DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 22
Issue 1 *Fall 2011*

Article 4

Unfriending the Stored Communications Act: How Technological Advancement and Legislative Inaction Have Rendered Its Protections Obsolete

Simon M. Baker

UNFRIENDING THE STORED COMMUNICATIONS ACT:

HOW TECHNOLOGICAL ADVANCEMENT AND LEGISLATIVE INACTION HAVE RENDERED ITS PROTECTIONS OBSOLETE

I. INTRODUCTION

"Admit it, you're guilty. Repeat after me, my name is _____ and I am a Facebook addict."[1] Or if you are still in denial about being a social media site addict,[2] you may at least be willing to admit that you know someone who is. Perhaps that person is among the fifth of young female users who check their Facebook accounts in the middle of the night.[3] Or perhaps she, too—like over half of young female users—talks to her friends more online than she does face-to-face.[4] In light of such startling numbers, it is evident that social networking sites are one of the most prominent Internet trends.[5] As of November 2011, Facebook had over 800

1. Kayla Webley, *It's Time to Confront Your Facebook Addiction*, TIME.COM (July 8, 2010), http://newsfeed.time.com/2010/07/08/its-time-to-confront-your-facebook-addiction/#ixzz142nXq3Hz.

2. One researcher found that while "Facebook addiction" or "Facebook addiction disorder" are not medically approved terms, the reality of addictive behaviors on Facebook are a growing problem for many Facebook users, and one that therapists are seeing more frequently in their patients. Elizabeth Cohen, Five Clues that You Are Addicted to Facebook, CNN Health (Apr. 23, 2009), http://www.cnn.com/2009/HEALTH/04/23/ep.facebook.addict/index.html ?iref=storysearch. In a recent study of 1,605 adults surveyed on their social media habits, 39% are self-described Facebook "addicts." Benn Parr, The First Thing Young Women Do in the Morning: Check Facebook [STUDY], Mashable.com (July 7, 2010), http://mashable.com/2010/07/07/oxygen-facebook-study/.

3. Parr, *supra* note 2.

4. *Id.*

5. Katherine Minotti, *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, 60 S.C. L. REV. 1057, 1058 (2009). *See also* Ryan A. Ward, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J. L. & TECH. 563,

million active users, over half of which log on every day.[6] Social networking now accounts for one out of every six minutes spent on the internet.[7] And perhaps most striking is that this unprecedented phenomenon shows no sign of slowing down.[8]

In fact, social media sites are having an ever-increasing influence on society, one which reaches even beyond the Internet. Unsatisfied with a mere online presence, these sites have taken on a life of their own, pervading almost every aspect of our existence complete with their own lexicon and etiquette.[9] No longer do we simply use Facebook, but we "facebook"[10] our friends. No longer do we need to talk to someone face to face to share information, instead we can "tweet."[11] And if we have a falling out with a friend, we no longer have to bother to tell her, we can simply "unfriend"[12] her.

---

563 (2011) ("Americans spend over 20% of their online time on social networks and blogs.").

6. *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Nov. 20, 2011, 12:17 PM).

7. Ben Parr, *Social Networking Accounts for 1 of Every 6 Minutes Spent Online [STATS]*, MASHABLE, (June 15, 2011), http://mashable.com/2011/06/15/social-networking-accounts-for-1-of-every-6-minutes-spent-online-stats/.

8. In America alone, Facebook's user base increased 454.5% between July 2008 and April 2011. See Nick Burcher, Facebook Usage Statistics by Country - July 2010 Compared to July 2009 and July 2008, Nick Burcher (July 2, 2010), http://www.nickburcher.com/2010/07/facebook-usage-statistics-by-country.html; Nick Burcher, Facebook Usage Statistics 1st April 2011 vs April 2010 vs April 2009, Nick Burcher (Apr. 05, 2011), http://www.nickburcher.com/2011/04/facebook-usage-statistics-1st-april.html.

9. *See infra* notes 10–12 and accompanying text.

10. Troy Janisch, *Facebook a Verb? That's What's Happenin'*, SOCIAL METEOR (Sept. 2, 2009), http://www.socialmeteor.com/2009/09/02/facebook-a-verb-thats-whats-happenin/.

11. *See* TWITTER, http://twitter.com/about (last visited Nov. 20, 2011, 8:23 PM).

12. The term is now official – *Oxford Word of the Year 2009: Unfriend*, OUPBLOG (Nov. 16, 2009), http://blog.oup.com/2009/11/unfriend/. *See also* Emma Barnett, *Facebook's 'Unfriend' Verb is Voted 'Word of the Year'*, THE TELEGRAPH (Nov. 17, 2009), http://www.telegraph.co.uk/technology/facebook/6591614/Facebooks-Unfriend-verb-is-voted--Word-of-the-Year.html.

As always, where society treads, the law soon follows. The increased use of these sites provides attorneys with a wealth of useful and discoverable information, which has had profound implications on their trial strategies.[13] For example, social media sites allow users to upload pictures, text, videos, and personal information onto their own personal "home-page,"[14] and attorneys have been quick to realize that these uploads sometimes provide crucial evidence about the individual litigants that can have had an immediate impact on the case at trial.[15]

However, the use of information gathered from social media sites is still subject to discovery and privacy rules. The more these sites grow, the more important it becomes to define the scope of discovery laws and the validity of subpoenas seeking this information.[16] Yet despite the importance of this question, it was

13. *See generally Social Media Effects On Law and the Legal System*, CLEAN CUT MEDIA (Feb. 13, 2009), http://www.cleancutmedia.com/news/social-media-effects-on-law-and-the-legal-system; JOHN G. BROWNING, THE LAWYER'S GUIDE TO SOCIAL NETWORKING: UNDERSTANDING SOCIAL MEDIA'S IMPACT ON THE LAW (2010).

14. More than thirty billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are shared each month. *Internet 2010 in numbers*, PINGDOM (Jan. 12, 2011), http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/.

15. Facebook's major contribution has been to discovery: "The growing use of social networking web sites presents opportunities for lawyers to gather evidence from these . . . sites [for use in both] criminal and civil cases." Minotti, *supra* note 5, at 1059. With lawyers' increased access to this evidence, unwitting plaintiffs in personal injury cases are routinely caught out by incriminating pictures of them posted on social media sites such as Facebook and MySpace. *See, e.g.*, Benjamin Rolf et al., *The Usefulness of Social Networking Websites to a Resourceful Defense Team*, 3 STRICTLY SPEAKING 1, *available at* http://www.dri.org/ContentDirectory/Public/Newsletters/0200/2008%20Product%20Liability%20Committee%20Strictly%20Speaking%20Winter.pdf. Defendants have also been caught out. *See, e.g.*, Minotti, *supra* note 5, at 1059–60.

16. This has particularly large ramifications in the United States, a country that not only has a reputation for being litigious but is also but home to over a quarter of all Facebook users. *See Facebook Users in the World, Facebook Usage and Facebook Penetration Statistics by World Geographic Regions*, INTERNET USER STATS USAGE AND POPULATION STATISTICS, http://www.internetworldstats.com/facebook.htm (last visited Nov. 28, 2011).

not until May of 2010 that a court[17] first considered whether subpoenas served directly on social networking sites can be quashed under current statutory law, the Stored Communications Act ("SCA").[18] In that case the court held that the SCA does not require a social media service to respond to a subpoena for discovery information.[19] However, it also noted that the SCA is outdated and does not adequately apply to modern communications.[20] This Comment agrees with the court's criticism of the Act and contends that the legislature must either radically reform or completely replace the SCA because it does not provide a sufficient framework with which courts can consistently determine whether subpoenas are valid. Congress has not reacted to the advances in technology and the subsequent changes in how we communicate, which has now rendered the law obsolete.

Part II of this Comment provides an overview of the SCA.[21] It first details the history of the Act; it then explains the reasons for its enactment and provides an overview of its traditional interpretation. Part III then focuses on the recent application of the Act by dissecting *Crispin v. Christian-Audigier, Inc.*, the first case to thoroughly analyze if and how the SCA should provide privacy to users of social media sites.[22] Part IV critiques the *Crispin* decision. It examines how that court grappled with the difficulties inherent in applying the SCA (a thirty-six year old statute) to modern forms of social networking and communications. It also attempts to rationalize the court's holding, explaining how the court balanced the need to implement practical policies, despite being constrained by the Act's dense and dated language. [23] It highlights some of the broader social issues raised by the scope of Internet privacy, and how other courts have tried to answer these concerns. Finally, Part V focuses on the future of the Stored

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

18. Stored Wire and Electronics Communications and Transaction Record Access (Stored Communications Act), Pub. L. No. 99-508, 100 Stat. 1860 (codified as amended in scattered sections of 18 U.S.C.).

19. *Crispin*, 717 F. Supp. 2d at 991.

20. *Id.* at 972 n.15.

21. *See infra* notes 25–104 and accompanying text.

22. *See infra* notes 105–171 and accompanying text.

23. *See infra* notes 172–191 and accompanying text.

Communications Act.[24] Illustrated through *Crispin*, this Part reveals the current law's failings and how the SCA must either be amended or replaced to implement Congress' original intent. In the face of technological advancements, the SCA can no longer provide an adequate legal framework for privacy protections.

II. BACKGROUND

A thorough understanding of the Stored Communications Act ("SCA") is necessary to comprehend the *Crispin* court's decision and the further policy implications that arise from it. First, this section examines the law prior to the SCA and highlights the major deficiencies that led to its enactment.[25] It then explains how the SCA has been interpreted and how it works to protect the privacy of electronic communications.[26]

A. Gaps in the Law

The American legal system has not always afforded all citizens the same rights to privacy that are enjoyed today. English jurist Sir Edward Coke famously wrote that "[t]he house of every one is to him as his castle and fortress."[27] But while this concept was firmly entrenched in English jurisprudence,[28] there was no similar protection in early American history.[29] In response,[30] the Framers

24. *See infra* notes 192–219 and accompanying text.

25. *See infra* notes 28–46 and accompanying text.

26. *See infra* notes 47–105 and accompanying text.

27. Semayne's Case, (1604) 77 Eng. Rep. 194 (K.B.), 5 Co. Rep. 91 a.

28. The concept of privacy "is as old as the basic concepts of English common law." WILLIAM & MARY MORRIS, MORRIS DICTIONARY OF WORD AND PHRASE ORIGINS 374 (2d ed. 1988).

29. In the years preceding the Bill of Rights, the American government of the time repeatedly engaged in "ill use of the warrant process to engage in suspicionless searches and seizures." THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 20 (2008). *See also* Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 514 (1994).

