

2011

Who is Poking Around Your Facebook Profile? The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites

Lindsay S. Feuer

Follow this and additional works at: <http://scholarlycommons.law.hofstra.edu/hlr>



Part of the [Law Commons](#)

Recommended Citation

Feuer, Lindsay S. (2011) "Who is Poking Around Your Facebook Profile? The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites," *Hofstra Law Review*: Vol. 40: Iss. 2, Article 8.
Available at: <http://scholarlycommons.law.hofstra.edu/hlr/vol40/iss2/8>

This document is brought to you for free and open access by Scholarly Commons at Hofstra Law. It has been accepted for inclusion in Hofstra Law Review by an authorized administrator of Scholarly Commons at Hofstra Law. For more information, please contact lawcls@hofstra.edu.

NOTE

WHO IS POKING AROUND YOUR FACEBOOK PROFILE?: THE NEED TO REFORM THE STORED COMMUNICATIONS ACT TO REFLECT A LACK OF PRIVACY ON SOCIAL NETWORKING WEBSITES

I. INTRODUCTION

From the classroom to the courtroom, the explosion of social networking websites has changed the way people communicate.¹ Terms such as “friend request,” “poke,” “like,” “tweet,” “wall,” “app,” “blog,” “message,” “tag,” “profile,” “news feed,” and “status” have developed new meanings in society.² Social media websites comprise “three of the world’s most popular brands online.”³ In April 2010, Facebook⁴ was the third most popular brand online in the world and in December 2011, had a total of more than 845 million active users.⁵ Websites such as Facebook and Myspace⁶ have gained popularity by facilitating the ability

1. See danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 212 fig.1 (2007) (noting that the first social networking site, SixDegrees.com, was launched in 1997); Edward M. Marsico, Jr., *Social Networking Websites: Are MySpace and Facebook the Fingerprints of the Twenty-First Century?*, 19 WIDENER L.J. 967, 967 (2010).

2. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1145-50 (2009) (“Facebook has a reasonably comprehensive snapshot both of who you are and of whom you know.”); Stone Irvin, *A Drive-By-Tweet for Health Sciences*, EMORY HEALTH, Fall 2009, at 23, 23; *Friend*, TECHTERMS.COM, <http://www.techterms.com/definition/friend> (last updated Nov. 20, 2009); *Like*, FACEBOOK, <http://www.facebook.com/help/like> (last visited Apr. 20, 2012).

3. *Social Networks/Blogs Now Account for One in Every Four and a Half Minutes Online*, NIELSEN WIRE (June 15, 2010), <http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online/>.

4. *Fact Sheet*, FACEBOOK, <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22> (last visited Apr. 20, 2012) (“People use Facebook to stay connected with friends and family, to discover what’s going on in the world, and to share and express what matters to them.”).

5. *Id.*; NIELSEN WIRE, *supra* note 3.

6. *Terms of Use Agreement*, MYSPACE (June 25, 2009), <http://www.myspace.com/help/terms> (“Myspace LLC . . . operates Myspace.com, which is a social networking platform that allows Members to create unique personal profiles online in order to find and communicate with old and

to gather and share information with friends, family members, acquaintances, colleagues, and even complete strangers.⁷ Similar to a digital yearbook, social networking websites allow users to share their thoughts, emotions, and embarrassing photos instantly with one another and “post”⁸ them for their “friends” to view and comment.⁹

Although the social networking phenomenon has helped individuals communicate more efficiently, it has also presented “a new set of challenges.”¹⁰ Since social networking websites have become a popular method of communication, attorneys and law enforcement officials now review these websites frequently throughout the discovery process.¹¹ These websites provide valuable information about a person or entity and are viewed as “evidence-gathering gold mines.”¹² The abundance of information that is available, but not always easily accessible, has presented courts with the challenge of balancing the need for disclosure with an individual’s right to privacy.¹³

new friends.”). In 2010, Myspace dropped the capital “S” in “space,” therefore, throughout this Note, Myspace will be spelled as “Myspace” and not “MySpace.” John D. Sutter, *Praise for MySpace’s New Look—But That Logo?*, CNN (Oct. 27, 2010), http://articles.cnn.com/2010-10-27/tech/myspace.revamp_1_myspace-myspace-social-network.

7. Riva Richmond, *On Networking Sites, Learning How Not to Share*, N.Y. TIMES, Jan. 29, 2009, at B5 (noting how people are similar to “well-behaved kindergartners” and love to share).

8. *Statement of Rights and Responsibilities*, FACEBOOK, <http://www.facebook.com/legal/terms> (last updated Apr. 26, 2011) (defining “post” as a “post on Facebook or otherwise [made] available to us (such as by using an application)”).

9. See Evan E. North, Comment, *Facebook Isn’t Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1284-85 (2010).

10. See Steven C. Bennett, *Civil Discovery of Social Networking Information*, 39 SW. L. REV. 413, 413, 415 (2010); *Fact Sheet*, *supra* note 4.

11. Mark A. Berman, *The Ethics of Social Networking Discovery*, N.Y. L.J., Nov. 2, 2010, at 5. See also Marsico, *supra* note 1, at 967-68 (explaining how social networking websites have helped law enforcement professionals gather evidence); Andrew C. Payne, Note, *Twitigation: Old Rules in a New World*, 49 WASHBURN L.J. 841, 843 (2010) (noting how social networking websites have increased the availability of electronic information available on the Internet); John S. Wilson, Comment, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1207-08 (2007) (discussing challenges of electronic evidence as a result of modern technology).

12. Marsico, *supra* note 1, at 973. See also Berman, *supra* note 11.

13. See, e.g., *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010); *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 654 (Sup. Ct. 2010). See also Payne, *supra* note 11, at 860-61; Mark S. Sidoti et al., *How Private Is Facebook?*, N.Y. L.J., Oct. 4, 2010, at S2. See generally North, *supra* note 9.

The Stored Communications Act (the “SCA”),¹⁴ a component of the Electronic Communications Privacy Act of 1986 (the “ECPA”),¹⁵ is the primary federal statute governing online privacy protection and disclosure by an Internet Service Providers (“ISP”).¹⁶ Congress passed the SCA in 1986 in order to “address privacy issues” and “restrict disclosure of private communications by providers of electronic communications services.”¹⁷ The SCA was enacted to create “Fourth Amendment-like” privacy protections by balancing “the interest and needs of law enforcement, industry and the privacy interests of the American people.”¹⁸ Now that the SCA has celebrated its twenty-fifth birthday, there is a pressing need for statutory reform.¹⁹ Since its enactment more than a generation ago, the SCA has not kept up with the drastic changes in technology.²⁰

Part II of this Note examines the history of social networking websites and Facebook, in particular. It analyzes the various ways users share and communicate information on these websites. While users are able to manage their own privacy settings on Facebook, these settings are inadequate and do not provide users with a reasonable expectation of privacy.²¹ Part II also demonstrates how social networking websites have

14. See Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1860 (codified at 18 U.S.C. §§ 2701–2712 (2006 & Supp. IV 2011)). The statute is commonly referred to as the SCA, although this title does not appear within the statute. See COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP’T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 115 n.1 (3d ed. 2009) [hereinafter SEARCHING AND SEIZING COMPUTERS], available at <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>.

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

16. See Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212–13 (2004); William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1205 (2010).

17. Sidoti et al., *supra* note 13, at S2.

18. S. Rep. No. 99-541, at 4-5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3558–59; Kerr, *supra* note 16, at 1212; Press Release, Congressman Jerrold Nadler, Nadler Examines the Electronic Communications Privacy Act and Its Application to Cloud Computing (Sept. 23, 2010), <http://nadler.house.gov/press-release/nadler-examines-electronic-communications-privacy-act-and-its-application-cloud>.

19. See Press Release, Congressman Jerrold Nadler, *supra* note 18; Tony Romm, *Digital Data Privacy Rules Turn 25*, POLITICO (Oct. 19, 2011, 10:31 PM EDT), <http://www.politico.com/news/stories/1011/66405.html> (“[A]s the Electronic Communications Privacy Act Turns 25 . . . it is time to revisit a law that never anticipated the day consumers would use Gmail, Facebook, Twitter, the iPhone and other tech staples of the digital age.”).

20. See Romm, *supra* note 19.

21. See, e.g., Payne, *supra* note 11, at 847; *Data Use Policy*, FACEBOOK, http://www.facebook.com/full_data_use_policy (last updated Sept. 23, 2011) (discussing the ways users can control the visibility of their information on Facebook).

established new social norms in society, in which individuals feel comfortable sharing information on the Internet. Part III discusses various privacy laws governing Facebook. It illustrates how the U.S. Supreme Court and lower courts have applied the Fourth Amendment and SCA to the digital age. Part III also reveals why courts, legislators, attorneys, law enforcement agencies, and legal scholars have had a difficult time understanding the SCA. This Note argues that Congress must amend the SCA to allow for liberal disclosure, since individuals are knowingly disclosing information on Facebook and, therefore, lack a reasonable expectation of privacy.²² Part IV analyzes several proposed amendments to the SCA that were discussed at congressional hearings and by the Digital Due Process coalition.²³ Part IV also discusses law enforcement's need for information and the danger posed by its absence. Additionally, Part IV reviews the Electronic Communications Privacy Act Amendments Act of 2011.²⁴ Part V argues that users knowingly disclose information on Facebook and as a result, law enforcement should be able to obtain the content of communications without a search warrant. Finally, this Note demonstrates that the SCA should be amended to coincide with the Fourth Amendment and reflect the notion that individuals do not have a right to privacy in information shared on social networking websites.

22. See *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 655 (Sup. Ct. 2010). The court stated: To permit a party claiming very substantial damages . . . [to] hide behind self-set privacy controls on a website, [in which] the primary purpose . . . is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.

Id.

23. See *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 1 (2010) [hereinafter *ECPA Cloud Computing Hearing*] (statement of Rep. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, & Civil Liberties); *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 1 (2010) [hereinafter *ECPA Location Technology Hearing*] (statement of Rep. F. James Sensenbrenner, Jr., Member, Subcomm. on the Constitution, Civil Rights, & Civil Liberties); *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 1 (2010) [hereinafter *ECPA Reform Hearing*] (statement of Rep. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, & Civil Liberties); *Who We Are*, DIGITAL DUE PROCESS, <http://www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163> (last visited Apr. 20, 2012).

24. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011) (as of May 17, 2011, the bill was referred to the Senate Committee on the Judiciary).

