanently archived text messages on its servers was an ECS because these were archived for backup reasons).

58. Kerr, *supra* note 15, at 1217 n.61; *cf. Jennings*, 736 S.E.2d 242, 245 ("We question the reasoning expressed in Theofel that such passive inaction can constitute storage for backup protection under the SCA . . . .").

59. *See, e.g.*, *Weaver*, 636 F. Supp. 2d at 772 (indicating that Hotmail was storing messages on a web-based email service "solely for the purpose of providing storage or computer processing services to such subscriber or customer" (quoting 18 U.S.C. § 2703(b)(2)(2012))); *Jennings*, 736 S.E.2d 242, 247 n.3 (Toal, C.J., concurring) (noting that because an Internet service provider can act as both an ECS and RCS, it might be the case that an email stored on a web-based email system is protected under the RCS category).

60. 717 F. Supp. 2d 965, 977 (C.D. Cal. 2010) ("Although some courts have considered the SCA's application to certain types of providers, none appears to

served subpoenas duces tecum on Facebook and Myspace seeking communications between the plaintiff and the defendant.[61] The plaintiff filed a motion to quash the subpoenas, arguing that the subpoenas were in violation of the SCA.[62] The court first concluded that any private messaging on the social networking sites is protected from civil discovery under the ECS category, similar to emails.[63] Further, the court analogized postings to a user's Facebook wall or Myspace comments to the restricted electronic bulletin board systems which Congress intended to protect under the SCA.[64] Therefore, it held that this content renders Facebook and Myspace ECS providers, at least to the extent that a Facebook or Myspace user restricts access to his or her profile.[65] In the alternative, the court held that this content could also be considered an RCS service because the communications were placed on the sites for storage purposes.[66] However, by implication, any Facebook wall postings or Myspace comments generally available to the public would not be protected by the SCA.[67]

Similarly, *Viacom International Inc. v. Youtube Inc.* held that an online service provider, YouTube, could not disclose a user's private videos uploaded to the site in the course of civil discovery because such information was protected under the RCS designation of the SCA.[68] Without elaboration the court indicated that YouTube qualified as an RCS because it provided "remote computing service to the public."[69]

3. Cloud Computing

There are no published cases available involving the SCA's application to cloud computing within the realm of civil discovery. However, the entire field of computer processing is starting to shift to cloud computing.[70] Therefore, once again, courts will

have addressed whether social-networking sites fall within the ambit of the statute.").

61. *Id.* at 968–69.
62. *Id.* at 969.
63. *Id.* at 980.
64. *Id.* at 981–89.
65. *Id.*
66. *Id.* at 990.
67. *See id.* at 991.
68. 253 F.R.D. 256, 264 (S.D.N.Y. 2008).
69. *Id.*
70. *See* Robison, *supra* note 18, at 1199–1200 (describing "the era of cloud computing").

have to apply the ECS and RCS definitions to new technology. Some suggest that cloud technology providers will not qualify as ECS because "many of today's popular cloud computing services are designed for purposes other than communication, such as word processing."[71]

Some also suggest that cloud providers do not qualify as RCS providers because many providers make revenue through "contextual advertising."[72] This means the service providers release customer' information to third-party advertising companies in order to facilitate tailored advertising.[73] It is possible this violates the RCS requirement that "'storage or computer processing' be the sole reason that a customer transmits her data to the cloud provider."[74]

Current case law prohibits Internet service providers from disclosing a user's private communications in the course of civil discovery due to the SCA. However, as use of social media becomes more integrated in our daily lives, the SCA's application to civil discovery will become increasingly important.

D. ALTERNATIVES TO THE SCA IN CIVIL DISCOVERY

Serving a subpoena on a third party Internet service provider is not the only way electronic information can be discovered in civil cases. Some courts have elected to ignore the SCA completely. And other courts have required parties to serve discovery requests on the user instead of on the service provider.

1. Ignore the SCA

There are at least two cases in which courts have ignored the SCA's application to civil discovery and allowed civil discovery subpoenas to be served directly upon Facebook and Myspace.[75] Commentators have criticized these opinions for rendering decisions in discord with federal law.[76]

71. *Id.* at 1209.

72. *Id.* at 1213–14.

73. *Id.*

74. *Id.* at 1214. *But see ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties, H. Comm. on the Judiciary*, 111th Cong. 144–45 (2010) (statement of Microsoft Corporation) (indicating that it views any cloud technologies that allow for collaboration or interaction between users as ECS, and any time the purpose of a program is to provide access to an application or remote storage of content it considers that program as an RCS).

75. *See* Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009); Romano v. Steelcase Inc., 907

In *Ledbetter v. Wal-Mart Stores, Inc.*, the court allowed a subpoena to be served by the defendant upon Facebook, Myspace, and Meetup.com for any relevant communications by the plaintiff.[77] Even though the application of the SCA was debated in the parties' briefs,[78] in a two-page opinion, the court did not address the SCA at all and merely concluded that the information "is reasonably calculated to lead to the discovery of admissible evidence."[79]

Similarly, in *Romano v. Steelcase Inc.*, the court granted the defendant's subpoena upon Facebook and Myspace seeking access to the plaintiff's accounts and deleted information.[80] At the outset of the opinion the court noted that it had considered the SCA's application to the discovery requests at issue.[81] However, that is the only mention of the SCA throughout the entire opinion.[82] In granting the subpoenas, the court only substantively considered whether New York's civil discovery rules permitted the broad scope of discovery and whether the plaintiff had Fourth Amendment protection of her social media posts.[83]

2. Serve Discovery Request upon the User, not the Provider

As noted above, the SCA does not apply to individuals.[84] Therefore individuals can disclose any information traditionally covered by the SCA.[85] Many courts have taken advantage of this exception to SCA protection and required the user of the Internet service provider to produce information instead of di-

N.Y.S.2d 650 (Sup. Ct. 2010).