30. The Fourth Amendment was, at least in part, designed to "protect individual citizens from unfettered invasions . . . into their homes." ROBERT M.

passed the Fourth Amendment,[31] requiring the federal government[32] to obtain a judicially sanctioned warrant based on probable cause before entering and searching private property.[33]

Fast forward to 1986, as the Fourth Amendment approaches its two-hundredth birthday. In some respects the Fourth Amendment had aged well—its protections for a man's castle are still strong.[34] However, the guiding aim behind the Fourth Amendment was broader than the protection of homes.[35] In this respect, its age was betraying it; the Fourth Amendment alone was ill-suited to apply its intended protections when faced with new technologies.[36]

Noting this gap in protection and the potentially devastating effects that it had on privacy,[37] Congress sought to remedy the

---

BLOOM, SEARCHES, SEIZURES, AND WARRANTS: A REFERENCE GUIDE TO THE UNITED STATES CONSTITUTION xvii (Jack Stark ed., 2003).

31. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

32. The Supreme Court has since held that the Fourth Amendment also applies to state government by way of incorporation through the Fourteenth Amendment. Mapp v. Ohio, 367 U.S. 643, 655 (1961).

33. JOHN WESLEY HALL, JR., 1 SEARCH AND SEIZURE § 3.1 (3d ed. 2000).

34. JAMES A. ADAMS, OVERVIEW OF CHAPTER 121: STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS (2010), *available at* LEXIS, 18 US NITA prec 2701.

35. The Fourth Amendment was intended to "'protect personal privacy and dignity against [all] unwarranted intrusion by the State.'" Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 352 (2009) (quoting Schmerber v. California, 384 U.S. 757, 767 (1966)).

36. S. REP. NO. 541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 ("When the Framers of the Constitution acted to guard against the arbitrary use of government power to maintain surveillance over citizens, there were limited methods of intrusion into the 'houses, papers, and effects' protected by the Fourth Amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such invasions.").

37. S. REP. NO. 90-1097, at 37–38 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2122, 2154 ("The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance . . . . Both proponents and opponents of wiretapping

situation by passing the Wiretap Act.[38] However, this Act was limited in scope[39] and once again technological advances outpaced the legislature's ability to react.[40] Even through several amendments to the Wiretap Act, Congress was unable to adequately address the "rapid advances in telecommunications wrought by the proliferations of computers and computer technology."[41]

Only eighteen years later, Congress passed the Electronic Communications Privacy Act.[42] Title II of this Act is the Stored Communications Act, which deals specifically with privacy for stored communications.[43] This Act was designed to plug the holes in protection left by the Fourth Amendment by "creat[ing] a set of Fourth Amendment-like privacy protections."[44] Currently, it is the

---

and electronic surveillance agree that the present state of law in this area is extremely unsatisfactory and that the Congress should act to clarify the resulting confusion.").

38. Title III of the Omnibus Crime Control and Safe Streets Act, Pub. L. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–17 (2006)).

39. It sought only to protect electronic information from being "intercepted." *Id.* Moreover, the legislation did not attempt to protect certain, now prevalent, forms of information such as text, digital, or machine communications. *See* S. REP. NO. 90-1097, at 38, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154. The House of Representatives Committee on the Judiciary concluded that the Wiretap Act's "statutory framework appears to have left unprotected an important sector of the new communications technologies. . . . Under existing law the interception . . . or the disclosure of [the most common communications] are probably not regulated or restricted." H. REP. NO. 99-647, at 17–18 (1986).

40. "Although it is not twenty years old, the Wiretap Act was written in different technological . . . era [sic]." H.R. REP. NO. 99-647, at 17 (1986).

41. Carlos Perez-Albuerne & Lawrence Friedman, Article, *Privacy Protection for Electronic Communications and the "Interception-Unauthorized Access" Dilemma*, 19 J. MARSHALL J. COMPUTER & INFO. L. 435, 438 (2001).

42. Congress passed this Act in part to replace the Wiretap Act, but also to create greater protections. Electronic Communications and Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

43. Stored Wire and Electronics Communications and Transaction Record Access (Stored Communications Act), Pub. L. No. 99-508, 100 Stat. 1860 (codified as amended in scattered sections of 18 U.S.C.).

44. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislature's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004). More specifically, it sought to "creat[e] a zone of privacy to protect Internet

only federal statutory protection for electronic communications that are held in storage.[45]

B. The Stored Communications Act

The Stored Communications Act was passed in response to fears that the Fourth Amendment alone could not adequately protect Internet communications from unreasonable government interference.[46] Moreover, the Act was specifically tailored to address the three main failings of the Fourth Amendment as applied to Internet communications.[47]

The first main failing of the Fourth Amendment was that it only applied when the subject of the search had a reasonable expectation of privacy.[48] The Supreme Court has repeatedly held that a user does not have a reasonable expectation of privacy in information that he discloses to a third party.[49] An expansive interpretation of this doctrine would eliminate a person's Fourth Amendment protection for any information sent through e-mail or posted on Internet forums, as this information is disclosed to the Internet Service Provider ("ISP") during transmission.[50] Second,

---

subscribers from having their personal information wrongfully used and publically disclosed." Timothy G. Ackerman, *Consent and Discovery Under the Stored Communications Act*, THE FED. LAW., Nov.–Dec. 2009, at 42.

45. MATTHEW BENDER & CO., 1-2 PRIVACY LAW AND THE USA PATRIOT ACT § 2.19 (2010).

46. *See* Kerr, *supra* note 44 and accompanying text.

47. Although these three reasons are briefly outlined below, see Kerr, *supra* note 44, at 1210–1212 for a more detailed analysis.

48. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

49. This is often called the Miller principle, from United States v. Miller, 425 U.S. 435 (1976). For a more detailed analysis of this principle, see MATTHEW BENDER & CO., *supra* note 45, § 2.05.

50. In the context of e-mails, there is still debate as to whether the user retains a reasonable expectation of privacy. However, at least one court has now held that a user does have a reasonable expectation of privacy in an e-mail. Warshak v. United States, *631 F.3d 266, 288* (6th. Cir. 2010). The *Warshak* court held that because there is a reasonable expectation of privacy, the Fourth Amendment applies and therefore the police must obtain a warrant in order to compel disclosure of documents from an ISP. *Id.* The court also held that insomuch as the SCA allowed such disclosure with anything less that a warrant

the Fourth Amendment does not provide sufficient safeguards from the government with respect to remotely stored information; the government can access electronic data stored with a third party by serving that third party with a subpoena, even if it does not have probable cause.[51] Finally, the Fourth Amendment does not apply to searches effected by private parties.[52] Thus, under the Fourth Amendment alone, there is nothing to stop an ISP from searching personal communications in its capacity as a private party and then voluntarily disclosing this information to governmental agencies.

Congress recognized the apparent inequity in the treatment of electronic information and physical communications,[53] and accordingly passed the SCA to remedy these problems in two main ways. The first manner in which the SCA seeks to buttress Fourth Amendment rights is by restricting a covered provider[54] from

---

it is unconstitutional. *Id.* But the issue is still far from clear; as yet this is the first and only court to rule on the issue in this way. At least in the context of social media sites however, the answer to whether users have legitimate expectation of privacy appears to be clearer. "In [respect to social media sites such as Facebook and MySpace], privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking." Dana L. Fleming & Joseph M. Herlihy, *What Happens When the College Rumor Mill Goes Online*, BOS. BAR. J., Jan./Feb. 2009, at 16.

51. Kerr, *supra* note 44, at 1211–12.

52. The Fourth Amendment is "wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private [party] not acting as an agent of the Government . . . .'" United States v. Jacobsen, 466 U.S. 109, 113 (1984) (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)).

53. *See* S. REP NO. 99-541, at 5 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3557, 3559. Courts have since strived to implement that intent; O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 87 (Cal. Ct. App. 2006) ("A fundamental purpose of the SCA [was] to lessen the disparities between the protections given to established modes of private communication and those accorded new communications media"); Theofel v. Farey-Jones, 341 F.3d 978, 982 (9th Cir. 2003), *amended by* 359 F.3d 1066 (9th Cir. 2004) ("Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents . . . the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.").

54. *See infra* notes 64–82 and accompanying text for an explanation of when a provider is subject to the SCA.

voluntarily disclosing an individual's information to the government.[55] Secondly, the SCA limits the government's ability to require those providers to disclose those communications or records.[56]

Although these goals may appear simple, their implementation has provided difficulties for courts since the Statute's enactment.[57] The SCA is far from clear, and its application and interpretation has been difficult. Both its language and interplay with other titles of the Electronic Communications Privacy Act has been variously called "confusing and uncertain"[58] and "complex [and] convoluted."[59] However, it is clear that Congress did not intend to design a catch-all to protect each and every electronically stored communication;[60] rather, its application, and thus protections, is limited.[61] This Comment now provides an overview as to the instances in which the SCA applies.

1. Preliminary Questions to Determine the Applicability of the SCA

The "focal point" of the Stored Communications Act is the entity that is currently in possession of the communication that the subpoena seeks to acquire. Therefore, the first question to ask when applying the SCA is whether the party who has the requested information is covered by the Act.[62] If the entity is not covered, then the extra protections offered by the SCA do not apply, and the

55. 18 U.S.C. § 2702(a)(3) (2006).

56. *See id.* § 2703(a).

57. Both commentators and courts alike have noted the Act and the surrounding area of law for its "lack of clarity." Steve Jackson Games, Inc. v. Unites States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994). *See also* Kerr *supra* note 44, at 1208 ("The [SCA] is dense and confusing and few cases exist explaining how the statute works.").

58. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

59. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

60. Kerr, *supra* note 44, at 1214.

61. *See infra* notes 62–73 and accompanying text. For a more detailed analysis see Kerr, *supra* note 44. *See also* RAYMOND T. NIMMER, 4 THE LAW OF COMPUTER TECHNOLOGY § 17:32 (4th ed. 2010).

62. Kerr, *supra* note 44, at 1213.

party seeking to withhold the information must rely solely on the often insufficient Fourth Amendment.[63] The restrictions regarding disclosure of electronically stored information apply only to a person or entity that provides, to the public, either an Electronic Communications Service (ECS) or a Remote Computing Service (RCS).[64] From this basic definition come two very important questions: (1) how to determine which persons or entities are public, and (2) whether that entity is providing an ECS, an RCS, both, or neither.