II. OVERVIEW OF SOCIAL NETWORKING

Before the days of finding your friends with the click of a mouse and talking to them through a keyboard, there were telephones, handwritten letters, and the Pony Express.²⁵ Following the introduction of social networking websites in 1997, individuals now communicate primarily through the Internet or mobile devices.²⁶ Friendships now live and die with one simple click of a button.²⁷

A. *The Social Networking Revolution*

Social networking websites have been defined as “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”²⁸ These websites enable users to articulate and visualize their social networks in order “to meet or reconnect with people, discover and share ideas and content, and consume news and events across the Internet.”²⁹ The technology gives people “the freedom to express themselves . . . and the ability to gather around subjects that they care about” by bridging online and offline connections.³⁰ As of June 2010, the world was spending “over 110 billion minutes on social networks and blog sites” every year.³¹ In 2009, social networking surpassed e-mail in worldwide reach.³²

25. Joe Joseph, *Did We Have Friends Before Social Networks?*, TIMES (London), Aug. 7, 2009, at 26. See also Todd Underwood, *The Pony Express*, FRONTIER TRAILS, <http://www.frontiertrails.com/oldwest/ponyexpress.htm> (last visited Apr. 20, 2012).

26. boyd & Ellison, *supra* note 1, at 212 fig.1; Payne, *supra* note 11, at 848; Gina Bianchini, *Aww, Social Networking Is Growing Up: A Brief History of Social Technology, and What It Means to You*, CNN MONEY (July 20, 2009, 8:00 AM ET), <http://tech.fortune.cnn.com/2009/07/20/aww-social-networking-is-growing-up/>. As of April 2011, “[i]nternet traffic in the United States alone approach[ed] three petabytes per month . . . and is growing by 40-50 percent annually.” See *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 55 (2011) [hereinafter *ECPA Government Perspectives*] (statement of Cameron F. Kerry, General Counsel, U.S. Department of Commerce). This flow of Internet traffic demonstrates how the Internet “has become the communications medium of choice for most Americans, especially younger Americans.” *Id.* A large portion of Internet traffic may be contributed to social networking websites. See *id.*

27. Austin Considine, *Defriended, Not De-Emoted*, N.Y. TIMES, Sept. 5, 2010, at ST6.

28. boyd & Ellison, *supra* note 1, at 211.

29. Bianchini, *supra* note 26. See also boyd & Ellison, *supra* note 1, at 211.

30. Bianchini, *supra* note 26.

31. NIELSEN WIRE, *supra* note 3.

32. Payne, *supra* note 11, at 848.

The first social networking website, SixDegrees.com, launched in 1997 and allowed users to create profiles and list their friends.³³ The website was used as a tool to help people connect and send messages to one another.³⁴ Unfortunately, the service closed in 2000 because it was “simply ahead of its time.”³⁵

The next major social networking website emerged in 2002 under the name Friendster.³⁶ Friendster was “focused on helping people stay in touch with friends and discover new people and things that are important to them.”³⁷ It was built to compete with online dating websites on the assumption that “friends-of-friends would make better romantic partners than would strangers.”³⁸ By September 2003, Friendster had 1.5 million registered users.³⁹ However, when Myspace launched in 2003, it quickly surpassed the competition and started the social networking “global phenomenon.”⁴⁰

Two friends, Tom Anderson and Chris DeWolfe, founded Myspace in 2003.⁴¹ Anderson was the chief executive officer and largest shareholder of eUniverse and realized that “online communities were the future of the Internet.”⁴² Myspace allowed users “to create or join groups, post photos or videos, post ‘bulletins,’ and write personal blogs.”⁴³ Myspace differed from SixDegrees.com and Friendster by allowing users to personalize their pages with different backgrounds and layouts.⁴⁴ The website attracted “musicians/artists, teenagers, and the post-college urban social crowd” who wanted to connect with their favorite bands.⁴⁵ Myspace grew quickly through word of mouth and by February 2004, it had one million registered users.⁴⁶ Facebook, however,

33. boyd & Ellison, *supra* note 1, at 214.

34. *Id.*

35. *Id.*

36. *Id.* at 215.

37. Christina Salva Dreifort, *Traditional Community and Social Networking Online Communities* 22 (Spring 2011) (unpublished M.A. thesis, California State University, Chico), available at <http://csuchico-dspace.calstate.edu/bitstream/handle/10211.4/294/Final-Christina%20Dreifort.pdf?sequence=1>.

38. boyd & Ellison, *supra* note 1, at 215.

39. David S. Evans, *How Catalysts Ignite: The Economics of Platform-Based Start-Ups*, in *PLATFORMS, MARKETS AND INNOVATION* 99, 119 (Annabelle Gawer ed., 2009).

40. boyd & Ellison, *supra* note 1, at 216-17; North, *supra* note 9, at 1284.

41. Wilson, *supra* note 11, at 1222.

42. Mark A. Urista et al., *Explaining Why Young Adults Use MySpace and Facebook Through Uses and Gratifications Theory*, 12 HUM. COMM. 215, 217 (2009).

43. Wilson, *supra* note 11, at 1222.

44. boyd & Ellison, *supra* note 1, at 217.

45. *Id.*

46. See Urista et al., *supra* note 42, at 217; *MySpace*, CRUNCHBASE, <http://www.crunchbase.com/company/myspace> (last visited Apr. 20, 2012).

quickly surpassed Myspace in its number of users, and by January 2009, Facebook became the “world’s default social network.”⁴⁷ Recently, Myspace has remarketed itself as a “social entertainment” website and not a social network in order to compete within the social networking market.⁴⁸

LinkedIn, a popular professional social networking site, was officially launched on May 5, 2003.⁴⁹ LinkedIn is known as “the world’s largest professional network on the Internet with more than 135 million members in over 200 countries and territories.”⁵⁰ “More than two million companies” have created LinkedIn pages.⁵¹ The goal of LinkedIn is to “connect[] the world’s professionals to make them more productive and successful.”⁵²

Facebook first launched in February 2004.⁵³ By December 2004, only ten months after the website first launched, Facebook had nearly one million active users.⁵⁴ A more detailed discussion of Facebook’s history will be analyzed in Part B of this Section.

Another major social networking website, Twitter, launched in 2006.⁵⁵ “Twitter is a real-time information network that connects [users] to the latest stories, ideas, opinions and news about what [they] find interesting.”⁵⁶ It was “designed to help [users] share information with the world.”⁵⁷ Twitter allows individuals to send short messages, known as “tweets,”⁵⁸ to specific people or the general public.⁵⁹ Some users include celebrities and politicians, such as President Barack Obama, Lance

47. Michael Arrington, *Facebook Now Nearly Twice the Size of MySpace Worldwide*, TECHCRUNCH (Jan. 22, 2009), <http://techcrunch.com/2009/01/22/facebook-now-nearly-twice-the-size-of-myspace-worldwide/>.

48. Andy Fixmer & Ronald Grover, *Social Networks: A Fresh Coat of Paint for MySpace*, BLOOMBERG BUSINESSWEEK, Nov. 1–Nov. 7, 2010, at 42, 42, 44.

49. *About Us*, LINKEDIN, <http://press.linkedin.com/about> (last visited Apr. 20, 2012).

50. *Id.*

51. *Id.*

52. *LinkedIn Says the 2011 Most Overused Professional Buzzwords in the United States Are “Creative,” “Organizational” and “Effective,”* LINKEDIN (Dec. 13, 2011), <http://press.linkedin.com/node/1051>.

53. *Timeline*, FACEBOOK, <http://newsroom.fb.com/content/default.aspx?NewsAreaId=20> (last visited Apr. 20, 2012).

54. *Id.*

55. boyd & Ellison, *supra* note 1, at 212 fig.1.

56. *About Twitter: The Fastest, Simplest Way to Stay Close to Everything You Care About*, TWITTER, <http://twitter.com/about> (last visited Apr. 20, 2012).

57. *Twitter Privacy Policy*, TWITTER (June 23, 2011), <http://twitter.com/privacy>.

58. *Frequently Asked Questions*, TWITTER, <http://support.twitter.com/entries/13920-frequently-asked-questions> (last visited Apr. 20, 2012) (defining a “Tweet” as a message posted by a user in 140 characters or less).

59. Payne, *supra* note 11, at 847.

Armstrong, and Britney Spears.⁶⁰ As of October 2011, Twitter had more than 100 million active users who created approximately 250 million tweets per day.⁶¹

Americans of all ages have been affected in some way by the explosion of social networking websites.⁶² Social networking has drastically reformed traditional “social structures that community members have always used to communicate with each other.”⁶³ Other social networking websites include Hi5, Bebo, Ryze, and Orkut.⁶⁴ This Note will focus specifically on Facebook and the legal issues surrounding users’ privacy when information is requested for discovery by law enforcement.

B. Facebook and Its 845 Million Friends

If the Internet were a high school, Facebook would win the “Most Popular” award, and its founder and chief executive officer Mark Zuckerberg would be king of the prom. Instead of a tuxedo, this prom king would wear a “t-shirt, blue jeans, and open-toe Adidas sandals.”⁶⁵

Zuckerberg first launched Facebook from his Harvard dorm room in February 2004 with co-founders Dustin Moskovitz, Chris Hughes, and Eduardo Saverin.⁶⁶ Their purpose was to replicate an average college day on a website.⁶⁷ Facebook’s founders hoped that Facebook would be “the thing that drove the college social experience, drove people to go out to the clubs and bars and even the classrooms and dining halls.”⁶⁸ It was designed to be “simple and clean,” yet have enough “pizzazz” to attract students’ attention.⁶⁹ Originally, Facebook was an exclusive website that

60. JOHN G. BRESLIN ET AL., *THE SOCIAL SEMANTIC WEB* 88-89 (2009). Some celebrities tweet by proxy, but many “take the time out to engage with the public and with their fans by posting tweets themselves.” *Id.* at 88.

61. Ben Parr, *Twitter Has 100 Million Monthly Active Users; 50% Log in Every Day*, MASHABLE (Oct. 18, 2011), <http://mashable.com/2011/10/17/twitter-costolo-stats/>.

62. See BRESLIN ET AL., *supra* note 60, at 174 (discussing the uses and benefits of social networking); North, *supra* note 9, at 1286.

63. North, *supra* note 9, at 1285.

64. BEBO, <http://www.bebo.com/> (last visited Apr. 20, 2012); Hi5, <http://www.hi5.com> (last visited Apr. 20, 2012); ORKUT, <http://www.orkut.com/PreSignup> (last visited Apr. 20, 2012); RYZE, <http://www.ryze.com/> (last visited Apr. 20, 2012). See also boyd & Ellison, *supra* note 1, at 212 fig.1 (listing launch dates of major social networking websites).

65. Michael M. Grynbaum, *Mark E. Zuckerberg '06: The Wiz Behind Thefacebook.com*, HARV. CRIMSON (June 10, 2004), <http://www.thecrimson.com/article/2004/6/10/mark-e-zuckerberg-06-the-whiz/>.