76. *See, e.g.*, Ward, *supra* note 8, at 577.

77. *Ledbetter*, 2009 WL1067018, at *2.

78. Defendant Wal-Mart Stores, Inc.'s Motion to Compel Production of Content of Social Networking Sites, *Ledbetter*, 2009 WL 1067018, 2009 WL3061763, at *4–5; Plaintiffs' Response in Opposition to Defendant Wal-Mart's Motion to Compel Production of Content of Social Networking Sites, *Ledbetter*, 2009 WL 1067018, 2009 WL 3061764 at *9; Wal-Mart's Reply in Support of Its Motion to Compel Production of Content of Social Networking Sites, *Ledbetter*, 2009 WL 1067018, 2009 WL 3061765, at *2.

79. *Ledbetter*, 2009 WL 1067018, at *2.

80. *Romano*, 907 N.Y.S.2d at 657.

81. *Id.* at 652.

82. *See id. passim*.

83. *See id.* at 652–57.

84. *See supra* text accompanying note 23.

85. *See, e.g.*, 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.").

recting subpoenas upon the service providers.[86] Most of these courts recognize that the SCA most likely prohibits any requests directly on the Internet service providers and explicitly recognize they are bypassing these restrictions.[87]

E. COMPETING VALUES: EFFICIENCY AND LIBERAL DISCOVERY

Before identifying and analyzing the proposed modifications to the SCA, it is necessary to consider the policy choices at stake. Any change in discovery rules implicates the competing values of efficiency and liberal discovery.[88] Liberal discovery does not mean complete and errorless discovery, as this is impossible.[89] Additionally, it is a waste of social resources, both in terms of economics and time, to attempt to discover and analyze every shred of evidence that might be relevant to a particular case.[90]

The Federal Rules of Civil Procedure reflect this reality in the very first rule, identifying that all of the rules should be interpreted in order to "secure the just, speedy, and inexpensive determination of every action and proceeding."[91] Similarly, the

86. *See, e.g.*, Glazer v. Fireman's Fund Ins. Co., 2012 WL 1197167, at *3 (S.D.N.Y. April 5, 2012); In re Air Crash near Clarence Center, New York, on February 12, 2009, 2011 WL 6370189, at *6 (W.D.N.Y. Dec. 20, 2011); EEOC v. Simply Storage Mgmt. Servs., 270 F.R.D. 430, 434 (S.D. Ind. 2010); Flagg v. City of Detroit, 252 F.R.D. 346, 359 (E.D. Mich. 2008); Mackelprang v. Fidelity Nat'l Title Agency of Nev., No. 2:06-CV-00788-JCM-GWF, 2007 WL 119149, at *6 (D. Nev. Jan. 9, 2007); Largent v. Reed, No. 2009-1823, 2011 WL 5632688, at *6–7 (Pa. Ct. C.P. Nov. 8, 2011). *But cf.* J.T. Shannon Lumber Co. v. Gilco Lumber Inc., 2008 WL 4755370, at *1 (N.D. Miss. Oct. 29, 2008) (holding that allowing a court to compel a defendant to consent to release information protected by the SCA would be an "end run around the [SCA]," though hinting that the plaintiff could serve a discovery request directly on the defendant to obtain the protected information).

87. *See, e.g.*, *Glazer*, 2012 WL 1197167, at *3 (requiring the plaintiff to produce electronically stored information in order to bypass SCA issues); *Mackelprang*, 2007 WL 119149, at *8 ("The proper method for obtaining such information, however, is to serve upon Plaintiff limited requests for production of *relevant* [Myspace] communications.").

88. *Compare* Richard L. Marcus, *Discovery Containment Redux*, 39 B.C. L. REV. 747, 749 (1998) (lauding the benefits of broad discovery measures), *with* James S. Kakalik et al., *Just, Speedy, and Inexpensive? An Evaluation of Judicial Case Management Under the Civil Justice Reform Act*, 49 ALA. L. REV. 17, 17 (1997) (identifying the perils of inefficient discovery).

89. *See* Robert G. Bone, *Improving Rule 1: A Master Rule for the Federal Rules*, 87 DENV. U. L. REV. 287, 302 (2010) (stating that in discovery "perfect accuracy is impossible").

90. *Id.*

91. FED. R. CIV. P. 1.

rules explicitly reject complete and errorless discovery for electronic information, providing that parties do not have to produce electronic information that would result in "undue burden or cost."[92] Therefore, the policy battle between liberal discovery and efficiency is not waged at the extremes. Rather, the ongoing argument is within the bounds of the current rules and how broadly or narrowly the discovery provisions should be interpreted.[93]

Those arguing for a broad interpretation of the federal discovery provisions prioritize "just" over "speedy" and "inexpensive" in rule one.[94] These scholars point to the benefits liberal discovery has provided to the justice system since its introduction in 1938.[95] For example, some argue that liberal discovery rules have expanded substantive law in areas where it is often hard to prove claims, such as disparate treatment cases.[96] Moreover, broad discovery is an important procedural mechanism available because it informs all parties of the merits of controversies and therefore allows for the "administration of justice."[97]

In contrast, those arguing for efficient discovery emphasize that "just" outcomes are only available if litigation is "speedy" and "inexpensive."[98] Congress endorsed this position when it enacted the Civil Justice Reform Act of 1990, which was rooted in the concern that civil litigants were denied access to justice due to inefficiencies and delay of the courts as a result of the

92. FED. R. CIV. P. 26(b)(2)(B).

93. *See* Bone, *supra* note 89, at 300 (explaining that judges have broad discretion to interpret Fed. R. Civ. P. 1 as a broadening or narrowing provision of the rest of the Federal Rules).