The first of these questions—whether an entity is public or private—is relatively clear.[65] Although the SCA does not provide a definition of the word "public," an entity provides a service "to the public" if it provides that service to "the community at large," whether or not it charges a fee.[66] This excludes systems that are proprietary or purely intra-company,[67] or situations in which the services are only available to users with a special relationship to the entity providing the service.[68]

The second question—whether an entity is providing an electronic communications service, a remote computing service, both, or neither—is much more difficult, and is often at the heart of SCA litigation.[69] The Act only applies to ECS and RCS providers; if an entity does not fit within these technical definitions, then it "can disclose or use with impunity the contents

63. *Id.*

64. 18 U.S.C. §§ 2702(a)–(b), 2703(a)–(b) (2006). *See also* Wesley College v. Pitts, 974 F. Supp. 375, 389 (D. Del. 1997) ("[A] person who does not provide an electronic communication service [or a remote communication service] . . . can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage.").

65. *See* Kerr, *supra* note 44, at 1226.

66. *See* Anderson Consulting LLP v. UOP, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998).

67. *See* NIMMER, *supra* note 66, § 17:32.

68. *See Anderson Consulting LLP*, 991 F. Supp. at 1042–43.

69. *See, e.g.*, Theofel v. Farey-Jones, 341 F.3d 978, 984–85 (9th Cir. 2003); Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635–36 (E.D. Pa. 2001); *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001).

of an electronic communication . . . ."[70] The SCA defines an ECS as an entity that "provides to users thereof the ability to send or receive wire or electronic communications."[71] An RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[72] The SCA further defines electronic communications system as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[73]

The ECS/RCS inquiry has been problematic for several reasons. First, the current law has simply not kept pace with technological advancement. Although computer technology has significantly developed since 1986 (when the SCA was enacted) the statute has not been altered, effectively "freezing into the law the understandings of computer network use as of 1986."[74] Following the seismic advances in technology, many of today's entities no longer fit neatly within these two distinct categories,[75] making application of the Act problematic. This in turn leads to the second difficulty in making the ECS/RCS distinction: the current case law has tended to blur the line between these two types of providers as judges have bent definitions in order to afford protection under the statute, even when the plain language of the Act makes it clear that it should not have been.[76] This second inquiry is also made difficult because these definitions are highly context sensitive; an entity can act as an ECS with respect to one

70. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 973 (C.D. Cal. 2010) (citing Wesley College v. Pitts, 974 F. Supp. 375, 389 (D. Del. 1997)).

71. 18 U.S.C. § 2510(15).

72. *Id.* § 2711(2).

73. *Id.* § 2510(14).

74. Kerr, *supra* note 44, at 1214.

75. *See* S. Rep. 99-541, at 2–3 (1986) (discussing how the increases in computing power since 1986 had led to a concomitant shift in how data is stored and processed, but noting there was no corresponding amendment to existing law, leaving outdated practices as the basis for the current statutory scheme); Kerr, *supra* note 46, at 1213–14, 1235.

76. Kerr, *supra* note 44, at 1215. This results in a lack of consistent and clear case law.

communication and an RCS with respect to another.[77] Also, an entity's role with respect to a single communication can change over time.[78]

Finally, even if the Act does apply to a certain entity, it may not apply to the actual communication that is being sought. A provider of an ECS is only prohibited from disclosing the contents of a communication while that information is being held "in storage."[79] For an ECS, the SCA defines "storage" as either (A) "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, [or] (B) any storage of such communication by an electronic communication service for purposes of back-up protection of such

77. The SCA focuses on the information being sought and the entity's relationship to that specific piece of information.

78. "Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular times (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself." *In re* United States, 665 F. Supp. 2d. 1210, 1214 (D. Or. 2009). Orin S. Kerr gives a more detailed example of how an entity's role can shift over time.

> Imagine that I send an e-mail to my friend Jane who has an account at a commercial ISP. When the message first arrives at the ISP, the ISP acts a provider of ECS with respect to the e-mail. The e-mail is in 'electronic storage' awaiting Jane's retrieval of the message. Once Jane retrieves my e-mail, she can either delete the message from the ISP's server or leave the message stored on the ISP's server for safekeeping. If Jane chooses to store the e-mail with the ISP, the ISP now acts as a provider of RCS [and possibly also an ECS, depending on the jurisdiction] with respect to that copy of the e-mail so long as the ISP is . . . public. The role of the ISP has [increased] from [solely] a transmitter of the e-mail to a storage facility available to the public, from an ECS to an RCS [and ECS] . . . . If Jane downloads a copy of the e-mail onto her personal computer, the ISP acts as neither a provider of ECS nor RCS with respect to the downloaded copy regardless of whether the ISP is available to the public. The ISP is not holding the downloaded copy either incident to transmission or for storage; in fact, the ISP does not hold that copy at all.

Kerr, *supra* note 44, at 1216–17 (internal citations omitted).

79. 18 U.S.C. § 2702(a) (2006).

communication."[80] In contrast, an RCS provider is only prohibited from disclosing consumer information that is kept "for the purpose of providing [remote] storage or computer processing services to [the] subscriber or customer."[81] Importantly, neither of these definitions includes information that has been "intercepted."[82]

2. Voluntary Disclosure

With these basic definitions in mind, a more thorough examination of the Act, and what it prohibits, is possible.

Section 2702 of the Act prohibits any covered entity from voluntarily disclosing both the customer's actual communications (content information) and the "record[s] or other information pertaining to [the] customer" (non content information).[83] The Act provides for different standards of protection for these two basic forms of information.[84]

---

80. *Id.* § 2510(17)(A)–(B). And, perhaps, unsurprisingly the various jurisdictions have not interpreted the definition of "storage" uniformly. For example, some jurisdictions hold that when an e-mail has been opened it is neither (1) being held in storage (i.e. it is no longer temporary, intermediate storage while delivery is pending), and (2) is also not being held for "back-up" purposes. *See, e.g.*, United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009); Flagg v. City of Detroit, 252 F.R.D. 346, 362–63 (E.D. Mich. 2008). However, some courts have taken a different approach. *See, e.g.*, Theofel v. Farey-Jones, 341 F.3d 978, 982 (9th Cir. 2003). This split will be discussed more below.

81. Crispin v. Christian Audigier Inc., 717 F. Supp. 2d 965, 973 (C.D. Cal. 2010) (citing 18 U.S.C. § 2702(a)(2)).

82. "Intercept[ion]" is defined in 18 U.S.C. § 2510(4). For greater discussion of the interplay between interception and unauthorized access and the difficulty that the courts have in defining the precise boundaries between the two, see Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001); Perez-Albuerne & Friedman, *supra* note 41. Also *see generally* Tatsuya Akamine, *Proposal For a Fair Statutory Interpretation: E-Mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act*, 7 J. L. POL'Y 519 (1999).

83. 18 U.S.C. § 2702(a) (subject to the exceptions listed in § 2702(b)) provides the rules for the disclosure of content information, § 2702(c) provides rules for non-content information.

84. The Act assists in determining what is content information, stating that "'contents', when used with respect to any wire, oral, or electronic

The SCA first states applicable rules for disclosure of content information.[85] Both public ECS providers and public RCS providers are prohibited from knowingly divulging the contents of any communication while held in electronic storage (in the case of an ECS), or while providing remote storage or computer processing services (in the case of an RCS).[86]

In contrast, the Act provides less protection for non-content information.[87] It only prohibits RCS and ECS providers from disclosing such information to government entities.[88] In addition to this diluted protection, both of these provisions only apply if the entity in question is providing a service to the public. Non-public entities and entities providing services solely to private parties may voluntarily disclose all information at will.[89]

---

communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Unfortunately this definition is not clear; not only does it fail to give any examples, but it only states what contents *includes* and does not actually define what it actually is. Kerr, *supra* note 44, at 1228. Some courts have tried to supplement this definition by attempting to clarify what is *excluded* from the definition of content. Jessup-Morgan v. Am. Online, Inc., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 2008).

85. Despite some ambiguity in the definition of "content information" the body of an e-mail and the subject line are "content" information. Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 646 (2003).

86. 18 U.S.C. § 2702(a)(1)–(2).

87. Non-content information includes information that is incidental to the main email text, such as the name of the sender, the recipient, the recipient's address, the time sent, and the place from which it was sent. *See* COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, U.S. DEPT. OF JUSTICE, SEARCHING & SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 122 (2002), *available at* http://www.cybercrime.gov/ssmanual/03ssma.html.

88. 18 U.S.C. § 2702(a)(3) (2006). Section 2702(c)(4) makes explicit that there is no such prohibition from disclosure of non-content records to non-governmental agencies in the list of exceptions for voluntary disclosure of content information.

89. *See, e.g.*, Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000) ("Section 2702 prohibits disclosure of electronic data, but this prohibition is limited to persons or entities that (1) provide an electronic communication service *to the public*; or (2) provide remote computing service *to the public*" (emphasis added)).

3. Required Disclosure—Disclosure Compelled by the Government

In contrast to voluntary disclosure (which is regulated by section 2702), section 2703 of the Act establishes when a governmental agency may compel disclosure of information from an ECS or RCS.[90] Whether disclosure is mandatory or voluntary is crucial because different standards apply to each scenario, and the protections afforded to an individual's privacy will be dependent upon this distinction.[91] Once again, the court must distinguish between content and non-content information.[92]

The government may force an RCS to disclose the content of any wire or electronic communication (i.e. content information) in three basic ways.[93] First, a government entity may require disclosure without notice if it first obtains a warrant using either (1) the procedures set forth by the Federal Rules of Criminal Procedure, or (2) in a state case, the applicable state procedures.[94] This is the most onerous method for required disclosure. The second and third methods are less burdensome, but the government entity must give prior notice to the subscriber or customer. If it does so, it may compel disclosure with either (1) an administrative subpoena authorized by a Federal or State statute or grand jury trial or (2) a court order for such disclosure under section 2703(d) of the Act.[95] The rules controlling a government entity's attempt to compel disclosure of content information from a provider of an ECS are more complex. If the contents have been held in storage for 180 days or less,[96] the government may only compel disclosure with a warrant.[97] But if the content has been in electronic storage

90. 18 U.S.C. § 2703 (2006).

91. *See id.* §§ 2702, 2703.

92. *See id.* § 2703.

93. *Id.* § 2703(b)(2).

94. *Id.* § 2703(b)(1)(A).

95. *Id.* § 2703(b)(1)(B)(i), (ii).