66. Grimmelman, *supra* note 2, at 1144; *Timeline*, *supra* note 53.

67. See BEN MEZRICH, *THE ACCIDENTAL BILLIONAIRES* 93 (First Anchor Books 2010) (2009) (discussing Zuckerberg’s purpose and thought process while developing Facebook).

68. *Id.*

69. *Id.*

one could only access with a Harvard.edu e-mail address.⁷⁰ The exclusivity made the website popular and enhanced the concept that a user's information would remain private.⁷¹ In an interview with Zuckerberg, only a semester after Facebook launched, he commented: "I'm going on the theory that like, I'm in college just like everyone else, so stuff that's applicable to me is probably applicable and useful to everyone else, as well."⁷²

Since 2004, Facebook has experienced several changes in order to earn the "Most Popular" award.⁷³ When Facebook first launched, it was only available to Harvard students, but quickly expanded to Stanford, Columbia, and Yale.⁷⁴ Today, Facebook is open to anyone around the world, and as of December 2011, it had over 845 million "active users"⁷⁵ who uploaded more than 250 million photos per day.⁷⁶ In 2012, Facebook was ranked the number one social networking website in a review comparison survey.⁷⁷ Over 425 million active users access their Facebook accounts on their mobile device through more than 475 mobile operators worldwide.⁷⁸ There are more than seventy languages available on the website and more than eighty percent of users are located outside the United States and Canada.⁷⁹ The average user has approximately 130 friends.⁸⁰ Facebook has become one of the most-trafficked websites in the United States, if not the world.⁸¹ According to Facebook, its "mission

70. *Id.* at 95. See also *THE SOCIAL NETWORK* (Columbia Pictures 2010) (describing the history of Facebook and the challenges and lawsuits that Zuckerberg faced).

71. MEZRICH, *supra* note 67, at 95 ("[E]xclusivity would make the site more popular; it would also enhance the idea that your info would remain in a closed system, private.").

72. Grynbaum, *supra* note 65 (internal quotation marks omitted).

73. See generally *Timeline*, *supra* note 53 (listing the many changes Facebook has gone through over the years).

74. *Id.*

75. Matthew J. Hodge, Comment, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com*, 31 S. ILL. U. L.J. 95, 98 (2006); *Fact Sheet*, *supra* note 4. See also *Statement of Rights and Responsibilities*, *supra* note 8 (defining an "active registered user" as "a user who has logged into Facebook at least once in the previous 30 days").

76. Overview, FACEBOOK, <http://newsroom.fb.com/content/default.aspx?NewsAreaId=21> (last visited Apr. 20, 2012).

77. 2012 Social Networking Websites Comparisons, TOP TEN REVIEWS, <http://social-networking-websites-review.toptenreviews.com/> (last visited Apr. 20, 2012).

78. Facebook IPO and What It Means (for You), DEI WORLDWIDE (Feb. 10, 2012), <http://deiworldwide.com/blog/facebook-ipo-means-to-you/>.

79. *Fact Sheet*, *supra* note 4.

80. North, *supra* note 9, at 1285.

81. See Facebook Statistics, Stats & Facts for 2011, DIGITAL BUZZ BLOG (Jan. 18, 2011), <http://www.digitalbuzzblog.com/facebook-statistics-stats-facts-2011/>; *Clash of the Titans: Facebook Passes Google as the Most Popular Website in the U.S.*, MAIL ONLINE, <http://www.dailymail.co.uk/sciencetech/article-1342944/Facebook-passes-Google-popular-site-Internet.html> (last updated Jan. 2, 2011, 12:34 AM); Matthew Shaer, *Google Admits Facebook Is the Most Popular Website in the World*, CHRISTIAN SCI. MONITOR (June 2, 2010),

is to give people the power to share and make the world more open and connected.”⁸²

C. Status Update: How Facebook Allows Its Users to Share Their Secrets, Thoughts, and Emotions with a Few Simple Clicks

Every day, millions of people use Facebook to “keep up with friends, upload an unlimited number of photos, share links and videos, and learn more about the people they meet.”⁸³ Many users call themselves “Facebook stalker[s],” which is commonly used to describe the act of secretly gathering information and monitoring another user’s activity on Facebook.⁸⁴ Facebook makes it easier for employers to see pictures of their employees at a party, ex-boyfriends to find out their ex-girlfriends are in a new relationship, and to even help potential suspects have their criminal charges dropped.⁸⁵ With the development of various applications, Facebook users have grown accustomed to publishing and sharing personal information on the Internet.⁸⁶ According to Zuckerberg, “[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.”⁸⁷ Like a noisy cafeteria at lunchtime, or a playground at recess, “Facebook is a place of indiscriminate musings and minutiae, where people report their every thought, mood, hiccup, cappuccino, increased reps at the gym or switch to a new brand of toothpaste.”⁸⁸ This “social norm” demonstrates the difficulties in maintaining any expectation of privacy.⁸⁹

<http://www.csmonitor.com/Innovation/Horizons/2010/0602/Google-admits-Facebook-is-the-most-popular-website-in-the-world>.

82. *About*, FACEBOOK, <http://www.facebook.com/facebook?v=info> (last visited Apr. 20, 2012).

83. *Id.*

84. Byron Dubrow, *What 2 Say When U Know 2 Much?*, USA TODAY, Mar. 8, 2007, at 4D.

85. Damiano Beltrami, *I’m Innocent. Just Check My Status on Facebook.*, N.Y. TIMES, Nov. 12, 2009, at A27 (discussing Rodney Bradford’s robbery charges, which were dropped when the Brooklyn district attorney discovered that Bradford had posted a message on his Facebook page from a computer in his father’s apartment at the time of the robbery); Richmond, *supra* note 7, at B5 (discussing the dangers of sharing information on social networking websites and how it has impacted the work place).

86. See Alyson Gregory Richter, *Social Networking Evidence and Ethical Issues: How to Get It and How to Get It In*, STATE BAR OF TEX., 1-2 (May 6, 2010), available at <http://www.texasbar.com/Materials/Events/9081/119821.pdf>.

87. Chris Matyszczyk, *Zuckerberg: I Know That People Don’t Want Privacy*, CNET NEWS (Jan. 10, 2010, 1:40 PM PST), http://news.cnet.com/8301-17852_3-10431741-71.html (describing an interview with Zuckerberg on Facebook sharing and privacy).

88. Aimee Lee Ball, *Are 5,001 Friends One Too Many?*, N.Y. TIMES, May 30, 2010, at ST1.

89. Matyszczyk, *supra* note 87 (discussing how individuals are comfortable with sharing information).

Some of the ways members share information and communicate are through status updates, profile information, direct messages, the poking feature, third-party applications, wall posts, the instant chat feature, pictures, videos, games, groups, events, notes, fan pages, and more.⁹⁰ A profile allows individuals to provide information about their interests, education, work background, contact information, or anything else they wish to share.⁹¹ When a user creates, changes, or shares information, such activity is displayed on his or her friends' "news feed."⁹² The news feed is "a device that automatically broadcasts a user's most important activities and status updates."⁹³ Users utilize Facebook "to share everything from the small stuff, like their thoughts on an article, to the most important events of their lives, like the photos of their wedding or the birth of their child."⁹⁴ The abundance of information that is shared and displayed on Facebook blurs the meaning of what is truly "private" anymore.⁹⁵

Recently, Facebook launched a program that allows users to view, send, and receive Facebook messages, e-mail, and text messages in one window.⁹⁶ The purpose of this feature is to organize conversations across different media and place them in one location in order to keep a constant flow of conversation.⁹⁷ Facebook has also partnered with Microsoft to create a feature on the search engine Bing.⁹⁸ When users enter a search on Bing, their search results may connect to Facebook and display their Facebook friends' recommendations based upon their friends' "likes" and interests.⁹⁹ In September 2011, Facebook launched an application called "Timeline" that places everything a user has shared since the day they signed up for Facebook on one page.¹⁰⁰ Facebook

90. Payne, *supra* note 11, at 846-47; *Overview*, *supra* note 76.

91. *Facebook Profile*, FACEBOOK, <http://www.facebook.com/about/profile/> (last visited Apr. 20, 2012).

92. Payne, *supra* note 11, at 847.

93. Richter, *supra* note 86, at 2.

94. Samuel W. Lessin, *Tell Your Story with Timeline*, FACEBOOK BLOG, <http://www.facebook.com/blog.php?post=10150289612087131> (last updated Dec. 6, 2011).

95. See Matyszczuk, *supra* note 87.

96. Joel Seligstein, *See the Messages That Matter*, FACEBOOK BLOG, <http://blog.facebook.com/blog.php?post=452288242130> (last updated Feb. 11, 2011).

97. *Id.*

98. Leslie Horn, *Microsoft, Facebook Social Searches Go Live on Bing*, PCMAG.COM (Nov. 2, 2010, 05:16 PM EST), <http://www.pcmag.com/article2/0,2817,2372020,00.asp> (discussing Microsoft and Facebook's partnership agreement creating a feature that detects a user's information on Facebook and displays it within a Bing search result).

99. *Id.* ("[Y]ou will show up in profile searches on Bing, even if you have selected not to have profile information show up on public search engines." (internal quotation marks omitted)).

100. Lessin, *supra* note 94.

describes Timeline as “an easy way to rediscover the things you shared, and collect all your best moments in a single place.”¹⁰¹

Users embrace online social communication because it is “intrinsically personal and . . . fulfills the fundamental need for connectedness—the feeling of belonging.”¹⁰² In 2010, Facebook users collectively updated their status messages at least sixty million times every day.¹⁰³ People feel comfortable sharing information, however, few realize that “if we were to draw a real-world analogy to posting . . . it would be more analogous to taking a megaphone into Madison Square Garden each time [they] typed in a message.”¹⁰⁴ A recent study found that people are blogging less and devoting more time to their social networks.¹⁰⁵ This is because “people . . . have something to say, but either are content to say it only to their friends, or don’t need more than 140 characters to express it.”¹⁰⁶

Although the average Facebook user has 130 friends, many users have hundreds, if not thousands.¹⁰⁷ A friendship on Facebook may not be “the same as a real friend, the kind who brings you chicken soup when you’re sick and posts multiple favorable reviews about your book on Amazon.”¹⁰⁸ Many users accept a friend request because it is easier than “going through the socially awkward process of rejecting them.”¹⁰⁹ As a result, status updates, photos, videos, wall posts, groups, and profile information are most likely accessible to many people with whom users have never had a conversation or even met.¹¹⁰ Furthermore, if a user does not control his or her privacy settings, anyone around the world can access that user’s information through a simple Google, Yahoo!, or Bing

101. *Id.*

102. David Rosenblum, *What Anyone Can Know: The Privacy Risks of Social Networking Sites*, IEEE SECURITY & PRIVACY, May/June 2007, at 40, 43.