94. *Cf. id.* at 293–95 (noting that pre-1970's judges applied rule one to "to support liberal interpretations of the discovery rules").

95. *See, e.g.*, Stephen N. Subrin, *Fishing Expeditions Allowed: The Historical Background of the 1938 Federal Discovery Rules*, 39 B.C. L. REV. 691, 697 (1998) (holding that liberal discovery has largely eliminated situations where "the merits of controversies are imperfectly understood by the parties, are inadequately presented to the courts, and too often fail to exert a controlling influence upon the final judgment").

96. Marcus, *supra* note 88, at 749–52.

97. Subrin, *supra* note 95, at 697; *see also* Geoffrey C. Hazard, Jr., *Discovery Vices and Trans-Substantive Virtues in the Federal Rules of Civil Procedure*, 137 U. PA. L. REV. 2237, 2239 (1989) ("[B]road access to document repositories is the most powerful weapon in the Rules discovery armory . . . .").

98. *E.g.*, Bone, *supra* note 89, at 299 ("Sometimes . . . judges emphasize Rule 1's reference to 'speedy' and 'inexpensive,' but sometimes they focus on achieving 'just' determinations, arguing that a party's fear of excessive cost and delay can impede court access and produce unjust outcomes.").

Federal Rules of Civil Procedure.[99] These scholars argue the introduction of mass quantities of electronically stored information has furthered the need to focus on efficiency because parties "cannot reasonably expect to obtain all electronically stored information" through discovery when there are terabytes of possibly relevant information available.[100]

* * *

The current interpretation of the SCA in civil discovery is an outmoded application of an outdated law. It does not correctly balance the values of efficiency and liberal discovery. In recognition of its failures, many commentators have proposed modifications to the SCA.

II. PROPOSED MODIFICATIONS TO THE SCA

Due to the anachronistic ECS and RCS definitions, the inconsistency of SCA application, and general uncertainty that the SCA has engendered in civil discovery, there have been many proposed modifications to the current application of the SCA. Each of these modifications should be analyzed to determine whether they strike the correct balance between efficiency and justice. The first proposed modification would have courts apply the Federal Rules of Civil Discovery and then correctly apply the SCA. The second proposed modification would simplify ECS and RCS categories. Finally, a proposed civil discovery exception would eviscerate SCA protection for civil litigants. None of these approaches strikes the right balance between efficiency and justice.

A. RETAIN THE STATUS QUO

One proposed modification to the SCA is not a modification at all, but merely a continuance of the status quo.[101] Under this approach, courts should first apply the Federal Rules of Civil Procedure to screen civil discovery subpoenas seeking infor-

99. Kakalik et al., *supra* note 88, at 17.

100. *See* Mia Mazza et al., *In Pursuit of FRCP 1: Creative Approaches to Cutting and Shifting the Costs of Discovery of Electronically Stored Information*, 13 RICH. J.L. & TECH. 11, 85 (2007) ("The days when the requesting party can expect to 'get it all' and the producing party to produce whatever they feel like producing are long gone." (quoting *Hopson v. Mayor & City Council of Balt.*, 232 F.R.D. 228, 245 (D. Md. 2005))).

101. *See* Ward, *supra* note 8, at 581–88.

mation from Internet service providers for overbreadth and admissibility.[102] Then, courts should apply the SCA to determine whether the service providers qualify for ECS or RCS protection.[103] This modification is both unjust and inefficient within the meaning of rule one.

The status quo approach does not satisfy the "just" requirement of rule one for two reasons. First, the current approach does not allow for full and complete discovery of information stored online because the SCA protects any information that qualifies as ECS or RCS from civil discovery with no exception.[104] Although some of this information is available through the user,[105] users can only supply screenshots of their content, which are not searchable by the requesting party, and users often do not have access to their deleted data.[106] Thus, there is a portion of information that is wholly undiscoverable in civil litigation regardless of its importance to the claims or defenses at issue. As a result, the status quo could create a situation where the merits of a controversy would be "imperfectly understood" and "inadequately presented to the court[]."[107] This is the precise situation rule one's "just" requirement and Rule twenty-six's liberal discovery provisions were designed to avoid.[108]

Second, one of the foundations of the American legal system is consistent adjudication for similarly situated parties.[109]

102. *Id.* at 582–84. Under the rules, a discovery request must be "relevant to any party's claim or defense" and must be "reasonably calculated to lead to the discovery of admissible evidence." FED. R. CIV. P. 26(b)(1).

103. Ward, *supra* note 8, at 584–88.

104. *See supra* notes 34–35 and accompanying text.

105. *See supra* Part I.C.2.

106. *See* Ward, *supra* note 8, at 564.

107. Subrin, *supra* note 95, at 697.

108. *See supra* notes 94–97 and accompanying text.