96. The rule adopted by the Ninth Circuit, which eschews the strict 180 day time limits for a more flexible approach, asks whether the e-mail has "expired in the normal course of business," making the test even less clear. Theofel v. Farey-Jones, 359 F.2d 978, 982 (9th Cir. 2004).

97. 18 U.S.C. § 2703(a) (2006).

for more than 180 days, the government may use any of the methods enumerated in section 2703(b).[98]

In contrast with the formidable procedures for compelled disclosure of content information, the rules for compelled disclosure of non-content information provide less protection. Section 2703(c) regulates the compelled disclosure of non-content information, which is identical for both ECS and RCS providers.[99] There are five methods by which the government can compel disclosure: (1) obtaining a warrant,[100] (2) obtaining a court order as defined under section 2703(d),[101] (3) obtaining consent of the subscriber or customer,[102] (4) by written request to the subscriber in the case of telemarketing fraud,[103] or (5) by simple request to the provider if the information is so called "basic subscriber information."[104]

III. SUBJECT OPINION: CRISPIN V. CHRISTIAN AUDIGIER, INC.

As explained in the previous section, the SCA is not a "catch-all statute designed to protect the privacy of [all] stored Internet [communications and records]."[105] However, until *Crispin*, no court had directly addressed whether the SCA applied to social media sites.[106] This part explores the *Cripsin* decision and highlights the issues addressed in applying the Act to modern communication technology.

98. *Id.* § 2703(b).

99. *Id.* § 2703(c).

100. *Id.* § 2703(c)(1)(A).

101. *Id.* § 2703(c)(1)(B).

102. *Id.* § 2703(c)(1)(C).

103. *Id.* § 2703(c)(1)(D).

104. *Id.* § 2703(c)(1)(E), (c)(2). *See* Kerr, *supra* note 44, at 1219 for analysis of the term "basic-subscriber information." This information includes (but is not limited to) name, address, connection records, and method of payment.

105. *See generally supra* notes 62–73; Kerr, *supra* note 44, at 1214–15.

106. "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." Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 977 (C.D. Cal. 2010).

The *Crispin* case was, at its heart, a breach of contract case. The plaintiff, Buckley Crispin, alleged that at some time between November of 2005 and January of 2006, he granted the defendants and their various sub-licensees, Christian Audigier, Inc., an oral license to use various pieces of his artwork in a limited matter.[107] He further alleged that the defendants violated this agreement, resulting in a breach of contract, copyright infringement, and a breach of the covenant of good faith and fair dealing.[108]

In response, Christian-Audigier, Inc. served subpoenas on both MySpace and Facebook, seeking not only basic subscriber information, but also user content in the form of communications between Crispin and a third party.[109] It claimed that this information was relevant in determining the scope, nature, and terms of the agreement and the measure of damages that Crispin should be awarded if he prevailed on the merits.[110]

Crispin then filed an ex parte motion to quash the subpoenas contending that, amongst other things, the social media sites were prohibited from disclosing communications under sections 2701(a)(1) and (2) of the SCA.[111] The trial judge disagreed, and refused to quash the subpoenas.[112] Crispin appealed, and the case moved up to the Circuit Court for the Central District of California.

---

107. *Id.* at 968.

108. *Id.* Crispin alleged that the defendant not only "failed to include his logo on a substantial quantity of apparel bearing his artwork, but at times they attributed the artwork to another artist or to Audigier himself." *Id.*

109. *Id.* The defendants requested both content and non-content information in their subpoenas.

110. *Id.* at 968–69.

111. *Id.* at 969.

112. The court concluded that the SCA did not apply because it only applies to electronic communication service providers, and the defendants in the case at bar were not ECS providers as defined in the statute. *Crispin*, 717 F. Supp. 2d at 969. In addition he concluded that the Stored Communications Act prohibits only the voluntary disclosure of information by ECS providers, and does not restrict disclosure compelled by subpoena. *Id.* at 969–70. He also found that "the SCA prohibits only the disclosure of communications held in 'electronic storage' by the ECS provider, and that the materials were not in electronic storage as that term is defined in the statute." *Id.* at 970.

The primary issue for the District Court, and the one that is relevant here, was whether the subpoenas could be quashed under the Stored Communications Act. In making its decision, the court split the social media sites into their two predominant functions[113] and examined the validity of the subpoenas separately for each. The first function is a private messaging function, which is comparable to traditional e-mail.[114] The second function is more akin to a traditional bulletin board in that it allows users to type messages and notes and "pin them up" for everyone with access to their page to see.[115] For both functions, the validity of the subpoenas depended on two key questions: (1) whether Facebook and MySpace were entities covered by the Act (i.e. whether they were either ECS or RCS providers), and (2) if so, whether the information sought by the subpoenas was in "electronic storage" for the purposes of the Act. If both of these questions were answered in the affirmative, the subpoenas would have to be quashed, but if not, the information sought would be discoverable from both Facebook and MySpace.[116]

A. Are Social Media Sites ECS or RCS providers?

1. Wall Posts/Comments

The court first considered whether the sites' wall posting and comments features constituted either an ECS or RCS service.[117] In ruling, the court analogized these functions to traditional electronic bulletin board service (BBS), and therefore found the previous

113. *Id.* at 976–77.

114. *Id.* at 976.

115. The Facebook terminology for this is "posting" on someone's "wall," "a space on each user's profile page that allow friends to post messages for the user to see." *Id.* at 977 (quoting *Facebook features*, WIKIPEDIA, http://en.wikipedia.org/wiki/Facebook_features#Wall). MySpace has a similar function which allows users to post a "comment" on another person's page. *Id.*

116. The Stored Communications Act does not interfere with regular discovery from opposing parties, rather it only regulates disclosure of information from a covered entity.

117. *See id.* at 987–88.

case law regarding BBS "relevant, if not controlling."[118] Previous definitions equate BBS services with a "traditional cork-and-pin bulletin board on which people post messages,"[119] finding that they were simply a modern equivalent of old technology.[120] The court also found that the SCA was intended to cover electronic bulletin boards,[121] so long as it is restricted in some fashion,[122] and therefore restricted BBS websites are classed as ECS providers. The court then found that Facebook was indistinguishable from a controlled-access BBS,[123] and thus acts as an ECS so long as there is some restriction on access.[124]

---

118. *Id.* at 980.

119. *Crispin,* 717 F. Supp. 2d at 980–81 (citing United States v. Riggs, 739 F. Supp. 414, 417 n.4 (N.D. Ill. 1990)).

120. *See, e.g.*, *Riggs*, 739 F. Supp. at 417 n.4 (BBS services "simulate[] an actual bulletin board by allowing computer users who access a particular computer to post messages, read existing messages, and delete messages.").

121. *Crispin*, 717 F. Supp. 2d at 981 (citing United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002)).

122. Although the legislative history and subsequent case law have made clear that computer bulletin board services may be covered by the Act, it has made equally clear that "[o]nly electronic bulletin boards which are not readily accessible to the public are protected." Kaufman v. Nest Seekers, LLC, No. 05 CV 6782(GBD), 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006). Therefore unless the BBS is "configured in some way so as to limit access by the general public" it is not protected under the SCA. Id. (citing Snow v. DirecTV Inc., 450 F.3d 1314, 1322 (11th Cir. 2006)). See also S. Rep. 99-541, reprinted in 1986 U.S.C.C.A.N. 3555, 3590 ("The bill does not for example hinder the development or use of 'electronic bulletin boards' [when the] service [is] widely known and [it] does not require any special access code or warning to indicate that the information is private. To access a communication in such a public system is not a violation of the Act, since the general public has been 'authorized' to do so by the facility provider.").

123. Facebook wall postings can only be viewed by someone who has been granted access to the user's profile page. Absent the most lax privacy settings (which allow anyone to view the user's wall) this acts as a restriction similar to password protection on a BBS.

124. *Crispin*, 717 F. Supp. 2d 981–82 (citing *Kaufman*, 2006 WL 2807177, at *5).

2. Private Messaging Service

The court held that there was no distinction between both Facebook's and MySpace's private messaging service and a traditional web-based e-mail service.[125] Because providers of such traditional e-mail services are undisputedly ECS providers there was no doubt that Facebook and MySpace were ECS providers with respect to that service. [126]

B. Was the Information Sought in Storage as Defined by the Statue?

Determining if the entity provides either an ECS or RCS service is only the first stage in determining if communications are covered by the SCA; even if an entity is such a service it is only prohibited from disclosing information held in certain forms of storage. An ECS is only prohibited from disclosing information in "electronic storage."[127] The SCA provides two definitions of electronic storage. The first definition of storage ("type A" storage) includes "any *temporary, intermediate* storage or a wire or electronic communications incidental to the transmission therefore."[128] The second definition of electronic storage ("type B" storage) is "any storage of such communication by an electronic communication service for purposes of *back-up protection* of such communication."[129] In contrast an RCS is only prohibited from disclosing information held in "remote storage."[130]

125. *Id.* at 982.

126. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902 (9th Cir. 2008); Theofel v. Farey-Jones, 359 F.2d 978, 1982 (9th Cir. 2004); *see also* PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 584 (2d ed. 2004).

127. *See supra* notes 79–80 and accompanying text.

128. 18 U.S.C. § 2510(17)(A) (emphasis added).

129. *Id.* at § 2510(17)(B) (emphasis added).

130. *Id.* at § 2702(a)(2)(B).

1. E-Mails

Unopened e-mails have posed few analytical problems for the courts; a clear majority of jurisdictions hold that unopened e-mails are in "electronic storage" for the purposes of the Stored Communications Act.[131] Specially, most courts have held that unopened e-mails are held in type A, temporary and intermediate storage.[132] To fully understand the courts' reasoning, a brief overview of how e-mail works is necessary.[133] In short, after a message is sent by the sender, it is stored on the ISP's server; however, this particular form of storage ceases when the message is delivered, i.e., when it is retrieved by the intended recipient.[134] Therefore the courts have held that this form of storage is the archetypal example of Type A "temporary and intermediate" storage.[135]

Whether or not opened e-mails are also held in electronic storage has been a more contentious question. Generally, all courts agree that an opened e-mail does not fit within the definition of type A storage.[136] Therefore, whether a communication is in

131. *See, e.g.*, Theofel v. Farey-Jones, 341 F.3d 978, 984–85 (9th Cir. 2003); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635–36 (E.D. Pa. 2001); *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001).

132. *Theofel,* 341 F.3d 984-85; *Fraser*, 135 F. Supp. 2d at 635–36; *In re Doubleclick*, 154 F. Supp. 2d at 511–12.