103. North, *supra* note 9, at 1287.

104. Rosenblum, *supra* note 102, at 45.

105. See Jeff Bercovici, *How Facebook and Twitter Are Replacing Blogging*, FORBES (Nov. 4, 2010, 1:55 PM), <http://blogs.forbes.com/jeffbercovici/2010/11/04/how-facebook-and-twitter-are-replacing-blogging/>.

106. *Id.* (referring in part to Twitter, which limits users’ messages to 140 characters).

107. North, *supra* note 9, at 1285.

108. Steven Levy, *How Many Friends Is Too Many?*, NEWSWEEK, May 26, 2008, at 15, 15.

109. danah boyd, *Friends, Friendsters, and Top 8: Writing Community into Being on Social Network Sites*, 11 FIRST MONDAY (Dec. 4, 2006), <http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1418/1336>.

110. See Levy, *supra* note 108, at 15 (discussing the implications of social networking websites since “people tend to cave in and agree to friendship when asked by someone they barely know, or in some cases don’t know at all”).

search.¹¹¹ This demonstrates the difficulty of ensuring that anything is truly “private” when posted on Facebook.¹¹²

D. “Privacy” Settings on Facebook

When a user joins Facebook, he or she must provide basic personal information including a name, e-mail address, gender, and birthday.¹¹³ Once an account is created, a user may add as much or as little additional information as he or she chooses.¹¹⁴ This information can be individually controlled through Facebook’s privacy settings.¹¹⁵

Through Facebook’s privacy settings users can opt to make their information available to the general public, or semi-private by restricting access to a self-selected group of “Friends” or “Friends of Friends.”¹¹⁶ If a user has chosen a semi-private profile, the select group of people who can access that user’s profile usually includes the user’s “friends.”¹¹⁷ A user’s “friends” may include anyone that the user either requested or accepted to be his or her “friend” on Facebook.¹¹⁸ As previously noted, a “friend” may include anyone from a lifelong companion to a complete stranger.¹¹⁹ Zuckerberg posted about his personal privacy settings, stating: “For those wondering, I set most of my content to be open so people could see it. I set some of my content to be more private, but I

111. BING, <http://www.bing.com/> (last visited Apr. 20, 2012); GOOGLE, <http://www.google.com/> (last visited Apr. 20, 2012); YAHOO!, <http://www.yahoo.com/> (last visited Apr. 20, 2012). See Linda Rosencrance, *Facebook to Make Listings Public via Search Engines*, PCWORLD (Sept. 5, 2007, 8:00 PM), http://www.pcworld.com/article/136864/facebook_to_make_listings_public_via_search_engines.html (discussing the release of Facebook’s information on search engines).

112. See Rosencrance, *supra* note 111 (“[O]nce users’ profiles are available on search engines, Facebook will become a quasi-White Pages of the Web, rather than a social networking site” which is “a step in the overall erosion of people’s privacy.”).

113. FACEBOOK, <http://www.facebook.com/> (last visited Apr. 20, 2012).

114. Richter, *supra* note 86, at 2.

115. *Statement of Rights and Responsibilities*, *supra* note 8.

116. North, *supra* note 9, at 1288. North explains:

The types of information found on social-networking sites can be divided into three categories based on the level of public disclosure. First, public social-networking information may include any text or media that is available to the general public. Second, semi-private information includes content that is restricted to either a self-selected group of “friends” or a wider, unmanageable group of “friends of friends.” Third, private information includes instant messages and user-to-user messages (essentially e-mails).

Id. See Richter, *supra* note 86, at 3. By selecting the “Public” setting, anyone on the Internet can view the user’s content. *Why Did Everyone Change to Public?*, FACEBOOK, <http://www.facebook.com/help/?faq=244664905564168#Why-did-Everyone-change-to-Public?> (last visited Apr. 20, 2012).

117. Hodge, *supra* note 75, at 99.

118. *Id.*

119. See *supra* text accompanying notes 107-10.

didn't see a need to limit visibility of pics with my friends, family or my teddy bear :).¹²⁰

Some information on Facebook is always available to everyone on the Internet because it is essential to help people find and connect with one another.¹²¹ This information includes a user's name, profile picture, gender, user identification, and networks.¹²² According to Facebook's data use policy, "[i]f you are uncomfortable sharing your real name, you can always deactivate or delete your account."¹²³

When creating an account, users must consent to Facebook's statement of rights and responsibilities and data use policy in order to access its website.¹²⁴ Within these policies, Facebook specifies that it collects users' information whenever they interact with Facebook, including all status updates, photos, comments, postings, tags, groups, GPS locations, messages, games, and more.¹²⁵ Facebook may collect information when a friend tags a user in a photo, video, place, or relationship status.¹²⁶ Moreover, Facebook may obtain a user's GPS location in order to inform a user that a friend may be nearby.¹²⁷ Facebook cautions users that it cannot guarantee complete safety.¹²⁸ Specifically, Facebook warns its users to always think before they post because just like anything else on the Internet, information shared on Facebook may be re-shared with others.¹²⁹

Twitter and Myspace have similar privacy policies to Facebook.¹³⁰ Twitter's policy informs its users that "[w]hat you say on Twitter may be viewed all around the world instantly."¹³¹ Myspace warns users not to forget that their "profile and Myspace forums are public spaces" and not

120. Mark Zuckerberg, FACEBOOK (Dec. 11, 2009), <http://www.facebook.com/zuck>.

121. *Data Use Policy*, *supra* note 21.

122. *Id.*

123. *Id.*

124. Hodge, *supra* note 75, at 98; *Statement of Rights and Responsibilities*, *supra* note 8.

125. *Data Use Policy*, *supra* note 21. Facebook also receives data when a user views another user's profile, clicks on advertisements, is tagged in a friend's photo, or joins a new group. *Id.* Moreover, Facebook receives data from computer and mobile devices regarding a user's internet protocol ("IP") address, location, browser, and pages that the user visited. *Id.*

126. *Id.*

127. *Id.*

128. *Statement of Rights and Responsibilities*, *supra* note 8.

129. *See Data Use Policy*, *supra* note 21.

130. *Compare id.* (describing how and what types of information Facebook collects from its users), with *Privacy Policy*, MYSPACE, http://www.myspace.com/Help/Privacy?pm_cmp=ed_footer (last updated Dec. 7, 2010) (discussing the types of information Myspace collects from its users), and *Twitter Privacy Policy*, *supra* note 57 (explaining the types of information collected and used by Twitter).

131. *Twitter Privacy Policy*, *supra* note 57.

to “post anything [they] wouldn’t want the world to know.”¹³² Myspace also reminds its users that it is not only their friends who are looking at their page because “the truth is that everyone can see it.”¹³³ Additionally, Myspace cautions users to “[t]hink twice before posting a photo or information [they] wouldn’t want [their] parents, potential employers, colleges or boss to see!”¹³⁴

Although Facebook provides various privacy settings, many users find the options to be confusing and complicated to manage.¹³⁵ As people share more information on Facebook, privacy has become a “dying concept.”¹³⁶ Users should assume that what they post on Facebook might become publicly available or shared with “unauthorized” individuals.¹³⁷

E. *Sharing Is the New Social Norm*

Since Zuckerberg first launched Facebook from his Harvard dorm room in 2004, society has changed the way it communicates and shares information.¹³⁸ Millions of people use Facebook everyday “to keep up with friends, upload an unlimited number of photos, share links and videos, and learn more about the people they meet.”¹³⁹ Thanks to Facebook, many people “have gotten back in touch with friends from high school and college, shared old and new photos, and become better acquainted with some people [they] might never have grown close to offline.”¹⁴⁰

Social norms have changed as people have become more comfortable sharing information on social networking websites.¹⁴¹ Facebook has created this “social norm” by making it easier for

132. *Myspace Safety*, MYSPACE, <http://www.myspace.com/help/safety/tips> (last visited Apr. 20, 2012).

133. *Id.*

134. *Id.*

135. Mark Zuckerberg, *A New Page in Facebook Privacy*, WASH. POST, May 24, 2010, at A19. See also Harry McCracken, *Facebook’s Privacy Reboot: Is That All You’ve Got for Us?*, PCWORLD (May 29, 2010, 2:04 PM), http://www.pcworld.com/article/197539/facebook_privacy_reboot_is_that_all_youve_got_for_us.html; Mark Zuckerberg, *Making Control Simple*, FACEBOOK BLOG (May 26, 2010, 10:55 AM), <http://blog.facebook.com/blog.php?post=391922327130> (posting by Mark Zuckerberg responding to user complaints on privacy settings).

136. John D. Sutter, *The Internet and the ‘End of Privacy,’* CNN (Dec. 13, 2010), http://articles.cnn.com/2010-12-13/tech/end.of.privacy.intro_1_online-privacy-blippy-social-network.

137. *Data Use Policy*, *supra* note 21 (discussing how some types of posts are always public).

138. See *supra* text accompanying notes 66, 83-90, 102-06.

139. *About*, *supra* note 82.

140. Elizabeth Bernstein, *How Facebook Ruins Friendships*, WALL ST. J., Aug. 25, 2009, at D1.

141. See *supra* text accompanying notes 87-88.

individuals to communicate more quickly and efficiently.¹⁴² Facebook users feel comfortable sharing anything and everything and “[w]hether it is women posting their bra colors, bosses posting pink slips, or people’s simple narcissism, you can find it all on Facebook.”¹⁴³ With the expansion of Facebook and social networking, “this type of unsolicited and often embarrassing communication is an inescapable sign of the times.”¹⁴⁴ Facebook users “see only benefits in sharing their every move online, with little concern for the consequences of foregone privacy.”¹⁴⁵

In a given day, more than half of Facebook’s active users log on to Facebook and upload more than 250 million photos.¹⁴⁶ Users spend hours on Facebook and other social networking websites “uploading photos of their children or parties, forwarding inane quizzes, posting quirky, sometimes nonsensical one-liners or tweeting their latest whereabouts.”¹⁴⁷ Individuals feel comfortable posting information on Facebook that they wouldn’t normally say out loud in conversation.¹⁴⁸ Through Facebook, users have opened up a “window” into their lives, allowing anyone to look inside with a few simple clicks.¹⁴⁹

III. ANALYSIS OF CONSTITUTIONAL AND STATUTORY AUTHORITY REGULATING PRIVACY

Since the first social networking website launched in 1997, more than 500 online social networking websites have come into existence.¹⁵⁰ The expansion of social networking websites has provided valuable evidence in both civil and criminal cases.¹⁵¹ As sharing personal information online has become the “social norm,” more attorneys and law enforcement officials have turned to these websites as a resource for discovery.¹⁵² Employers are also turning to social networking websites in order to discover whether its employees are complying with policies and regulations.¹⁵³ Some employers are even requiring applicants to disclose

142. See discussion *supra* Part II.C.

143. James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L.J. 793, 797 (2010) (footnotes omitted).

144. *Id.* (citation omitted) (internal quotation marks omitted).