109. William O. Douglas, *Stare Decisis*, 49 COLUM. L. REV. 735, 736 (1949) ("[T]here will be no equal justice under law if a negligence rule is applied in the morning but not in the afternoon."); Christopher J. Peters, *Foolish Consistency: On Equality, Integrity, and Justice in Stare Decisis*, 105 YALE L.J. 2031, 2039 (1996) ("Such justifications of stare decisis include the notions that the rule allows for advantageous predictability in the ordering of private conduct, that it promotes the necessary perception that law is stable and relatively unchanging, that it prevents frustration of private expectations, that it serves the resource-saving goal of judicial efficiency, and even that it preserves the separation of powers by enforcing judicial restraint."); Justice Antonin Scalia, *The Rule of Law as a Law of Rules*, 56 U. CHI. L. REV. 1175, 1178 (1989) ("[O]ne of the most substantial . . . competing values [in adjudication], which often contradicts the search for perfection, is the appearance of equal

This foundation is upheld through liberal discovery rules that reduce the uncertainty of judicial outcomes.[110] However, the current judicial interpretation of the SCA applies its protection inconsistently across similarly situated parties when they are seeking to discover email communications, and some courts even refuse to apply its protections at all.[111] Consistent adjudication is not ensured through consistent liberal discovery in a system that inconsistently admits electronically stored information.

Additionally, the current application of the SCA is inefficient for two reasons, both of which result from out of date ECS and RCS definitions.[112] First, judges have to jump through analytical hoops to apply the anachronistic ECS and RCS definitions to current technology.[113] Judicial wrangling with the SCA's definitions in civil discovery diverts the attention of judges from deciding on the merits of the cases before them to applying obsolete definitions to new technology in order to determine whether a piece of information is to be protected from civil discovery. This unnecessarily delays the adjudication of cases because judges are forced to rule on these protective orders before even considering the merits of the case.[114]

treatment. As a motivating force of the human spirit, that value cannot be overestimated.").

110. *See* Subrin, *supra* note 95, at 697 ("[A] large part of the uncertainty in the outcome [of trials] result[s] from the want of information on the part of litigants and their counsel as to the real nature of the respective claims and the facts upon which they rest" (quoting Edson Sunderland, *Foreword* to GEORGE RAGLAND JR., DISCOVERY BEFORE TRIAL iii (1932))).

111. *See supra* Parts I.B, I.C.1.

112. *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties, H. Comm. on the Judiciary*, 111th Cong. 21, 139–40 (2010) (statement of Richard Salgado, Law Enforcement and Security Counsel, Google Inc.) (arguing that the ECPA is out of date and has thus resulted in much confusion as to what is protected and what is not and noting that Gmail is at times an ECS, at times an RCS, but as for everything else was "largely unanticipated in 1986 when ECPA was passed, and determining whether a particular piece of information held by Google for any one of those services is held as an ECS or RCS is no trivial task"); *id.* at 143 (Response to post hearing questions from Mike Hintze, Assoc. Gen. Counsel, Microsoft Corporation) ("Technology has changed drastically since ECPA was enacted in 1986. It was not possible at that time to contemplate the manner and extent of the changes that have occurred in the 24 years since the ECS and RCS definitions were drafted. Technological changes, coupled with the rather ambiguous definitions, create significant challenges for online service providers in determining the appropriate classification for their services.").

113. *See supra* note 51 and accompanying text.

114. *E.g.*, In re Subpoena Duces Tecum to AOL, LLC., 550 F. Supp. 2d 606,

Second, the uncertainty surrounding the SCA's application to civil discovery has diverted social resources away from service providers' income-producing lines of business to the legal departments. While not necessarily inefficient within the meaning of rule one, it misallocates economic resources. This diversion takes place because service providers are unsure as to what they can disclose and what they must protect, especially with new technologies like cloud computing.[115] The diversion of resources also occurs when judges grant third party subpoenas to obtain a user's information from Internet service providers.[116]

The advocates of this approach alleged that it is a "uniform approach to discovery requests" for electronically stored information.[117] Also, these proponents argue that applying the rules first will quash many third party subpoenas before the SCA issues are even considered.[118] As noted above, many of the current problems with the SCA's application to civil discovery are a result of the inconsistent and complicated application to new technology; thus, a uniform approach to discovery requests of electronically stored information is something to strive for. However, both of these alleged benefits avoid the root problems of the SCA. It does not take into account the reduction of available information in discovery or the inefficiencies it engenders in the judicial process and the overall economy. Therefore, a more holistic solution should strive for uniformity of application to electronic civil discovery requests, like this proposed solution, but it must also attempt to eradicate the underlying issues with the SCA.

611 (E.D. Va. 2008).

115. *E.g.*, *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties, H. Comm. on the Judiciary*, 111th Cong. 21, 139–40 (2010) (Response to post hearing questions from Richard Salgado, Law Enforcement and Security Counsel, Google Inc.) (arguing that Gmail can be both an ECS and an RCS at different times, but most current technology could not have been anticipated by the 1986 ECPA); *id.* at 143–45 (Response to post hearing questions from Mike Hintze, Assoc. Gen. Counsel, Microsoft Corporation) (describing the complicated, confusing, and laborious process for determining whether technologies like geolocation, social networking, and online calendars qualify for ECS or RCS protection).

116. *Cf.* Kakalik et al., *supra* note 88, at 30 (explaining the costs of early case management).

117. Ward, *supra* note 8, at 581.

118. *See id.* at 582–84.