133. This Comment only details enough of the basics necessary for an understanding of the case law. For a more detailed analysis see generally David J. Loundry, *E-Law 4: Computer Information Systems Law and System Operator Liability*, 21 SEATTLE U. L. REV. 1075 (1998).

134. *Email Sever FAQ – Part One*, VICOMSOFT (2002), http://www.vicomsoft.com/downloads/learning/email_qa.pdf; *Email Sever FAQ – Part Two*, VICOMSOFT (2002), http://www.vicomsoft.com/downloads/learning/email2_qa.pdf.

135. *See, e.g.*, *Theofel*, 359 F.3d at 1075 (9th Cir. 2004).

136. Once an e-mail has been opened its "continued storage [can]not be construed as 'temporary' or 'incidental to' [its] transmission, [and therefore is not in Type A storage]." Flagg v. City of Detroit, 252 F.R.D. 346, 361 (E.D. Mich. 2008). Other courts agree, as did a house committee: "'[T]emporary, intermediate storage' describes an e-mail message that is being held by a third party Internet service provider until it is requested to be read." *In re*

"electronic storage" (and in turn whether an entity can be classified as an ECS) depends upon whether the opened e-mail is held in the other type of electronic storage—type B storage. Type B storage is "any storage of [a] communication by an electronic communication service for purposes of back-up protection of such communication."[137] Unfortunately, neither the SCA itself, nor its legislative history, nor any court interpreting the Act has given a precise definition of "back-up protection," which has led to varying approaches to this issue.[138] Such was the judicial landscape that the *Crispin* court found itself facing when it addressed this question.

Previously, the Ninth Circuit had held that a copy of a communication stored on an ISP's server *may* be for back-up purposes, even if that communication had already been read.[139] In *Theofel v. Farey-Jones*, the court held that such a communication is held as a back-up because an "obvious purpose . . . is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from [his] own computer."[140] Because this back-up function was *a* purpose of storage, even if not the sole purpose, the communication was in storage, and therefore the ISP was acting as an ECS.[141] Similarly in *Quon v. Arch Wireless Operating Co.*, the Ninth Circuit held that permanent "archiving" of text messages by a pager service could be for "back-up" purposes.[142] The *Quon*

Doubleclick, 154 F. Supp. at 512 (quoting H. REP. NO. 106-932, at 11 n.7 (2000)).

137. 18 U.S.C. § 2510(17)(B).

138. Crispin v. Christian Audigier Inc., 717 F. Supp. 2d 965, 983 (C.D. Cal. 2010) (citing Fraser v. Nationwide Mut. Ins. Co., 352 F.3d, 107 114 (3d. Cir. 2003)).

139. *Theofel*, 359 F.3d at 1075.

140. *Id.*

141. *Id.* Also the court noted that there was nothing in the Act that required the back-up to be for the benefit of the ISP as opposed to the user. *Id.*

142. 529 F.3d 892, 901 (9th Cir. 2008) ("We turn to the plain language of the SCA, including its common-sense definitions, to properly categorize Arch Wireless. An ECS is defined as 'any service which provides to users thereof the ability to send or receive wire or electronic communications.' . . . On its face, this describes the text-messaging pager services that Arch Wireless provided . . . . Contrast that definition with that for an RCS, which 'means the provision to

court rejected the idea that archival necessarily suggested "permanent storage," as opposed to "back-up storage," the former of which would transform the entity into an RCS provider, and therefore subject to lesser restrictions on disclosure of information.[143]

But other courts have disagreed and distinguished the *Theofel/Quon* approach. Primarily those courts have noted that *Quon* appeared to oversimplify the issue, and that the so-called "common sense definitions" it applied in determining whether an entity is providing "back-up storage" or "remote storage" (and therefore whether an entity is an ECS or an RCS) were flawed.[144] Also, those courts, most notably the court in *United States v. Weaver*,[145] made clear that court's reasoning in *Theofel* "relie[d] on the assumption that users download e-mails from an ISP's server to their own computer."[146] The difference between web-based and non-web based e-mail providers is key.[147] In contrast to the user in *Theofel*, who had downloaded his e-mails to his own computer, in

---

the public of computer storage or processing services by means of an electronic communications system.' . . . Arch Wireless did not provide to the City 'computer storage'; nor did it provide 'processing services.' By archiving the text messages on its server, Arch Wireless certainly was 'storing' the messages. However, Congress contemplated this exact function could be performed by an ECS as well, stating that of this an ECS would provide (A) temporary storage incidental to the communication; and (B) storage for back-up protection.").

143. *Id.*

144. By applying these "common sense definitions," the *Quon* court attempts to determine what kind of provider an entity is in a vacuum, without considering the exact role the entity plays at a specific time, with regards to a specific piece of information. Other courts have eschewed this approach. "Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself." *In re* United States, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009).

145. 636 F. Supp. 2d 769 (C.D. Ill. 2009).

146. *Id.* at 772.

147. See Web-Based E-mail (Hotmail) VS Desktop E-mail (Outlook), ZHACKS.com (Mar. 08, 2010), http://www.zhacks.com/tag/compare-web-and-desktop-email/. A user of a web-based e-mail provider does not download his/her messages, instead they are stored solely with the provider. However a user of a non-web based e-mail service actually downloads his e-mails to his own personal computer. *Id.*

Weaver the party was using a web-based e-mail service. Therefore, the defendant in *Weaver* had not downloaded his e-mails; instead, the communications were held by the provider. The court held that when a user stored his e-mails solely with the entity in question, the entity is not providing a back-up, but is instead a form of storage; therefore, it is a functioning as RCS.[148] In other words, at the time that the e-mails were opened and stored solely with the e-mail provider, the entity "ceased to be an ECS provider and became an RCS provider."[149] The court in *Flagg v. City of Detroit* agreed with the *Weaver* court logic.[150] Both of these courts distinguished *Quon*, noting its application to be excessively rigid and at "unitary."[151]

148. *Weaver*, 636 F. Supp. 2d at 772. Importantly in distinguishing *Theofel*, the *Weaver* court also noted that web-based e-mail is now the default type of internet service. *Id.* "Thus, unless a Hotmail user varies from default use, the remote computing service is the only place he or she stores messages." *Id.* James Dempsey puts this distinction in context. "In the past, particularly at the time when [the Stored Communications Act] was written, many e-mail users accessed their e-mail by downloading it onto their personal computers. . . . Now, many users [do not, and their] e-mail . . . sits [solely] on a third party server." James X. Dempsey, *Digital Search & Seizure: Standards for Government Access to Communications and Associated Data*, 970 PLI/Pat 687, 707 (2009). The *Weaver* court explicitly noted the change in technology and sought to keep abreast of it when coming to a decision.

149. *Crispin v. Christian Audigier Inc.*, 717 F. Supp. 2d 965, 985 (C.D. Cal. 2010) (discussing *Weaver*, 636 F. Supp. 2d at 769).

150. Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008). In *Flagg* the entity in question ("SkyTel") had been providing the city of Detroit with text messaging services. *Id.* at 362–63. By the time the law suit was bought SkyTel had ceased to be an active provider of messaging services; however, it did still maintain a database of messages that had been sent and received during the service contract. *Id.* at 363. The court held that by the time of the suit SkyTel had become an RCS provider – there was not and could not be any "back-up" as the original messages no longer existed. Rather it now served as a "virtual filing cabinet" or remote storage location for the city, a classic RCS function. *Id.*

151. By focusing on the original purpose of the entity the *Quon* court fails to take into account that the SCA can apply differently to different copies of communications at different times. Also, this approach has been criticized as "unitary" in so much as it tends to suggest that "service providers contract with their customers to provide either an ECS or and RCS, but not both." *Id.* at 362. The Act's proper focus is on the "specific type of [storage] being provided with

The *Crispin* court came down in favor of the *Flagg/Weaver* approach. It held that until the messages were opened, they are in "temporary and intermediate" storage and that therefore Facebook and MySpace were acting as ECS providers. But it also held that once the private messages had been opened by Crispin, they were neither in "temporary intermediate storage" nor in "back-up storage," and that the entities providing those services were not acting as ECS providers.[152] Instead, the messages were held in remote storage, and the entities were operating as RCS providers.[153]

2. Wall Posts/Comments

According to the *Crispin* court, "the Facebook wall and MySpace comments present a distinct and [even] more difficult problem"[154] than private messages. Although it noted that many courts had previously held that a BBS is "the paradigmatic type of entity covered by the SCA"[155] it found itself faced with a dearth of case law providing adequate discussion as to the precise theory under which of the SCA's protections apply—that is, whether they are in ECS "electronic storage" or RCS "back-up storage."[156] In

---

regard to a particular communication [at a particular time, and not] upon broad notions of the service that this entity generally or predominantly provides. *Id.*

152. *Crispin*, 717 F. Supp. 2d at 987.

153. However, in so holding the *Crispin* court made it clear that its decision was also consistent with *Theofel*. It noted a Ninth Circuit amendment of the original *Theofel* decision which made clear that a service provider could be both an ECS and an RCS, and that if a user stores communications solely with an RCS, it is not being held for "back-up" purposes. *Id.* (citing *Theofel*, 359 F.3d at 1076–77). This amendment clarified that the original *Theofel* was not unitary, but only appeared that way due to the facts of the case. *Id.*

154. *Id.* at 988.

155. *Id.*

156. *See id.* Further complicating matters, of the few decisions that had been given, there had been several directly conflicting decisions, none of which offer any reasons for the outcome given. The court in *Konop* treated a BBS on a website as an ECS provider after holding that information thereon was held in "electronic storage." Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002). However, it "did not indicate whether th[is] storage was [type A] temporary and immediate storage or [type B back-up storage]." *Crispin*, 717 F.

response to this ambiguity the *Crispin* court first sought to determine if the information was being held in "electronic storage," the more restrictive of the two types of storage.

Unlike e-mail which is stored with an ISP while waiting delivery to its final destination, an electronic bulletin board is the final destination for a post.[157] In other words, because a wall post does not need to be opened, there is no intermediate step in which it is held pending delivery and consequently is never in type A temporary intermediate storage. Consequently, the court held that in the context of electronic bulletin boards and bulletin board services, there is never type A temporary and intermediate electronic storage.[158]

However, the court did find that Facebook wall postings and MySpace comments are held in type B back-up electronic storage, and therefore these two entities were acting as ECS providers.[159] The courts reasoning was short, stating that precedent dictated "that a user's or an ECS provider's passive decision not to delete a communication after it has been read by the user renders that communication stored for back-up purposes as defined in the statute."[160]

The *Crispin* court relied on the precedent in *Konop v. Hawaiian Airline, Inc.*[161] In *Konop* the court held that information held on a bulletin board service was held in electronic storage, but did not further explain whether this was because the communications were in type A storage or in type B storage.[162] Nonetheless, the *Crispin* court took note of this holding and then used two further steps in a

---

Supp. 2d at 988 (citing *Konop* 302 F.3d at. 879). Distinctly, a federal district court in Texas summarily concluded that a BBS is an RCS provider on the basis that it provides only remote storage. Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994).