145. *Id.* at 798 (“Facebook use is just a symptom of an underlying unconcern for the private-visible confirmation that oversharing is the new black.”).

146. *Fact Sheet*, *supra* note 4; *Overview*, *supra* note 76.

147. Bernstein, *supra* note 140, at D1.

148. *Id.* at D2.

149. *Id.*

150. See boyd & Ellison, *supra* note 1, at 214; Richter, *supra* note 86, at 2.

151. Kathrine Minotti, *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, 60 S.C. L. REV. 1057, 1059 (2009).

152. *Id.* See also Matyszczyk, *supra* note 87 (“[S]haring ha[s] become a new social norm.”).

153. See James Parton, *Obtaining Records from Facebook, LinkedIn, Google and Other Social*

their Facebook usernames and passwords in an attempt to discover incriminating information.¹⁵⁴ Although this information is valuable, it may be difficult to discover—especially if a user has deleted information from his or her account.¹⁵⁵ As a result, this information may only be obtained from the social networking provider.¹⁵⁶

According to Facebook's data use policy, Facebook will only share a user's information in response to a legal request if it has a good faith belief that such disclosure is required by law.¹⁵⁷ Additionally, Facebook asserts that it may not disclose information pursuant to the SCA.¹⁵⁸ According to Facebook's deputy general counsel, it is unclear exactly what content is protected by law.¹⁵⁹ Facebook, however, claims that it may not release the content of a user's account without a search warrant issued upon probable cause.¹⁶⁰

As technology is constantly transforming, it has been difficult for Congress to provide Facebook with guidance as to what information may be disclosed and when.¹⁶¹ This Section illustrates the pressing need to reform the SCA to reflect the notion that a user does not have a reasonable expectation of privacy when sharing personal information with 845 million "friends." Part A evaluates privacy under the Fourth Amendment with respect to advances in technology. Part B discusses the

Networking Websites and Internet Service Providers., DRI TODAY (May 24, 2010, 9:40), <http://forthedefense.org/file.axd?file=2010%2f5%2fObtaining+Records+From+Social+Networking+Websites.pdf>.

154. See Philip Gordon, *Is It Really Illegal to Require an Applicant or Employee to Disclose Her Password to a "Friends-Only" Facebook Page?*, WORKPLACE PRIVACY COUNS. (Mar. 8, 2011), <http://privacyblog.littler.com/2011/03/articles/social-networking-1/is-it-really-illegal-to-require-an-applicant-or-employee-to-disclose-her-password-to-a-friendsonly-facebook-page/>. Whether employers may require applicants to disclose their username and password has not yet been decided in court. See *id.* According to the Civil Liberties Union of Maryland, this practice violates the SCA because applicants are forced into disclosing personal information. *Id.* This argument is weak, however, as the employer would only gain access to the information upon an applicant's authorized consent. See *id.*

155. See Payne, *supra* note 11, at 848, 865.

156. See *id.* at 848.

157. Data Use Policy, *supra* note 21.

158. See Mark Howitson, Deputy Gen. Counsel, Facebook, Keynote Address at LegalTech New York 2010: Facebook: Perspectives on Corporate eDiscovery and Social Media (Feb. 2, 2010) [hereinafter Howitson Keynote Address], available at http://www.legaltechshow.com/rs5/contest.asp?sweeps_code=lny2010 (discussing why Facebook does not hand over personal information when served with a subpoena).

159. *Id.*

160. Information for Law Enforcement Authorities, FACEBOOK, <http://www.facebook.com/safety/attachment/Information%20for%20Law%20Enforcement%20Authorities.pdf> (last visited Apr. 20, 2012). Content may include a user's "messages, photos, videos, wall posts, and location information." *Id.*

161. Robert Terenzi, Jr., Note, *Friending Privacy: Toward Self-Regulation of Second Generation Social Networks*, 20 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1049, 1071 (2010).

SCA and how courts have faced challenges when applying the statute. Part C examines how the U.S. Supreme Court analyzed the Fourth Amendment and SCA issues in *City of Ontario v. Quon*.¹⁶²

A. Facebook and the Fourth Amendment—The “Katz” Is Out of the Bag

The Fourth Amendment has been interpreted by the Supreme Court “in light of contemporary norms and conditions” and has not “simply frozen into constitutional law those . . . practices that existed at the time of the Fourth Amendment’s passage.”¹⁶³ Section 1 examines how the Supreme Court has applied the Fourth Amendment to modern technology. Section 2 articulates how lower courts have interpreted the Fourth Amendment with respect to the Internet and electronic communications.

1. The Supreme Court’s Evolving Interpretation of the Fourth Amendment

The Fourth Amendment provides “[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures.”¹⁶⁴ In *Katz v. United States*,¹⁶⁵ the Supreme Court held that under the Fourth Amendment, “[w]hat a person *knowingly* exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private . . . may be constitutionally protected.”¹⁶⁶ Justice John M. Harlan concurred in the Court’s opinion, noting that an individual will be protected by the Fourth Amendment where “first . . . a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”¹⁶⁷ Justice Harlan recognized that “conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.”¹⁶⁸

162. 130 S. Ct. 2619 (2010).

163. *Payton v. New York*, 445 U.S. 573, 591 n.33 (1980).

164. U.S. CONST. amend. IV.

165. 389 U.S. 347 (1967).

166. *Id.* at 351-52 (emphasis added) (citations omitted).

167. *Id.* at 361 (Harlan, J., concurring). See also Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 353 (2009) (describing Justice Harlan’s two-prong approach as a “flexible test designed to account for the many varied situations under which Fourth Amendment searches may take place”).

168. *Katz*, 389 U.S. at 361.

Applying the Fourth Amendment to advancements in technology has presented a recurring challenge for the Supreme Court.¹⁶⁹ In *Olmstead v. United States*,¹⁷⁰ Justice Louis D. Brandeis acknowledged in his dissent that “[t]ime works changes, [which] brings into existence new conditions and purposes” and “[t]he progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping.”¹⁷¹ Justice Brandeis wisely noted that when applying the Constitution, the Court must consider not “only of what has been but of what may be.”¹⁷² This suggests that Justice Brandeis believed that the Fourth Amendment should be interpreted to encompass changes in technology.¹⁷³ Moreover, as Justice Antonin G. Scalia recognized in *Kyllo v. United States*,¹⁷⁴ “[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”¹⁷⁵

The Supreme Court has not yet addressed the particular issue of whether an individual is entitled to Fourth Amendment protection in information posted on Facebook or other social networking websites.¹⁷⁶ The Supreme Court has held, however, that an individual does not have a reasonable expectation of privacy in conversations with a third party, as there is no certainty that the third party will not reveal the contents of the conversations to the police.¹⁷⁷ Additionally, the Supreme Court has held that individuals lack any reasonable expectation of privacy in bank records, financial statements, and deposit slips, since the information is “voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”¹⁷⁸ When disclosing information to a third party, individuals risk that their information may be conveyed to the Government.¹⁷⁹

169. See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 580-81 (2009).

170. 277 U.S. 438 (1928).

171. *Id.* at 472-74 (Brandeis, J., dissenting).

172. *Id.* at 473.

173. See *id.* See also Kerr, *supra* note 169, at 580.

174. 533 U.S. 27 (2001).

175. *Id.* at 33-34.

176. See Hodge, *supra* note 75, at 101.

177. See *United States v. White*, 401 U.S. 745, 752-53 (1971).

178. *United States v. Miller*, 425 U.S. 435, 442 (1976).

179. *Id.* at 443 (“The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.”). The Court in *Miller* also held that “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . even if the information is revealed on the assumption that it will be used only for a limited purpose.” *Id.*

Similarly, the Supreme Court held in *Smith v. Maryland*¹⁸⁰ that an individual was not entitled to Fourth Amendment protection where, at the request of the police, a telephone company installed a pen register to record the telephone numbers dialed within the individual's home.¹⁸¹ The Supreme Court was "not inclined to make a crazy quilt of the Fourth Amendment."¹⁸² Moreover, the Court noted that telephone users understand that phone companies must permanently record all numbers dialed in order to calculate monthly bills.¹⁸³ Individuals voluntarily convey this information and in doing so, assume the risk that the company may reveal this information to the police.¹⁸⁴ Therefore, the installation and use of a pen register was not a search under the Fourth Amendment because individuals do not have a reasonable expectation of privacy in the phone numbers they dial.¹⁸⁵

2. How Lower Courts Have Applied the Fourth Amendment to Electronic Communications and Social Networking Websites

Since the Supreme Court has not yet addressed whether individuals have a reasonable expectation of privacy in social networking websites, it is important to look to lower courts' decisions for guidance.¹⁸⁶ Many lower courts "have made clear that there is no reasonable expectation of privacy in communications to large audiences, such as posts on social media websites."¹⁸⁷ These courts have recognized that due to shifting social norms and the existence of written policies on social networking websites, individuals lack any expectation of privacy in information disclosed on social networking websites.¹⁸⁸

In *Cohen v. Facebook, Inc.*,¹⁸⁹ the Northern District of California recognized that "Facebook has emerged as a platform on which individuals can disseminate vast amounts of information, ranging from trivial details of daily personal life to breaking developments in international newsmaking events."¹⁹⁰ The court further noted that "Facebook exists because its users *want* to share information—often

180. 442 U.S. 735 (1979).

181. *Id.* at 737, 742-44.

182. *Id.* at 745.

183. *Id.* at 742.

184. *Id.* at 743.

185. *Id.* at 745-46.

186. See Hodge, *supra* note 75, at 101-02.

187. Hector Gonzalez et al., *Do Privacy Rights in Electronic Communications Exist?: Courts Are Proceeding Cautiously*, N.Y. L.J., Jan. 17, 2012, at S6.

188. *Id.* ("[A]s people use new technology and devices to communicate, seemingly private disclosures are leaving electronic trails that are visible to others . . .").

189. 798 F. Supp. 2d 1090 (N.D. Cal. 2011).