B. COLLAPSE THE ECS AND RCS DISTINCTION

In order to remedy the inconsistencies that result from the archaic ECS and RCS definitions, some suggest collapsing the two categories into one.[119] This remedy would eliminate the distinction between service providers and instead shift the focus to whether individual files are protected.[120] Under this reform, the SCA would apply to all "network service providers" but keep the ECS and RCS distinction for files in order to preserve the differing legal standards for criminal investigations.[121] One commentator further suggests that social networking sites should be explicitly included in the definition of "network service provider" in accordance with the *Crispin* decision.[122]

This modification to the SCA makes important strides towards justice and efficiency in the discovery of information stored online. Providing a more general and flexible definition for Internet service providers will simplify the statute and reduce confusion as to which providers are covered under the current ECS and RCS definitions.[123] This broad definition is important going forward because it is flexible enough to cover a broad range of developing technologies, such as cloud computing.[124] Providing clarity of coverage to courts will increase efficiency during the discovery process[125] and also produce more consistent protections across media platforms.[126]

However, this remedy is no panacea. It still retains the outdated ECS and RCS definitions for civil discovery purposes, merely shifting the focus from service providers to files.[127] As stated above, retaining these definitions, in general, would re-

119. *See* Kerr, *supra* note 15, at 1235; Burshnic, *supra* note 9, at 1288–89.

120. Kerr, *supra* note 15, at 1235; Burshnic, *supra* note 9, at 1288–89.

121. Kerr, *supra* note 15, at 1235; Burshnic, *supra* note 9, at 1288–89. For an explanation of how the ECPA applies to criminal investigations, see generally Kerr, *supra* note 15, at 1218–33.

122. Burshnic, *supra* note 9, at 1288; *see also supra* text accompanying notes 60–67.

123. *See* Kerr, *supra* note 15, at 1235; Burshnic, *supra* note 9, at 1288–89.

124. For an explanation of the problems the ECS and RCS categories pose for cloud providers, see Part I.B.3.

125. *See* Burshnic, *supra* note 9, at 1288 ("It would also promote judicial economy; courts, like the one in *Crispin*, would no longer have to unnecessarily labor over the ECS/RCS distinction.").

126. *See* Kerr, *supra* note 15, at 1233 (explaining that the Ninth Circuit's interpretation of the ECS and RCS categories is in conflict with the traditional understanding of the two categories and that simplification of the definition is necessary to remedy this conflict).

127. *See* Burshnic, *supra* note 9, at 1288–89.

sult in unjust outcomes due to the limitations on liberal discovery and inconsistent outcomes and would increase judicial and economic inefficiencies.[128] Therefore, it does not effectively reform the confusion that the definitions engender.

Moreover, adding social networking sites to the definition of a "network service provider" would repeat the same mistakes of the current ECPA, namely that it would codify privacy protections based on the technological landscape of today instead of drafting a broad and flexible rule to apply to present and future technology.[129] Some might say that this argument could attach to any legislation regulating technology; in other words, any legislation written today could be rendered outdated by developments in technology.[130] While it is true that any law written today is hampered by our present assumptions regarding technology, the more narrow the definition as to what is protected by the SCA, the more likely it is to become outdated. For example, if Internet users stopped using social networking sites, just like users stopped using electronic bulletin boards, this part of the definition would be rendered obsolete. But if the definition included all Internet service providers, the definition would only be rendered obsolete if people stopped using the Internet. Thus, while this remedy makes significant strides, it falls short of breaking through the shackles of the 1986 ECS and RCS definitions.

C. PROVIDE A CIVIL DISCOVERY EXCEPTION

A more holistic change to the SCA would be to add a civil discovery exception thereby permitting subpoenas to be served directly upon Internet service providers.[131] Under this approach, proposed by Professors Zwillinger and Genetski, a civil litigant could petition the court to disclose the information protected by the SCA by showing it is relevant and unavailable from other sources.[132] If the request is granted, the court would give the service provider notice and an opportunity to "quash or

128. *See supra* notes 104–16 and accompanying text.

129. For an explanation of the technological landscape of 1986, see *supra* notes 18–21 and accompanying text.

130. *See, e.g.*, Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239, 275 (2007) (describing that "future-proofing" technology is difficult because "the path of technological change is clouded in mystery").

131. *See* Zwillinger & Genetski, *supra* note 56, at 597–98; Burshnic, *supra* note 9, at 1289–92.

132. Zwillinger & Genetski, *supra* note 56, at 597.

modify" the order if the information sought "would cause an undue burden on such provider."[133] If the order is granted, the service provider is entitled to cost reimbursement incurred through the production from the requesting party.[134]

This approach provides for more liberal discovery and therefore satisfies the interests of justice in rule one. It allows civil litigants the opportunity to discover all relevant electronic information by lifting the veil of SCA protection. For instance, if a user did not have access to relevant information because the user deleted it or deactivated her account, this procedural amendment would allow such information to be discovered from the service provider. In some lawsuits, such information could be essential to merits of the controversy and to the "administration of justice."[135]

This proposal, however, fails to remedy the ECS and RCS definitions and therefore will result in inconsistent application of the cost-shifting burden explained above.[136] The question of whether electronically stored information is covered by these proposed procedures is still subject to the outdated ECS and RCS definitions that create unjustly inconsistent outcomes and judicial and economic inefficiency.[137]

Still, as a general matter this modification strikes a reasonable balance between justice and efficiency because of its cost-shifting mechanism. Typically, the responding party pays for any production costs related to discovery.[138] Thus, it is likely if there was a wholesale discovery exception to the SCA with no statutory requirement to cost-shift, the responding party would have to pay for the service provider's production expenses.[139] There are some procedures that would allow the responding party to cost-shift for the production of electronically stored in-

133. *Id.* at 598.