157. *Crispin*, 717 F. Supp. 2d at 988 (citing *Snow v. DIRECTV, Inc.*, No 2:04-CV-515FTM33SPC, 2005 WL 1226158 at *3 (M.D. Fla. May 9, 2005) (finding that nobody could "allege that the messages are being stored [on a BBS] while waiting to be transferred to [another] final destination.")).

158. *Id.* at 988–89.

159. *Id.* at 989.

160. *Id.* at 989 (referring to § 2510 (17)(B)).

161. 302 F.3d 868 (9th Cir. 2002).

162. *Id.* at 879.

chain of reasoning to get from the general rule handed down in *Konop* to its outcome.

First, given that both the *Crispin* court (along with many others) had already decided that there can be no type A storage in the context of bulletin board services,[163] the court held that logically *Konop* must be interpreted as "holding that the postings [on a BBS], once made, are stored [in type B storage,] for back-up purposes."[164] Second, it reiterated that because "a BBS post is in all material ways analogous to a Facebook wall posting or MySpace comment" it is an inescapable conclusion that such comments and wall postings are also being held for back-up purposes.[165] While this essentially linear train of reasoning is open to criticism,[166] it suggests that the court was determined to apply the SCA whenever possible and that it was in favor of granting the protections that the SCA offers.

The court additionally committed itself to this position later in the decision, when it held that alternatively "Facebook and MySpace are RCS providers as respects the wall postings and comments."[167] The court analogized these wall postings to storage of user-created videos on YouTube.[168] In both cases, the entity provides a storage service for a user who had granted limited access to the content to a prescribed group of people, in short a classic RCS service.[169] The court further held that Facebook and YouTube were no less RCS providers simply because the media that they stored was visual.[170]

---

163. *Id.*

164. *Crispin*, 717 F. Supp. 2d at 988.

165. *Id.*

166. *See infra* notes 177–183 and accompanying text.

167. *Crispin*, 717 F. Supp. 2d at 990.

168. *Id.* (citing Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008)).

169. *Id.*; *Viacom Int'l Inc.*, 253 F.R.D. at 264.

170. The court reasoned that the very point of storage (i.e., retrieval) would be made impossible without the data being visual in some manner. *Crispin*, 717 F. Supp. 2d at 990 (citing Flagg v. City of Detroit, 252 F.R.D. 346, 359 (E.D. Mich. 2008) ("[I]t is difficult to see how an archive of text messages would be of any use or value to a customer if the service provider did not also offer a mechanism for retrieving messages from this archive.").

By providing this alternate justification for applying the SCA to wall postings, the court further protected users' expectations of privacy. This was a theme throughout the *Crispin* decision in which the court took an expansive view of the SCA. Ultimately, the court held that social media sites operate as ECS providers with respect to unopened e-mails, wall posts, and comments, and were acting as RCS providers with respect to opened e-mails and private messages. Therefore, the SCA could be applicable to every piece of information that a user uploads onto a social media site.[171]

IV. ANALYSIS

This part analyzes the *Crispin* decision, exploring not only the advances that the case made to SCA jurisprudence, but also the limitations inherent in the decision. It also highlights some of the policies underlying the court's decision and attempts to use these to predict how the case may influence later decisions and how the law in this area may develop.

A. Opened E-mails

As noted above, the *Crispin* court was the first to consider whether the SCA should apply to social media sites. As a result, the case turned on principles of statutory interpretation as much as prior case law (and therefore also the extent to which the court was willing to try to enforce the purpose behind the statute). Specifically, the amount of protection that the SCA would afford to opened e-mails, if any, depended entirely on how the court chose to interpret and apply the term "electronic storage." The *Crispin* court held that e-mails or private messages that have been previously opened are not held in electronic storage (i.e., were neither stored temporarily nor for back-up purposes); therefore, Facebook and MySpace were not acting as ECS providers with respect those messages.[172] However, the court also held that any

171. Subject to other requirements, such as the entity being public, etc. *See supra* notes 62–104 and accompanying text.

172. *Crispin*, 717 F. Supp. 2d at 986.

archived copies of these opened messages that Facebook and MySpace had kept were being held in remote storage, meaning that Facebook and MySpace were instead acting as RCS providers with respect to these opened messages.[173] This was essentially a compromise, limiting, but still providing a basic level of enhanced protection for opened e-mails.

The court's interpretation of "electronic storage" in *Crispin* is sound, and is the most consistent with the Act. Primarily, the decision definitively and explicitly rejected the so-called "unitary approach" of *Quon* and firmly established that the type of storage that an entity is providing is a context sensitive inquiry. There is little doubt that this is what Congress intended.[174] In addition, by declining to hold that opened e-mails are held in "back-up" storage, the court avoided an overly broad definition of that term. Although the court based its decision on common sense and plain language,[175] its impact has significant ramifications. If an entity is deemed to be holding a communication as a back-up, even if the user does not have a copy, then the term "storage" (used to determine when an entity is proving an RCS) would become

---

173. *Id.* at 990.

174. The drafters of the SCA apparently considered how the Act would apply when a recipient opened an e-mail but then left it on the ISP server:

> Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by section 2702(a)(2).

United States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (quoting H.R. Rep. No. 99-647, at 65 (1986)). Accepting that a private message on Facebook or MySpace and a traditional e-mail are sufficiently similar, this is strong evidence that the *Crispin* court adopted the correct approach. *See also* Kerr, *supra* note 44, at 1215.

175. Because most users have web-based e-mail, they do not actually keep a copy of their e-mails; rather the sole copy is in the possession of the provider in question. Logically then, an entity cannot be keeping that message for "back-up" purposes—one cannot back up something that does not exist. Rather, the entity is providing a storage service for that e-mail so that the use can access a copy at any time.

redundant. Consequently, if the terms "back-up" and "storage" were interchangeable, the distinction between ECS and RCS providers would become illusory, rendering the less restrictive provisions relating to RCS providers superfluous.[176] The court manages to sidestep this problem and avoids violating the generally accepted canon of statutory construction that a statute should be read as a whole and to avoid redundancy. Although this resulted in opened e-mails having only the lesser protections associated with RCS providers, the decision is undoubtedly correct in view of both the statutory text and common sense.

In addition, the court's definition of "remote storage" was well considered. By classifying social media sites as RCS providers with respect to open e-mails, it still allows a basic level protection for users' information, and buttresses the Fourth Amendment right to privacy. In essence, the court took a middle ground, choosing the most logical position in light of the statute's language and the aims that Congress sought to realize in its enactment.

B. Wall Postings

As noted above, the court held that information held on a wall posting such as a bulletin board was being held in electronic storage.[177] In reaching this conclusion, the court relied on precedent from *Konop* without further exploration of the Act and without forging any new ground.[178] While the outcome was most likely correct, one unfortunate side effect of the court's borrowed reasoning was that it robbed the court of the opportunity to explore the issue in greater detail. While the chain of reasoning from *Konop* was strong, it was completely predicated upon the assumption that *Konop* is a correct statement of the law.

176. To explain, consider the *alternative* holding—that unopened e-mails are held for back-up purposes even on web-based systems in which the user does not retain a copy. In this scenario, the fact that the entity holds the e-mail as a back-up would mean that it is held in type B electronic storage under 18 U.S.C. § 2510(17)(B). Consequently, the entity will be providing an ECS service. It would be unnecessary to consider whether the e-mail was also held "in storage" as an RCS because RCS providers offer less protection for the user.

177. *Crispin*, 717 F. Supp. 2d at 989.

178. *See supra* notes 162–166 and accompanying text.

Obviously the court's duty was to apply the precedent that binds it. However, by not taking the time to fully explore the issue, the court does not add much clarity to an area desperately in need of some guidance, a fact that the court candidly acknowledged.[179]

This reasoning aside, it is fair to say the court nonetheless arrived at the correct outcome. Primarily, it is clear that Congress intended for the SCA to cover private electronic bulletin boards; the relevant legislative history shows an unambiguous intent to try to provide protection for information that the author tries to keep private.[180] And in turn, the court's decision furthers the simple policy behind the Act: to ensure privacy for certain communications when the Fourth Amendment fails.

However, there are perhaps alternate reasons for the court's decision that social media sites are covered by the SCA. The simple policy that was once behind the Act has been superseded by new and more complex factors, and it would be naïve to believe that these issues did not also play a role in the court's decision. Stated bluntly, social media sites are now an industry in and of themselves.[181] They are at the cutting edge of modern digital communications technology, and an influx of subpoenas would

179. *Crispin*, 717 F. Supp. 2d at 988 ("As the Ninth Circuit . . . observed, 'until Congress brings the laws in line with modern technology, . . . [this] will remain a confusing and uncertain area of law'" (quoting Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002))).

180. *Konop*, 302 F.3d at 875 (quoting S. Rep. No. 99-541, at 35-36: "This provision [of the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public.").

181. *See e.g.*, *Social Media Marketing Report*, MARKETING WHITE PAPERS (Nov. 06, 2010), http://marketingwhitepapers.s3.amazonaws.com/SocialMediaMarketingReport2010.pdf. In 2009, social media games such as Farmville and Mafia Wars generated an estimated $725 million in the United States alone, an amount that is expected to triple by 2012. Paul Verna, *Social Gaming: Virtual Crops Yield Real Profits*, EMARKETER (Oct. 19, 2010), http://www.researchandmarkets.com/reportinfo.asp?cat_id=0&report_id=1295470&q=social%20gaming%20&p=1. It is predicted that in 2012 U.S. advertisers will spend $2.6 billion on social media sites. *Social Networking*, PROCON.ORG, http://socialnetworking.procon.org/#20 (last visited Nov. 22, 2011, 5:23 PM).

undoubtedly have a negative effect on service providers.[182] The concern is that excessive subpoenas could impose a burden on social media sites, not only limiting their economic productivity, but also their contributions to technology.[183]

But the balance is a fine one. While there is no doubt that social media sites have made positive contributions to society, it does not necessarily follow that as a result they should be excused from the

182. *See* O'Grady v. Superior Court of Santa Clara County, 44 Cal. Rptr. 3d 72, 89 (Cal. Ct. App. 2006):

> We also note the assertion by amicus curiae United States Internet Industry Association (USIIA) that civil subpoenas are often served on service providers and that compliance with them would impose severe administrative burdens, interfering with the manifest congressional intent to encourage development and use of digital communications. The severity of this burden cannot be determined from this record, but the threat of routine discovery requests . . . would seemingly permit civil discovery from the service provider whenever its server is thought to contain messages relevant to a civil suit.