190. *Id.* at 1092.

about themselves—and to obtain information about others, within and among groups and subgroups of persons they already know or with whom they become acquainted with through using Facebook.”¹⁹¹

Additionally, in *Romano v. Steelcase, Inc.*,¹⁹² the N.Y. Supreme Court granted access to an individual’s Facebook and Myspace accounts because the websites were likely to contain material evidence.¹⁹³ The court recognized that individuals consent to sharing their personal information with others when they sign up for Facebook, notwithstanding their privacy settings.¹⁹⁴ Individuals understand that the nature of social networking websites is to share personal information with others.¹⁹⁵ Moreover, the court held that the plaintiff was not entitled to Fourth Amendment protection, “as neither Facebook nor MySpace guarantee[d] complete privacy” to its users.¹⁹⁶ Specifically, these websites warn users that information posted may become publicly available.¹⁹⁷ As a result, the court held that privacy with respect to social networking “is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking.”¹⁹⁸ The N.Y. Supreme Court recently cited to *Romano*, holding that postings on a Facebook account “if relevant, are not shielded from discovery merely because [the] plaintiff used the service’s privacy settings to restrict access.”¹⁹⁹

In *Maremont v. Susan Fredman Design Group, Ltd.*,²⁰⁰ the Northern District of Illinois held that the plaintiff did not have a common law right to privacy in posts made on Facebook and Twitter since approximately 1250 people were authorized to view the plaintiff’s accounts.²⁰¹ Furthermore, the California Court of Appeals recognized that postings made on Myspace are opened to the public eye, and, therefore, no reasonable person would have an expectation of privacy in their

191. *Id.*

192. 907 N.Y.S.2d 650 (Sup. Ct. 2010).

193. *Id.* at 654-55.

194. *Id.* at 657.

195. *Id.*

196. *Id.* at 656 (discussing how users are warned that their profiles are public spaces and that privacy settings are not perfect or impenetrable).

197. *Id.* at 657.

198. *Id.* (internal quotation marks omitted).

199. *Patterson v. Turner Constr. Co.*, 931 N.Y.S.2d 311, 312 (App. Div. 2011).

200. No. 10 C 7811, 2011 WL 6101949 (N.D. Ill. Dec. 7, 2011).

201. *Id.* at *7-8. In order to bring a common law right to privacy claim, the plaintiff must demonstrate that there was: “(1) an unauthorized intrusion into seclusion; (2) the intrusion would be highly offensive to a reasonable person; (3) the matter intruded upon was private; and (4) the intrusion caused plaintiffs anguish and suffering.” *Id.* at *7 (internal quotation marks omitted).

postings.²⁰² As a result, the court held that individuals do not have a right to privacy in information posted on Myspace.²⁰³

Recently, the Eastern District of Virginia held that individuals do not have a reasonable expectation of privacy in internet protocol ("IP") address information collected and stored by Twitter.²⁰⁴ The court compared the facts in *United States v. Miller*²⁰⁵ and *Smith* to information stored on Twitter.²⁰⁶ By accessing Twitter, individuals rely on Internet technology "indicating an intention to relinquish control of whatever information would be necessary to complete their communication."²⁰⁷ Individuals understand that "communications with Twitter [may] be transmitted out of private spaces and onto the Internet for routing to Twitter" and, therefore, do not have a reasonable expectation of privacy.²⁰⁸ Moreover, the court found it was significant that users accept Twitter's privacy policy²⁰⁹ as a condition to creating a Twitter account.²¹⁰ Even if users do not read Twitter's policies, they knowingly, willingly, and voluntarily reveal their information to Twitter's website and, therefore, lack any reasonable expectation of privacy.²¹¹

202. *Moreno v. Hanford Sentinel, Inc.*, 91 Cal. Rptr. 3d 858, 862 (Ct. App. 2009) (recognizing that "[p]rivate is not equivalent to secret"). Additionally, individuals do not have a reasonable expectation of privacy in file sharing software on a personal computer, since the software allows files to be openly shared with others using a similar program. *See United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009), *cert denied*, 130 S. Ct. 1309 (2010) ("One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking.").

203. *Moreno*, 91 Cal. Rptr. 3d at 863.

204. *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, No. 1:11-DM-3, 2011 WL 5508991, at *16-17 (E.D. Va. Nov. 10, 2011).

205. 425 U.S. 435 (1976).

206. *In re Application of the United States*, No. 1:11-DM-3, 2011 WL 5508991, at *17-18. Information stored on Twitter is similar to information obtained through pen registers, as both record information that "must be revealed to intermediaries as a practical necessity of completing communications over their respective networks." *Id.* at *18. The information is automatically revealed to a third party and may be associated with a particular person. *Id.* When individuals voluntarily convey information to Twitter, they forego any reasonable expectation of privacy. *See id.*

207. *Id.*

208. *Id.*

209. According to Twitter's privacy policy: "When using any of our Services you consent to the collection, transfer, manipulation, storage, disclosure and other uses of your information . . ." *Twitter Privacy Policy*, *supra* note 57. Additionally, the policy informs users that Twitter's "servers automatically record information." *Id.* When creating a Twitter account, user's provide personal information. *Id.* Users consent that this information may be publicly listed on Twitter. *Id.*

210. *In re Application of the United States*, No. 1:11-DM-3, 2011 WL 5508991, at *19 ("Petitioners voluntarily chose to use Internet technology to communicate with Twitter and thereby consented to whatever disclosures would be necessary to complete their communications.").

211. *Id.* at *16, *19 ("The mere recording of IP address information by Twitter and subsequent access by the government cannot by itself violate the Fourth Amendment."). *But see* *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 264-65 (S.D.N.Y. 2008) (denying disclosure of the contents

These cases demonstrate that courts are consistently holding that individuals lack any reasonable expectation of privacy in communications on social networking websites.²¹² Social networking websites have created “a public transcript of consciousness—storing [users’] thoughts, locations, social lives and memories in data warehouses all over the world.”²¹³ Information and details about a person’s life are only a few clicks away.²¹⁴ As a result, this information should not be subject to Fourth Amendment protection.

B. The SCA

Congress enacted the SCA in an attempt to “align[] newer forms of technology with the Fourth Amendment and preserve[] the ‘vitality’ of the Amendment by ensuring that privacy protections ‘kept pace’ with current advances in technology.”²¹⁵ The SCA provides “a range of statutory privacy rights against access to stored account information held by network service providers” by “regulating the relationship between government investigators and service providers in possession of users’ private information.”²¹⁶ Applying the SCA to social networking websites and modern technology has been a recurring challenge, as the SCA “fails to provide a clear framework for understanding whether a user has a reasonable expectation of privacy in his communications stored in the cloud.”²¹⁷ This struggle will continue to exist until Congress amends the SCA in order to reflect a proper balance between the needs of law enforcement and individuals’ diminishing privacy interests as a result of social networking websites.²¹⁸

of a user’s YouTube videos because YouTube’s privacy policy cannot “fairly be construed as a grant of permission from users to reveal . . . the videos that they have designated as private and chosen to share only with specified recipients”).

212. See *supra* Part III.A.2.

213. Sutter, *supra* note 136.

214. *Id.*

215. Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 628 (2011).

216. Kerr, *supra* note 16, at 1212. The SCA creates a code of procedure for federal and state law enforcement officers to follow in order to obtain stored communications from network service providers, regulates disclosure of consumer information, and prohibits unlawful access to certain stored communications. SEARCHING AND SEIZING COMPUTERS, *supra* note 14, at 115.

217. Kattan, *supra* note 215, at 645.

218. *Id.* at 652 (discussing how “the SCA fails to serve the interests of law enforcement, service providers, and customers” as a result of the emergence of cloud computing).

1. Purpose of the SCA

The federal government enacted the SCA in 1986 as a component of the ECPA.²¹⁹ The SCA is a complex statute that attempts to enhance privacy protection of information stored on computer networks.²²⁰ It creates certain “Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users’ private information.”²²¹ The purpose of the SCA was to create a “balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies” that can withstand rapid technological changes.²²² The SCA limits the government’s right to obtain an individual’s personal information from an ISP.²²³

The SCA was designed to provide privacy protection in the modern age since Congress felt that “consumers would not trust new technologies if the privacy of those using them was not protected.”²²⁴ Congress specifically designated the statute to govern “large-scale electronic mail operations, cellular and cordless phones, paging devices, miniaturized transmitters for radio surveillance, and . . . digitized networks.”²²⁵ The SCA “does not easily apply” to social networking websites, as these websites do not fit within any of the categories enumerated in the statute.²²⁶

When the SCA was enacted in 1986, computers were expensive and primarily used for storing and processing information.²²⁷ E-mail providers only maintained a user’s information temporarily in “electronic storage” before the information was delivered to the recipient.²²⁸ The World Wide Web did not exist, e-mail was a foreign term, and the web browser would not be introduced until the mid-1990s.²²⁹ The world’s smallest cellular phone weighed approximately

219. Kerr, *supra* note 16, at 1208.

220. See S. Rep. No. 99-541, at 1, 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555, 3557; Robison, *supra* note 16, at 1204-05.

221. Kerr, *supra* note 16, at 1212.

222. S. Rep. No. 99-541, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559.

223. Bennett, *supra* note 10, at 421.

224. H.R. Rep. No. 106-932, at 10 (2000).

225. *Id.* (quoting H.R. Rep. No. 99-647, at 18 (1986) (internal quotation marks omitted)).

226. Alan Klein et al., *Social Networking Sites: Subject to Discovery?*, NAT’L L.J., Aug. 23, 2010, at 15, 15 (stating that the SCA does not easily apply to content on Myspace and Facebook).

227. S. Rep. No. 99-541, at 3, *reprinted in* 1986 U.S.C.C.A.N. at 3557; Scolnik, *supra* note 167, at 376 (discussing how the SCA was passed when computers were far more expensive and far less powerful than they are today).

228. S. Rep. No. 99-541, at 3, *reprinted in* 1986 U.S.C.C.A.N. at 3557. See also Kerr, *supra* note 16, at 1213.

229. Sidoti et al., *supra* note 13, at S2.

fifteen ounces to two pounds and cost almost \$3300.²³⁰ Zuckerberg was only two years old and Facebook would not be founded for another eighteen years.²³¹ Today, technology, and the Internet in particular, has evolved to the extent that it has “changed the way people handle their affairs, and consequently the government’s handling of personal communications.”²³² Some of the fundamental changes in communications technology include e-mail, mobile location devices, cloud computing, and social networking.²³³

The SCA provides privacy protection to both electronic communication services (“ECS”) and remote computing services (“RCS”).²³⁴ The distinction between ECS and RCS is extremely complex and has posed a great amount of difficulty for courts and electronic communications providers to interpret—especially with respect to social networking websites.²³⁵ The biggest distinction between an ECS and RCS is that an RCS provider “may divulge the contents of a communication with the ‘lawful consent’ of the subscriber to the service, while the provider of an ECS may divulge such a communication only with the ‘lawful consent of the originator or an addressee or intended recipient of such communication.’”²³⁶

ECS is defined within the statute as “any service which provides to users thereof the ability to send or receive wire or electronic

230. 1986 Cell Phone, YOUTUBE (Mar. 9, 2010), <http://www.youtube.com/watch?v=A0iXebyRWgU>. Today, an iPhone weighs only 4.9 ounces. *iPhone 4S Technical Specifications*, APPLE, <http://www.apple.com/iphone/specs.html> (last visited Apr. 20, 2012).