134. *Id.*

135. Subrin, *supra* note 95, at 697. *But see* Mazza, *supra* note 100, at 98 ("[D]ecisions on motions regarding who will be required to pay for discovery responses (the cost of which may run into the hundreds of thousands, if not tens of millions, of dollars) can impact severely how an action proceeds and in fact may be outcome-determinative in some cases.").

136. *See* Zwillinger & Genetski, *supra* note 56, *passim*.

137. *See supra* notes 104–16 and accompanying text.

138. *See* Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978) ("[T]he presumption is that the responding party must bear the expense of complying with discovery requests . . . .").

139. *See id. But see* FED. R. CIV. P. 26(b)(2)(B) (providing that parties need not produce electronic information that would result in "undue burden or cost").

formation that is "not reasonably accessible because of undue burden or cost," though the specifics of cost-shifting rules are jurisdiction-specific and constantly in flux, and it is unclear if such information would qualify under these standards.[140] Consequently, if there were a civil discovery exception that didn't require cost-shifting, requesting parties would likely always request information directly from the social networking site because they have an incentive to gather complete information and no economic disincentive.[141] This proposed modification would allow complete discovery of electronic information only when a requesting party believes the information likely to be produced outweighs the cost. This will necessarily reduce unnecessary litigation costs.

* * *

While none of the proposals above strike the right equilibrium between justice and efficiency, there are features of each proposal that can be incorporated into a balanced solution to amend the SCA. Any amendment to the SCA should attempt to create a uniform approach to requesting electronically stored information in civil discovery. Further, broadening the category of information covered by the SCA will reduce current confusion as to what information is covered and help ensure the legislation is not rendered obsolete through future changes in technology. Finally, providing a cost-shifting provision for information that is difficult to reach would strike the right balance between justice and efficiency.

III. A BALANCED PROPOSAL TO AMEND THE SCA

As evidenced by the problems with the status quo, the SCA needs to be amended in order to provide consistent application across current and future technologies. In order to render SCA protection in civil discovery explicit and not merely implied, legislators should amend the SCA to contain a civil discovery provision that incorporates three features. First, this provision

140. FED. R. CIV. P. 26(b)(2)(B); *see also* Mazza, *supra* note 100, at 99 ("[T]he law on shifting the cost of producing ESI remains jurisdiction-specific, often unsettled, sometimes conflicting, and continually evolving.").

141. For example, in disparate treatment cases often plaintiffs must find evidence of a "smoking gun" in order to prove liability, which incentivizes plaintiffs to obtain as much information as possible. *See* Marcus, *supra* note 88, at 749–50.

ought to include a broad definition of protected information in order to reduce judicial and economic inefficiencies. Second, the amendment should retain and codify the user exception. Third, the amendment should allow for information rendered inaccessible by the SCA to be discovered through the service provider if the requesting party pays the responding party's costs. Such an amendment would satisfy both the interests of justice and efficiency.

A. BROADEN THE DEFINITION OF PROTECTED INFORMATION

Enlarging the scope of SCA protection through a broader definition of protected information will increase efficiency in the discovery of information stored online. The current ECS and RCS definitions are obsolete and result in judicial and economic inefficiencies.[142] The problem with the current definitions is that they were written to reflect the technological landscape of the day and not drawn broadly to adapt to new technologies.[143] The proposal to collapse the ECS and RCS is limited by the fact that it merely transfers the outmoded definitions to files.[144] To avoid this pitfall, a broad catchall definition should be drafted for electronic information stored on the Internet.

The categories of ECS and RCS providers should be abandoned in favor of a single network service provider category.[145] Under the SCA, the definition of a "network service provider" should be broad enough to encompass all present and future technologies that transmit information over the Internet. The statutory definition of a "network service provider" should be any Internet service provider that provides services to users. There should also be a note of statutory interpretation in the statute that makes clear that this definition is to be broadly construed. The broad definition coupled with this note of statutory interpretation will encompass all present and foreseeable future Internet service providers.

This definition of a network service provider is admittedly broad and somewhat vague. However, this is by design. A broad definition of what is covered will allow the SCA's new civil discovery provision to adapt to the changing technological tides

142. *See supra* notes 113–30 and accompanying text.

143. *See supra* notes 18–23, 51, 112 and accompanying text.

144. *See supra* Part II.B.

145. This is the same approach advocated for by Orin Kerr and Rudolph Burshnic. *See* Kerr, *supra* note 15, at 1235; Burshnic, *supra* note 9, at 1288–89.

and will avoid the current problem of fitting new technologies into old definitions. Also, the definition should not include a list of examples as to what is covered because then the statute would fall prey to the doctrine of *noscitur a sociis*.[146] This canon of construction interprets a general word to be read in accordance with the specific terms listed in a series.[147] Thus, the practical effect of including a list of electronic communications covered by the civil discovery amendment would be to lock the definition into the technologies of today instead of allowing it to adapt to the technologies of tomorrow.