Id. Although the *Crispin* court makes no specific reference to such considerations its decision is certainly in accord with the sentiment expressed by the *O'Grady* court.

183. It would appear that Facebook agrees – it does not seem to welcome subpoena requests for information. Until recently, its "Safety for Law Officers" page "'urge[ed]' parties to civil litigation resolve their discovery issues without involving Facebook." *Digital Forensics & eDiscovery Advisory 1.14: Facebook Subpoenas*, CONTINUUM WORLDWIDE (Oct. 13, 2010), available at http://www.continuumww.com/Home/Resources.aspx. It further stated that "[a]lmost without exception, the information sought by parties to civil litigation is in the possession of, and readily accessible to, a party to the litigation" before concluding that "[r]equests for account information are therefore better obtained through party discovery." *Id.* Although Facebook has since removed that page and now promotes its clear policy of complying with legal requests, it still dissuades users from issuing a subpoena to get information. Facebook's manual, along with the Safety for Law Officers page make very apparent (1) its duties and limits under the SCA, (2) the long list of requirements for a subpoena stemming from § 2703(c), and (3) that it "reserves the right to charge a reasonable fee" for this service. FACEBOOK, http://www.facebook.com/safety/groups/law/guidelines/ (last visited Nov. 21, 2011 3:15 PM). *See also Obtaining Records From Facebook, LinkedIn, Google and Other Social Networking Websites and Internet Service Providers*, FOR THE DEFENSE, available at http://forthedefense.org/file.axd?file=2010%2F5%2FObtaining+Records+From+Social+Networking+Websites.pdf.

burdens answering subpoenas. Arguably society's interest in justice for parties in civil suits should trump this fear if the information sought really is unobtainable elsewhere. In light of this balance, the court's resolve to extend this privacy (and arguably protect the social media sites) will be tested as Facebook's privacy settings continue to evolve. The *Crispin* court seems to suggest that as long as access to a group is controlled, the SCA will apply.[184] Indeed, the court stated that "the number of users who can view the [wall posting] has no legal significance."[185] It further stated that "basing a rule on the number of users who can access information would result in arbitrary line-drawing," and could work to discriminate larger firms with thousands of employees who can access the stored information, as this could exclude the firm from the statute's reach.[186]

While the logic of this statement is sound, the practical implications of such a rule may be unworkable. Shifting from an analytical perspective to a common sense approach highlights the other side of this debate. If the purpose of the SCA is to provide a Fourth Amendment-like expectation of privacy, it is fair to ask whether the SCA should protect users who share information with thousands of people, even if those people have been handpicked and individually approved. How reasonable can it be it to expect that information to stay private? And how legitimate is the distinction between the user who creates a completely open Facebook group and a user who indiscriminately accepts everyone and anyone into that group upon request?[187]

---

184. *Crispin*, 717 F. Supp. 2d at 991.

185. *Id.* at 190.

186. *Id.*

187. This will become even more of an issue after the Sixth Circuit's landmark case in Warshak v. United States, *631 F.3d 266* (6th. Cir. 2010). In that case the Sixth Circuit held that a user does have a Fourth Amendment right to privacy in e-mails sent, even when sent through a third party ISP. *Id.* at 282. The *Warshak* decision—if accepted and applied in more jurisdictions—could very well act as grease on the slippery slope. If the courts accept that users have a reasonable and legitimate expectation of privacy in e-mails sent, the next issue will become whether users have the same expectations in wall posts and photo-albums posted online that have only limited access to other users. And if protection is forthcoming, how limited will these groups have to be, and what

How a court would deal with these issues remains unknown. It might even be fair to say that under the current statutory scheme these questions have no satisfactory answer. After putting the problems of judicial interpretation and general inconsistency aside, the root of the problem can still be traced back to the SCA. It is simply not designed to deal with modern technology.[188] The Act itself does not even use the term "e-mail," let alone "social media site."[189] Mark Zuckerberg—founder of Facebook—was barely two when the SCA was passed. And the rate of technological advancement is only increasing.[190] Simply put, the SCA is ill-equipped to provide a solution. Although the *Crispin* court probably came to the right decision, the means it used to get there were strained. The next part of this Comment addresses the practical problems and real-life impact that this confusion and uncertainty has not only on the legal system, but also on society in general.

---

criteria will be used to judge "exclusiveness"? Current law suggests that the actual number of persons able to view these postings was not dispositive and had no legal significance. The court noted that basing a legal rule on the amount of people who could view the messages would result in arbitrary line drawing. Instead the court focused on the statutory inquiry as to whether the general public had access to the information: "It shall not be unlawful under [the SCA] for any person . . . to . . . 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." 18 U.S.C. § 2511(g)(i). Therefore it seems that so long as the user maintains some minimal control over privacy settings the court will find sufficient privacy. This argument is perhaps disingenuous however; if a user indiscriminately accepts all friend requests, it is hard to argue that the user expects privacy, and that the information is not readily accessible to the public. Of course, from a purely practical standpont this may be a moot point; the more people that have access to the wall, the more likely that it will be directly discoverable from one of them (independent of the SCA).

188. *See* Kerr, *supra* note 44, at 1233–42.

189. *See* Stored Wire and Electronics Communications and Transaction Record Access (Stored Communications Act), Pub. L. No. 99-508, 100 Stat. 1860 (codified as amended in scattered sections of 18 U.S.C.).

190. Ray Kurzweil, *Time to Embrace Technological Change*, NATIONAL PUBLIC RADIO (Jan. 24, 2011), http://www.npr.org/templates/story/story.php?storyId=5563001.

V. IMPACT

A. Necessity of Reform

1. Legal Perspective

It is clear from the mental and verbal gymnastics and inconsistent results reached by different courts that this is an old and outdated statute. The *Crispin* court explicitly acknowledges this.[191] The court also acknowledged the need for reform, admitting that until a new framework is implemented this will remain "a confusing and uncertain area of the law."[192] The *Crispin* court is not alone in this sentiment. Many other scholars, most notably Professor Orin S. Kerr, have also called for reform to the SCA.[193] This paper agrees with that position, but further contends that that reform must come from statute as opposed to piece-by-piece change effected through judicial activism. First, several courts have already grappled with the problems inherent in applying the SCA to modern technology and have had little success. Not only have courts found it difficult to interpret the Act, but those difficulties have been magnified into an inconsistent and confusing body of case law.[194] At one extreme, a Pennsylvania

191. *Crispin*, 717 F. Supp. 2d at 988 ("The difficulty in interpreting the statute is compounded by the fact that the [SCA] was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like [Facebook and MySapce].") (internal quotations omitted).

192. *Id.*

193. *See* Kerr, *supra* note 44, at 1233–42, calling for among other things increase protections, simplification, and a suppression remedy. This last reform would fit particularly well with the court's and Act's apparent intent to fully protect privacy. *See also* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820–21 (2003)).

194. "Courts have taken inconsistent approaches in applying the SCA to social network information and many of these cases have obvious flaws. Even the *Crispin* decision, which represents a step in the right direction, provides incomplete guidance in determining whether social networks should be protected from disclosing certain content under the SCA." Ward, *supra* note 5, at 588.

court recently held that everything posted a social media site is essentially discoverable because the user has no legitimate expectation of privacy.[195] At the other end of the scale, the Sixth Circuit Court of Appeals has recently held that a user has a complete expectation of privacy in e-mails sent, and therefore, in so much as the SCA allows law enforcement agencies to acquire content sent through e-mail without a warrant, it is unconstitutional.[196] This inconsistency is unacceptable in such an important area of the law, and the courts' inability to come to create a uniform jurisprudence suggests that the legislature must take the initiative to introduce a comprehensive solution to the problem. Second, a comprehensive and wholesale reform would result in greater consistency in this area of law than piecemeal decisions.[197] In an area of such legal significance and practical importance, users of technology deserve to know how just how private their communications really are.[198] Finally, with the constitutionality of this area still unclear,[199] it is for the legislature

195. McMillen v. Hummingbird Speedway, Inc., Case No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *3–4 (Pa. D. & C. Sept. 9, 2010). Note however that this decision appears to be untenable for several reasons, not least for the fact that is clearly violates the SCA. Eric Goldman, *Court Orders Disclosure of Facebook and MySpace Passwords in Personal Injury Case – McMillen v. Hummingbird Speedway*, TECH. & MARKETING L. BLOG (Oct. 30, 2010), http://blog.ericgoldman.org/archives/2010/10/court_orders_di_1.htm.

196. Warshak v. United States, 631 F.3d 266, 288 (6th. Cir. 2010).

197. Even some of the more reasoned cases in this area cannot alone provide the guidance and clarification needed. *See generally* Ward, *supra* note 5, at 588; *About the Issue*, DIGITAL DUE PROCESS: MODERNIZING SURVEILLANCE LAWS FOR THE MODERN AGE, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Nov. 18, 2011 07:23 AM).

198. When it comes to internet privacy, "[everyone] deserve[s] clear and simple rules." *Id.*

199. With last year various courts have given conflicting decisions as to whether the Fourth Amendment applies directly to e-mail let alone whether the SCA applies. Traditionally e-mails have not been protected by the Fourth Amendment as this requires disclosure to third party. MATHEW BENDER, PRIVACY LAW AND THE USA PATRIOT ACT § 2.03 (2011). But a recent Sixth Circuit decision held that a user does have a privacy interest in an email sent. *Warshak*, 631 F.3d at 288. While the law is unclear, one thing is certain—as yet there is no definite answer to many of these important questions.

to make the reform. In such an uncertain area, any reform must come from a body that is not only directly elected, but who has the resources to properly investigate the necessary changes, adequately analyze proposed changes, and to authoritatively implement the change.