231. See *Fact Sheet*, *supra* note 4; Mark Zuckerberg, FORBES <http://www.forbes.com/profile/mark-zuckerberg/> (last visited Apr. 20, 2012) (stating that Zuckerberg was twenty-seven years old in 2012).

232. H.R. Rep. No. 106-932, at 8-9 (2000). The ACLU has created a video outlining the various changes in technology since 1986 in order to increase awareness and encourage immediate action in reforming the SCA. *Online Privacy Stuck in 1986!*, YOUTUBE (Oct. 6, 2011), <http://www.youtube.com/watch?v=paLwr1nHiHU> (showing a video about how technology has advanced, while electronic privacy laws have remained at a standstill).

233. *About the Issue*, DIGITAL DUE PROCESS, <http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163> (last visited Apr. 20, 2012) (discussing the various changes in technology since the SCA was adopted in 1986).

234. Kerr, *supra* note 16, at 1214.

235. *Id.* at 1235 (providing suggestions on how to simplify the statute); Scolnik, *supra* note 167, at 376-77 (discussing the distinctions between ECS and RCS under the SCA); Howitson Keynote Address, *supra* note 158 (discussing the difficulty of applying the SCA to Facebook).

236. *Flagg v. City of Detroit*, 252 F.R.D. 346, 349-50 (E.D. Mich. 2008) (citing 18 U.S.C. § 2702(b)(3) (2006)). What satisfies the statute’s consent requirement has never been considered by a court. Orin Kerr, *Was the Stored Communications Act Actually Violated in City of Ontario v. Quon?*, THE VOLOKH CONSPIRACY (Apr. 19, 2010, 9:33 PM), <http://volokh.com/2010/04/19/was-the-stored-communications-act-actually-violated-in-city-of-ontario-v-quon/>.

communications.”²³⁷ Service providers must have the ability to send or receive electronic communications and hold the electronic communication in electronic storage.²³⁸ ECS providers are prohibited from “knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage.”²³⁹

In contrast, RCS is defined as “the provision to the public of computer storage or processing services by means of an electronic communications system.”²⁴⁰ An electronic communications system means “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.”²⁴¹ An RCS provider may not give any person or entity a subscriber’s communications that are carried or maintained on its service, unless there is an exception within the statute.²⁴² Some exceptions include a subscriber’s lawful consent, protection of the provider’s property rights, disclosure of the information that is necessary to avoid death or serious injury in an emergency situation, and execution of the subscriber’s intent.²⁴³

Congress intended the SCA to protect electronic communications that are considered “private.”²⁴⁴ The SCA does not apply to electronic communications that are readily accessible to the “general public.”²⁴⁵ Applying the distinction between an ECS and RCS to modern technology has been difficult for some courts.²⁴⁶ A single provider “can act as an RCS with respect to some communications, an ECS with respect to other communications, and neither an RCS nor an ECS with respect to other communications.”²⁴⁷ If a single provider qualifies as both an ECS and RCS, courts may not know what form of lawful consent is required in order for a subscriber to release any communications.²⁴⁸ According to the language of the statute, if the

237. Stored Communications Act, 18 U.S.C. § 2510(15).

238. Robison, *supra* note 16, at 1206.

239. Stored Communications Act, 18 U.S.C. § 2702(a)(1).

240. *Id.* § 2711(2).

241. *Id.* § 2510(14).

242. *See id.* § 2702(b) (discussing the different exceptions for disclosure of communications).

243. *Id.*

244. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002).

245. *See* Bennett, *supra* note 10, at 422.

246. *See, e.g.,* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010) (explaining how the court treated various communications tools on social networking websites differently under the SCA).

247. Kerr, *supra* note 16, at 1215-16.

248. *See* Flagg v. City of Detroit, 252 F.R.D. 346, 359 (E.D. Mich. 2008) (analyzing the SCA and the different levels of consent required if a provider is an ECS or RCS).

communication is in “electronic storage” in an ECS for 180 days or less, the information may only be retrieved pursuant to a warrant issued by a court.²⁴⁹ However, if the contents have been stored for more than 180 days, or qualify as an RCS, the electronic communication can only be disclosed with a valid warrant issued by a court, a court order, or an administrative subpoena after proper notice is given to the customer or subscriber.²⁵⁰ Courts and electronic communications providers have faced an extreme amount of difficulty interpreting the SCA, especially when applying it to newer technology and Facebook.²⁵¹

2. How Courts Have Interpreted the SCA

Despite the technological advances and exponential increases in the use of electronic communication in the United States since 1986, Congress has not amended the SCA.²⁵² As a result, courts have struggled with the challenge of applying the ancient statute to modern technology.²⁵³ This has caused a form of “legal acrobatics” within the court system.²⁵⁴

A California district court attempted to analyze whether Facebook and Myspace fell within the SCA’s definition of an ECS or RCS provider.²⁵⁵ Prior to *Crispin v. Christian Audigier, Inc.*,²⁵⁶ no court had determined whether a social networking website qualified as an ECS or RCS.²⁵⁷ In *Crispin*, the defendant served subpoenas duces tecum on Facebook and Myspace for the plaintiff’s subscriber information and communications relating to the case.²⁵⁸ The plaintiff moved to quash the subpoenas, claiming that the communications were protected under the SCA.²⁵⁹

The court analyzed the various facets of Facebook and Myspace, such as private messages, wall postings, and comments.²⁶⁰ Since

249. Stored Communications Act, 18 U.S.C. § 2703(a) (2006 & Supp. IV 2011). This is sometimes known as the “180 day rule.” Kattan, *supra* note 215, at 640.

250. Stored Communications Act, 18 U.S.C. § 2703(a)–(b) (discussing the requirements for disclosure of a customer’s communications or records within an electronic communication).

251. See *Crispin*, 717 F. Supp. 2d at 988. See also Howitson Keynote Address, *supra* note 158 (discussing the difficulty of applying the SCA to Facebook, since the SCA was enacted in 1986 before the expansion of cell phones, GPS systems, and texting).

252. Sidoti et al., *supra* note 13, at S2-S3.

253. *Id.* at S3.

254. *Id.* at S14.

255. *Crispin*, 717 F. Supp. 2d at 980-82.

256. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

257. *Id.* at 977 & n.24.

258. *Id.* at 968-69.

259. *Id.* at 969.

260. *Id.* at 987-89.

Facebook and Myspace postings can potentially be viewed only by those users that an individual selects, the court found them comparable to electronic bulletin board services ("BBS").²⁶¹ BBS are "communications networks" which "may be public or semi-public in nature, depending on the degree of privacy sought by users."²⁶² The court held that wall posts are similar to BBS and, therefore, ECS providers.²⁶³ Alternatively, the court also characterized wall postings as RCS providers, as the postings may be accessible to a limited set of users and stored on the service provider's website.²⁶⁴

It was not decided whether wall posts and comments could be retrieved through a subpoena under the SCA.²⁶⁵ Instead, the court remanded the case in order to review the plaintiff's privacy settings.²⁶⁶ Evidence of the plaintiff's privacy settings would have helped the court determine whether the general public or a limited number of people had access to the wall posts and comments.²⁶⁷ If the plaintiff's Facebook and Myspace profiles were readily available to the general public, disclosing the information would not have violated the SCA.²⁶⁸

The analysis in *Crispin* demonstrates the "legal acrobatics" courts have faced in determining whether social networking websites qualify as an ECS or RCS provider.²⁶⁹ The SCA is "outdated and not ideally structured to address modern electronic communications disclosure and privacy issues."²⁷⁰ This form of "legal acrobatics" will continue until Congress brings the law in line with modern technology.²⁷¹

Other courts have reached various conclusions when interpreting the SCA. In *Konop v. Hawaiian Airlines, Inc.*,²⁷² the Ninth Circuit Court

261. *Id.* at 980.

262. *Id.* at 980 n.33 (quoting S. Rep. No. 99-541, at 8-9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562-63).

263. *Id.* at 980-82.

264. *Id.* at 990. The court came to this conclusion because "there is no intermediate in-transition stage where the posting or comment has yet to be opened." Sidoti et al., *supra* note 13, at S14. Additionally, the court characterized wall postings as ECS and RCS providers since they are stored for the purpose of backup protection and may be restricted by the poster to a limited number of selected users. *Id.*

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

266. *Id.*

267. *Id.*

268. *See id.* (noting that in order to quash the subpoena of the wall postings, it must be assumed that the information is not available to the general public, as information accessible to the general public does not violate the SCA). This conclusion can be evidenced by the court's decision to quash the subpoena of private messages because they were not readily accessible to the general public. *See id.*

269. *See* Sidoti et al., *supra* note 13, at S14.

270. *Id.*

271. *Id.*

272. 302 F.3d 868 (9th Cir. 2002).

of Appeals determined that the SCA was violated where an unauthorized individual accessed the content of a restricted website.²⁷³ The unauthorized individual did not qualify as a “user” under the SCA and, therefore, did not have authority to access the communications on the website.²⁷⁴ The court recognized that the ECPA is complex, as “the existing statutory framework is ill-suited to address modern forms of communication.”²⁷⁵ Moreover, “until Congress brings the laws in line with modern technology, protection of the Internet and websites . . . will remain a confusing and uncertain area of the law.”²⁷⁶

In *Flagg v. City of Detroit*,²⁷⁷ the Eastern District of Michigan avoided the SCA issue regarding discovery of text messages from a non-party service provider, since it was difficult to answer and there was “a more straightforward path . . . readily available” under Rule 34 of the Federal Rules of Civil Procedure.²⁷⁸ Additionally, in *In re Facebook Privacy Litigation*,²⁷⁹ the plaintiff failed to state a cause of action under the SCA, therefore, the court did not address the merits of whether Facebook was an ECS or RCS provider.²⁸⁰

The South Carolina Court of Appeals held in *Jennings v. Jennings*²⁸¹ that Yahoo! was both an ECS and RCS provider with regards to e-mails stored on its website and such communications would be protected under the SCA.²⁸² Furthermore, in *In re Subpoena Duces Tecum to AOL, LLC*,²⁸³ the Eastern District of Virginia held that the AOL corporation may not divulge the contents of an individual’s electronic communications because the SCA “does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas.”²⁸⁴ These cases demonstrate the various ways courts have attempted to apply the SCA to modern technology.