Cloud computing provides an illustrative example of how this new definition would work. If a user, Joe Briefcase,[148] performed most of his computing in an Internet cloud provided by Microsoft (e.g., word processing, spreadsheets, email communications) Microsoft would be completely covered by the new definition of "network service provider" because it is providing services to Joe Briefcase. This is true even if Joe stores some of this information on his computer's hard drive because the manner in which Joe stores his information does not change the fact that Microsoft is providing him Internet services. Also, this is a moot point due to the user exception to be discussed below. If Joe stores his information locally on his computer, discovery can be requested through him and not Microsoft.

In addition to broadening the definition of what service providers are covered, the new statute should abolish the current statute's heightened protection for service providers that offer their services to the public.[149] There is no legislative history in support of this distinction[150] and the two proffered reasons for the distinction by commentators no longer accord with reali-

146. *See* Gustafson v. Alloyd Co., 513 U.S. 561, 575 (1995) ("[A] word is known by the company it keeps (the doctrine of *noscitur a sociis*)."); Beecham v. United States, 511 U.S. 368, 371 (1994) ("That several items in a list share an attribute counsels in favor of interpreting the other items as possessing that attribute as well.").

147. *Gustafson*, 513 U.S. at 575; *Beecham*, 511 U.S. at 371.

148. Joe Briefcase is a fictional character created by David Foster Wallace in his essay *E Unibus Pluram: Television and U.S. Fiction* that appears in A SUPPOSEDLY FUN THING I'LL NEVER DO AGAIN 39 (1997).

149. *See* 18 U.S.C. § 2702(a)(1)–(3) (2006) (prohibiting ECS and RCS entities serving "the public" from disclosing any person's communications to any person, entity, or government).

150. Kerr, *supra* note 15, at 1226 (explaining that the legislative history is not clear about why only ECS and RCS providers that offer services to the public are covered).

ty.[151] One of the reasons offered for the distinction is that nonpublic providers of services, like a university email system, are for the benefit of the provider—the university—and not the user and, therefore, the user's information should not be protected.[152] However, it cannot be said that public accounts are only for the benefit of the user because Internet service providers to the public are for profit entities that see the users as benefiting the provider.[153] A second reason presented for the current distinction between public and private is that nonpublic providers have more of an incentive to not disclose their user's information because they have a "long-term, multifaceted relationship with their users" whereas public providers only see users as a source of revenue.[154] However, this is a distinction without a difference because in civil discovery a third party's incentive to protect user's privacy does not matter; the only thing that matters is the legal tools available to protect that privacy. Further, service providers that offer services to the public have just as much of an incentive to protect privacy because privacy breaches have a negative impact on a company's bottom line.[155]

Some might also argue that this new definition is overly broad and places too much emphasis on efficiency. After all, this definition applies to limit third party discovery requests from all present and future Internet service providers. Accordingly, the new statute could protect highly relevant material simply because it is stored online. However, as noted below, there still remains a user exception and a cost-shifting option to obtain information stored with these service providers.

Therefore with this new definition, judges, lawyers, and service providers would no longer have to fit the square peg of current and new technologies into the round ECS and RCS holes, thereby increasing efficiency of the entire discovery process.

151. For an explanation of these two rationales, see *id.* at 1226–27.

152. *Id.*

153. *E.g.*, Robison, *supra* note 18, at 1213–14 (describing how cloud computing companies use contextual advertising to drive revenues).

154. Kerr, *supra* note 15, at 1227.

155. *See* Alessandro Acquisti, et al., *Is There a Cost to Privacy Breaches? An Event Study*, Workshop on the Economics of Information Security 1, 12 (2006), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf (finding a statistically significant negative relationship between privacy breaches and a company's market value).

B. RETAIN THE USER EXCEPTION TO THE SCA

Retaining the user exception to the SCA will strike the correct balance between efficiency and liberal discovery. Serving civil discovery requests on the user instead of the provider is the "easiest and most efficient way to conduct" discovery of electronically stored information.[156] This is because a user is more familiar with where responsive information is available than the service provider,[157] service providers would incur third party legal fees if subpoenas were granted,[158] and it is drastically more expensive for a provider to preserve all possible relevant information for all of its users' ongoing civil litigation than for a user to preserve such information.[159] Additionally, retaining the user exception to the SCA allows for full and liberal discovery. All information that a user has legal access to can be discovered through a rule thirty-four request directly on the user.[160]

The user exception to the SCA should be codified in the civil discovery amendment in order to make it explicit to the courts and litigants that this is the most reasonably accessible tool for discovering electronically stored information. The statutory language should read: "This statute does not apply to legally valid civil discovery requests served upon an Internet service provider's user." Although many courts have noted that this exception is inherent in the statute,[161] some litigants do not use it and other courts have not recognized it.[162] Therefore, in

156. Megan Uncel, Note, *"Facebook Is Now Friends with the Court": Current Federal Rules and Social Media Evidence*, 52 JURIMETRICS J. 43, 58 (2011). For an example of the costs of such third party subpoenas, see *supra* note 116 and accompanying text.

157. *Cf.* Mazza, *supra* note 100, at 19 ("The 'cost and time required to have legal professionals read documents closely' for responsiveness, privilege, and other confidentiality concerns, especially 'in the context of cases involving hundreds of thousands (or even millions) of pages of records, can be astronomical.'") (internal citations omitted).

158. *See id.*; *supra* note 116 and accompanying text.

159. *See* Mazza, *supra* note 100, at 30 ("Once the scope of a litigation hold has been determined, it is up to a party and its counsel to take reasonable steps to see that sources of information within the scope are located and actually placed on hold during implementation.").