2. A Policy Perspective

The SCA needs to be reformed through legislation. But the need for reform runs deeper than a mere theoretical interest in the uniformity and clarity of decisions, and this Comment is designed to examine this issue from more than a purely legal standpoint. There are issues with the SCA that have consequences far outside the courtroom. Law is the bedrock of society, and it must provide a solid foundation upon which companies of all sizes are able to build, and this solid foundation only becomes more necessary as we continually strive to build higher and greater things. One of the newest trends in the computer and technology fields is the rapid expansion of "cloud computing."[200] As this technology has developed, more and more businesses have sought to take advantage of this powerful tool,[201] which promises potential savings in costs, time, productivity, and flexibility.[202] But learning a valuable lesson from the foolish man who build his house on

200. Cloud computing is a modern form of data storage. It is "an emerging architecture by which data and applications reside in cyberspace, allowing users to access them through any web-connected device." Diane Murley, *Law Libraries in the Cloud*, 101 LAW LIBR. J. 249, 249–50 (2009) (quoting John B. Horrigan, *Use of Cloud Computing Applications and Services*, PEW INTERNET & AMERICAN LIFE PROJECT (Sept. 12, 2008), http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services/Data-Memo.aspx. For a more detailed overview, see David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2216–18 (2009).

201. *Comments on Information Privacy and Innovation in the Internet Economy*, DIGITAL DUE PROCESS 5 (June 14, 2010), http://www.digitalddueprocess.org/files/NTIA_NOI_061410.pdf.

202. David Raths, *Will Clouds Reign?*, 6 PUB. CIO 18, 22–23 (2008); Dan Lohrmann, *How Safe is Cloud Computing?*, PUBLIC CIO (Jan. 26, 2011), http://www.govtech.com/pcio/How-Safe-is-Cloud-Computing.html.

sand,[203] companies have been slow to fully embrace cloud computing over fears about privacy.[204] Without a clear and consistent body of law concerning disclosure of information stored "in the cloud," fewer companies are using this technology.[205] Moreover, companies will be less willing to use the versions that are available.[206] The knock-on effects of this are no less troublesome; as the legislature fails to address this cutting edge area, it is the United States that is suffering.[207] Potential businesses are moving abroad and the domestic economy is missing out on this $100 billion dollar market.[208]

Clarity is not the only major shortcoming of the SCA. Even in parts that have been definitively interpreted the law still fails to create a modern standard for privacy on the Internet. And these drawbacks are not limited to faceless corporations and large-scale issues; the lack of guidance also has an impact on an individual level. Privacy has famously been called "the right most valued by civilized men."[209] But as we store more information online instead of in paper form, that right is put in jeopardy, not because of an inherent shift in legal doctrine, but due to both legislative inaction and the rapidly evolving nature of the relevant technology. Until the legislature ends this reluctance to modernize the law and sets a workable and clear standard for Internet privacy, the potential benefits of new technology will never be fully realized.

---

203. *Matthew* 7:26.

204. *See* Horrigan, *supra* note 202, at 5.

205. *Id.* at 4.

206. *Id.*

207. Jeffery Rayport & Andrew Heyward, *Envisioning the Cloud: The Next Computing Paradigm*, MARKETSPACE, 38 (Mar. 20, 2009), http://marketspacenext.files.wordpress.com/2011/01/envisioning-the-cloud.pdf.

208. Markus Klems, *Merrill Lynch Estimates "Cloud Computing" To Be $100 Billion Market*, WEB2JOURNAL (Jan. 19, 2011), http://web2.sys-con.com/node/604936.

209. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). And it appears that this right is no less coveted in the internet domain; eighty-eight percent of Americans believe that internet users should be entitled to the same level of privacy protection as have traditionally been afforded to offline information, while only four percent actively disagree. *Results from June 4-7 Nationwide Poll*, ZOGBY INTERNATIONAL (June 7, 2010), http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf.

A prime example of how both individuals and companies are affected by both the courts' inability to tread a consistent path and the legislature's reluctance to provide them with an adequate map is the increasing use of location data. Amidst (and perhaps despite) cries of "Big Brother,"[210] cell-phone tracking technology has arrived, and is growing at a rapid pace.[211] This allows a user to be traced, and for anyone with permission, to determine exactly where he or she is at any given moment.[212] While many potential businesses have sought to capitalize on this potential new market,[213] many consumers have been wary, largely because the "laws are [ ] years behind technology."[214] For this market to reach its potential, the end users of the products have to feel confident that the information gathered is not going to be abused. Because location data is so easy to store and collate, without adequate privacy protections many consumers fear that their data will be mishandled.[215] Under the current law this fear is not ungrounded; location data is not "content information" and so is subject to the lesser protections of the SCA, if it applies at all.[216] Simply put,

---

210. Richard Ford, *'Big Brother' Database for Phones and E-mails*, THE TIMES (May 20, 2008), http://msl1.mit.edu/furdlog/docs/2008-05-20_times_dataveillance.pdf.

211. Michael B. Farrell, *Cellphone Tracking Services: Friend Finder or Big Brother?*, CHRISTIAN SCIENCE MONITOR (May 1, 2009), http://www.csmonitor.com/Innovation/Tech-Culture/2009/0501/cellphone-tracking-services-friend-finder-or-big-brother.

212. For more information, *see, e.g.*, *How Cell Phone Tracking Works*, TECH-FAQ, http://www.tech-faq.com/how-cell-phone-tracking-works.html (last visited Nov. 22, 2011).

213. The scale of this market *could* reach over twelve billion in the next three years. Robin Wauters, *Mobile Location-Based Services Could Rake in $12.7 Billion by 2014: Report*, TECHCRUNCH (Feb. 23, 2010), http://techcrunch.com/2010/02/23/location-based-services-revenue/.

214. Michael B. Farrell, *supra* note 211.

215. Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor & Norman Sadeh, *Location-Sharing Technologies: Privacy Risks and Controls*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 199, 199 (2010), http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

216. Ford, *supra* note 210. While not subject to the SCA the British government had even suggested a scheme whereby this information would be

under its current interpretation the SCA does not adequately guarantee the right to privacy, which is hampering, or at least delaying, technological advancement.[217] In many ways this is expected; most of current issues regarding the SCA involve technology that was not even considered possible, let alone in use at the time of the SCA's enactment. But in turn, that means these problems cannot be fixed by judicial interpretation of the SCA.[218] There exists a real need for a new framework that specifically deals with the new issues that have surfaced.

VI. CONCLUSION

Just as the Wiretap was considered obsolete in 1986, so too has the SCA met a similar fate.[219] But unlike 1986, when Congress realized that the then current law had become antiquated, the

---

kept on record for a period of time. *Id.* An overhaul of the SCA could help appease these fears in the United States.

217. DIGITAL DUE PROCESS, *supra* note 197.

218. Assuming that it could be properly called judicial interpretation at all. If judges are tasked with trying to fix issues that were unforeseen at the time of the SCA's enactment they would not be engaging in interpretation of the statute at all, but would cross the line into judicial activism, yet another reason for the legislature to step in.

219. Both scholars and judges alike have noted that the Stored Communications Act is unable to provide robust and adequate protections against government search of communications stored in a physical location but in an intangible form, predominantly online communications and e-mail conversations. "The Internet present[s] a host of potential privacy issues that the Fourth Amendment does not address. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th. Cir. 2008). "In *Konop*, the Ninth Circuit noted . . . the existing statutory framework is ill-suited to address modern forms of communication." Murray v. Fin. Visions, Inc., No. CV-07-2578-PHX-FJM, 2008 U.S. Dist. LEXIS 93419, at *15–16 (Nov. 6, 2008). *See also* Kerr, *supra* note 44, stating that the Fourth Amendment alone "cannot . . . provide robust protections for online communications for intangible property." In fact Kerr goes further, suggesting that the "the details of how the Internet works make it almost 'custom designed' to frustrate . . . protections in remotely stored files." *Id.* at 1212. Testimony has even been given to a U.S. House Judiciary Committee on the subject of how the SCA is obsolete. Fred H. Cate, *Stored Communications Act (SCA) Needs Revisions*, IU NEWSROOM (Sept. 23 2010), http://newsinfo.iu.edu/news/page/normal/15669.html.

current Congress has not had the same "noteworthy display of foresight,"[220] and seen the need for amendments to the SCA. In summary: inaction has led to obsolescence. "The [benefits of technology] should not come at the price of privacy."[221]

It is not the courts' place to overhaul this area. Such a complex and immense task falls clearly on the shoulders of the legislature. However, in the conspicuous absence of any action on the legislature's behalf, others they have picked up the torch.[222] Even the courts are starting to walk down paths of reform on which the legislature seem unwilling to tread.[223] One can certainly understand why the courts have taken on this role; interpretation has been needed, and the legislature has been slow to respond. But it is nonetheless important to realize this judicial action for what it is; a temporary respite as opposed to a final solution. Legislative action is needed lest the courts be forced into Congress' role.

Without doubt, the *Crispin* decision is a well considered opinion that will only gain importance as more courts are left to define the scope of electronic discovery rights in the field of social media sites. Similarly there is little doubt that *Crispin* will help guide other courts to a more thorough and considered approach to electronic communications of social-media sites. But it is important to remember that neither *Crispin*, nor any other court can provide definitive answers to the problems posed by the SCA. Instead, they have merely created a platform for legislative action. It can only be hoped that Congress takes note of this, and that

220. *See* Perez-Albuerne & Friedman, *supra* note 41, at 436.

221. *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on Courts, Civil Liberties and the Admin. of Justice of the H. Comm. on the Judiciary*, 111th Cong. 4–21 (2010) (Statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology), *available at* http://judiciary.house.gov/hearings/printers/111th/111-98_56271.PDF.

222. In the absence of any legislative action, various groups, distinguished scholars, and professors have repeatedly called for reform. See, e.g., Kerr, supra note 46, at 1232–33; Cate, supra note 225.

223. *See, e.g.*, the court's expansive view of the SCA in Crispin v. Christian Audigier Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010). For a more forceful (and less patient approach) see the recent Sixth Circuit decision in which parts of the SCA were recently held to be unconstitutional. Warshak v. United States, 631 F. 3d 266, 288 (6th. Cir. 2010).

through its completeness, its importance, and its admonishment of the Act as a whole, *Crispin* may help not only to guide future judicial opinion but also may eventually encourage and shape legislative reform.

*Simon M. Baker**

* J.D. Candidate 2012, DePaul University College of Law; LLB, University of East Anglia, England. Special thanks go to both Professor Paul McGrady and Aaron Dozeman for their help in developing this article. Thanks also to Dan Malachowski for his guidance early on, and to my lovely wife Rachel, for everything.