160. *See* Uncel, *supra* note 156, at 58 ("Federal Rule of Civil Procedure 34 grants parties the opportunity to discover evidence that is within the responding party's 'possession, custody, or control.'"). Any information a user can access from her account is discoverable through this rule. *Id.*

161. *See supra* note 86 and accompanying text.

162. For examples of court decisions not discussing the user exception but applying the SCA to protect information stored on the Internet, see *United*

order to increase efficiency, the user exception should be codified to give clear guidance to courts and litigants.

It could be argued that retaining only the user exception to the SCA and not providing any discovery through the provider possibly eliminates much discoverable information.[163] There is a risk of spoliation whereby a user could delete any responsive information once litigation commences.[164] However, this risk can be sufficiently reduced by supplementing discovery requests with document protection orders and through the Model Rules of Professional Conduct, which suggest that it is unethical for a lawyer to assist or counsel in the "destruction, alteration, or concealment of evidence that is relevant to a legal proceeding" or in foreseeable litigation.[165] This approach does leave open the possibility that a shrewd client might destroy important information without the lawyer's counsel.[166] This narrow loophole can be closed through the cost-shifting discovery mechanism discussed below.

C. PROVIDE A COST-SHIFTING CIVIL DISCOVERY EXCEPTION

Providing a cost-shifting mechanism that would allow litigants to obtain information otherwise unavailable is in the best interests of justice. As noted above, the Zwillinger and Genetski procedure for obtaining this information is a good model for how to add a cost-shifting discovery exception. This proposal would allow a civil litigant to obtain information from an Internet service provider if that litigant showed the information was relevant and unavailable from other sources, if that litigant paid for the other party's costs, and if it did not result in undue burden or cost upon the service provider.[167] Though, there should be one addition to Zwillinger and Genetski's amend-

States v. Councilman, 418 F.3d 67 (1st Cir. 2005); *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004); *Bower v. Bower*, 808 F. Supp. 2d 348 (D. Mass. 2011); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010); *Viacom Int'l Inc. v. Youtube Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008).

163. *See, e.g.*, Ward, *supra* note 8, at 564 (noting that users often do not have access to their deleted data).

164. *See* Uncel, *supra* note 156, at 53 ("For example, in the context of social media evidence, spoliation issues often go hand in hand with party requests. There is a legitimate risk 'that the witness will erase all the comments from his [social networking profile] immediately upon receiving' the request.") (internal citations omitted).

165. *Id.* at 57–58 (internal citations omitted).

166. *See id.* at 58 ("A stealthy client thus could delete his social media profile without legal penalty.").

167. *See supra* notes 126–28 and accompanying text.

ment. The responding party should have to pay for the costs of producing any information that was deleted, altered, or concealed after the time when litigation was filed, threatened, or reasonably foreseeable.[168] There should be a safe harbor exception for information that is lost by the service provider as a result of the "routine, good-faith operation of an electronic information system."[169]

This would provide an added disincentive for spoliation and provide equity in cost shifting. In addition to the current sanctions for failing to preserve evidence,[170] a party that intentionally spoils evidence would have to pay for the costs of restoring that evidence. This is in accordance with fundamental notions of equity as well because a party that spoils evidence should not benefit by shifting the cost of producing that evidence onto the other party.

Some might argue that this fails to meet the rule one requirement of being "just" because cost-shifting can sometimes be cost-prohibitive and therefore dispositive.[171] However, dispositive cost-shifting usually only occurs when there are large-scale requests for terabytes of information costing millions of dollars.[172] Although the use of online communications is increasing,[173] it is not likely to be the case that these requests will result in prohibitively large amounts of data.[174]

168. *Accord* AM. BAR ASS'N, SPOLIATION OF EVIDENCE 5 (Daniel F. Gourash et al. eds., 2d ed. 2006) ("Generally, no duty to preserve evidence arises before litigation is filed, threatened, or reasonably foreseeable . . . .").

169. FED. R. CIV. P. 37(e).

170. *See generally* AM. BAR ASS'N, *supra* note 168, at 54–78 (describing a district court's broad discretionary authority to impose sanctions including an adverse inference, default judgment, or fines and penalties).

171. *See* Mazza, *supra* note 100, at 98 ("[D]ecisions on motions regarding who will be required to pay for discovery responses (the cost of which may run into the hundreds of thousands, if not tens of millions, of dollars) can impact severely how an action proceeds and in fact may be outcome-determinative in some cases.").

172. *See id.*

173. *See supra* notes 1–5 and accompanying text.

174. For example, as of 2012 Gmail only allows users to store 10 GB of data, Picasa allows users to store 1 GB of pictures and videos, and AOL allows the preservation of 9,000 emails. *Free Storage Limits*, GOOGLE, http://support.google.com/picasa/bin/answer.py?hl=en&answer=1224181 (last visited Mar. 10, 2014); *Message: My Mailbox Is Full*, AOL, http://help.aol.com/help/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=220725 (last visited Mar. 10, 2014); *Your Storage Limit*, GOOGLE GMAIL, http://support.google.com/mail/bin/answer.py?hl=en&answer=6558 (last visited Mar. 10, 2014).

CONCLUSION

The SCA has outlived its usefulness in the area of civil discovery. The current application of the SCA creates inconsistent protection, inefficiency in civil discovery, and limits the amount of discoverable information. In order to strike the right balance between efficiency and justice, legislators should add a civil discovery amendment to the SCA that broadens the definition of protected information, codifies the user exception, and allows for a cost-shifting discovery provision.