273. *Id.* at 875-76, 875 n.3.

274. *Id.* at 880 (internal quotation marks omitted).

275. *Id.* at 874.

276. *Id.*

277. 252 F.R.D. 346 (E.D. Mich. 2008).

278. *Id.* at 366.

279. No. C 10-02389 JW, 2011 WL 6176208 (N.D. Cal. Nov. 22, 2011).

280. *Id.* at *3-4, *3 n.7.

281. 697 S.E.2d 671 (S.C. Ct. App. 2010).

282. *Id.* at 676 (“[E]ven if Yahoo was acting as an RCS with respect to the emails at issue, there is no question that Yahoo was also acting as an ECS with regard to those same emails.”).

283. 550 F. Supp. 2d 606 (E.D. Va. 2008).

284. *Id.* at 611 (noting that the SCA does not apply to private parties in civil litigation).

3. Challenges in Applying the SCA to Modern Technology

The reality of the SCA is that “the existing statutory framework is ill-suited to address modern forms of communication.”²⁸⁵ Several courts have experienced difficulty in analyzing problems involving modern technology within the confines of the current statutory framework.²⁸⁶ Until Congress brings the law in line with modern technology, it will be difficult for courts to come to a concrete, unified interpretation of the SCA.²⁸⁷ This is a challenge since “[t]he law cannot keep up with the pace of change in computer networking[]” and by “the time legislatures or courts figure out how to deal with a new product or service, the technology has already progressed.”²⁸⁸

According to Mark Howitson, Facebook’s deputy general counsel, Facebook will not turn over any information without a civil subpoena, unless it receives the user’s lawful consent.²⁸⁹ Even if Facebook receives a lawful subpoena, it interprets the SCA to only allow disclosure of basic subscriber information.²⁹⁰ Basic subscriber information includes, but is not limited to, a user’s name, length of service, credit card information, e-mail address, and IP address.²⁹¹ Moreover, Facebook will not disclose the contents of a user’s communications in response to a court order.²⁹² Facebook views all of its user’s information on their website as “content” under the SCA, and, therefore requires a warrant based upon probable cause.²⁹³ Howitson stated that he is “itching for that fight” and waiting for a case to go before a federal judge “to define exactly what content on Facebook is protected so that it’s clearer to everyone.”²⁹⁴

Although Justice Brandeis stated, “[i]n the application of a constitution . . . our contemplation cannot be only of what has been but of what may be[,]” he could have never predicted the impact social

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

286. *See supra* Part III.B.2.

287. *Konop*, 302 F.3d at 874. *See also* Nicholas Matlach, Comment, *Who Let the Katz Out?: How the ECPA and SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles in Katz v. United States Will Fix It*, 18 COMMLAW CONSPECTUS 421, 457 (2010) (“Congress follows the turtle law: slow and steady wins the race.”).

288. Robison, *supra* note 16, at 1197.

289. Howitson Keynote Address, *supra* note 158.

290. *Id.*

291. *See id.* *See also Information for Law Enforcement Authorities*, *supra* note 160.

292. *Information for Law Enforcement Authorities*, *supra* note 160.

293. Stored Communications Act, 18 U.S.C. § 2702(a)(2) (2006) (“[A] person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the *contents* of any communication which is carried or maintained on that service.” (emphasis added)); Howitson Keynote Address, *supra* note 158. *See also Information for Law Enforcement Authorities*, *supra* note 160.

294. Howitson Keynote Address, *supra* note 158.

networking would have on our society.²⁹⁵ People have become extremely comfortable sharing their personal information on Facebook and the Internet.²⁹⁶ This “social norm” has led to a lack of an expectation of privacy on social networking websites.²⁹⁷ A CNN report stated, “[w]elcome to the world of public living—where most everything about a person’s habits, location and preferences [are] just a few clicks away.”²⁹⁸ Since the SCA was designed to provide privacy protection in the modern age, the statute must properly reflect a user’s lack of expectation of privacy in information posted on Facebook.²⁹⁹

C. *City of Ontario v. Quon*

In a recent case, *City of Ontario v. Quon*,³⁰⁰ the U.S. Supreme Court held that a public employer’s search of its employee’s text messages stored on an employer-provided pager was not a violation of the employee’s Fourth Amendment rights.³⁰¹ The Supreme Court denied the petition for certiorari filed by Arch Wireless, the wireless service provider, challenging the Ninth Circuit’s ruling that it violated the SCA.³⁰² *Quon* is an interesting case as it discusses both the Fourth Amendment and the SCA with regards to cellular telephones and text messages.³⁰³

In *Quon*, a City of Ontario (the “City”) employer noticed that its employee, Quon, was exceeding the monthly character limit on the pager provided to him by the City.³⁰⁴ As a result, the City requested a transcript of Quon’s text messages from Arch Wireless in order to determine

295. See *Olmstead v. United States*, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

296. Matyszczyk, *supra* note 87.

297. See Chad Perrin, *Why You Should Never Trust Facebook*, TECHREPUBLIC (Nov. 12, 2010, 7:04 AM PST), <http://www.techrepublic.com/blog/security/why-you-should-never-trust-facebook/4708>. There are only two ways to ensure any real privacy on Facebook. First, “[n]ever use Facebook. Never create an account in the first place.” *Id.* Second, “[n]ever share anything with Facebook that divulges any information at all that you would prefer to keep private. This includes email addresses as part of your supposedly private account data that you would not want shared with spammers, or authentication information (usernames and passwords) you use anywhere else.” *Id.*

298. Sutter, *supra* note 136.

299. See S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. See also *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 656-57 (Sup. Ct. 2010) (holding that users do not have any reasonable expectation of privacy in their Facebook or Myspace profiles since they are aware that all information may become public and neither website guarantees complete privacy).

300. *City of Ontario v. Quon* (*Quon II*), 130 S. Ct. 2619 (2010).

301. *Id.* at 2633.

302. *Id.* at 2627. See also *Quon v. Arch Wireless Operating Co.* (*Quon I*), 529 F.3d 892, 903 (9th Cir. 2008).

303. *Quon II*, 130 S. Ct. at 2632-33.

304. *Id.* at 2625.

whether the text messages were work-related.³⁰⁵ Arch Wireless provided the City with the transcripts, and Quon claimed that this violated the SCA and his Fourth Amendment right to privacy.³⁰⁶

The Ninth Circuit held that Arch Wireless violated the SCA since it qualified as an ECS and knowingly provided an electronic communications service to the City.³⁰⁷ When Arch Wireless “knowingly turned over the text-messaging transcripts to the City, which was a ‘subscriber,’ not ‘an addressee or intended recipient of such communication,’ it violated the SCA.”³⁰⁸ If Arch Wireless instead qualified as an RCS, it would not have violated the SCA by providing the City with the transcripts.³⁰⁹ RCS providers “can release such information ‘with the lawful consent of . . . the subscriber’” and it was “undisputed that . . . the City was a ‘subscriber.’”³¹⁰ The court held that Arch Wireless was an ECS under the statute, as it transmitted electronic communications and archived the communications for “backup protection” and not for “storage purposes.”³¹¹

Although the Supreme Court did not specifically address the merits of the SCA claim, it held that Quon’s Fourth Amendment rights were not violated since the search of his text messages was reasonable.³¹² The Court did not address whether Quon had a reasonable expectation of privacy in his text messages, and instead presumed that he did for the sake of the case.³¹³ Justice Anthony M. Kennedy delivered the opinion and recognized that “[t]he Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in

305. *Id.* at 2626.

306. *Id.*

307. *Quon I*, 529 F.3d at 902-03.

308. *Id.* at 903.

309. *Id.* at 900.

310. *Id.*

311. *Id.* at 902. If Arch Wireless retained a permanent copy of the text messages to benefit the City, the court may have held Arch Wireless was an RCS. *See id.* at 902-03. If Arch Wireless was an RCS, it would not have violated the SCA. *See supra* text accompanying notes 309-10.

312. *City of Ontario v. Quon (Quon II)*, 130 S. Ct. 2619, 2632-33 (2010).

313. *Id.* at 2630 (“For present purposes we assume several propositions *arguendo*: First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City . . .”).

society has become clear.”³¹⁴ Further, the Court noted that “[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.”³¹⁵

Although the Court denied certiorari on the SCA issue, the Court still addressed the SCA in its opinion.³¹⁶ The Court held that “even if the Court of Appeals was correct to conclude that the SCA forbade Arch Wireless from turning over the transcripts, it does not follow that petitioners’ actions were unreasonable.”³¹⁷ The existence of statutory protection under the SCA did not make the search per se unreasonable under the Fourth Amendment.³¹⁸ As a result, “[t]he otherwise reasonable search . . . [was] not rendered unreasonable by the assumption that Arch Wireless violated the SCA by turning over the transcripts.”³¹⁹

Although the City officials needed Arch Wireless to generate a transcript of the messages, the Supreme Court held “it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny.”³²⁰ This demonstrates that the Court was not troubled by the SCA violation because the search was otherwise reasonable under the Fourth Amendment.³²¹ As a result, “[b]ecause the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable” under the Fourth Amendment.³²²

314. *Id.* at 2629. Justice Alito recognized in *United States v. Jones* that “[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative” as the “legislative body is well situated to gauge changing public attitudes to draw detailed lines, and to balance privacy and public safety in a comprehensive way.” 132 S. Ct. 945, 964 (2012) (Alito, J., concurring). Additionally, “judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person.” *Id.* at 962.

315. *Quon II*, 130 S. Ct. at 2629. The Court also expressed concern in deciding whether Quon had a reasonable expectation of privacy in his text messages since the law is only “beginning to respond to these developments” and “[a]t present, it is uncertain how workplace norms, and the law’s treatment of them, will evolve.” *Id.* at 2630. Additionally, the Court was cautious in its decision since “[a] broad holding concerning employees’ privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted.” *Id.* Justice Alito expressed similar concern in his concurrence in *Jones* and recognized that dramatic technological change “may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile.” *Jones*, 132 S. Ct. at 962 (Alito, J., concurring).

316. *Quon II*, 130 S. Ct. at 2627, 2632.

317. *Id.* at 2632.

318. *See id.*

319. *Id.*

320. *Id.* at 2626, 2631.

321. *See id.* at 2631-32. This is evidenced by the fact that the Court was not concerned that the City only obtained the transcripts as a result of Arch Wireless’s SCA violation because the City’s search was reasonable under the Fourth Amendment. *See id.*

322. *Id.* at 2632.

IV. SOLUTIONS PROPOSED IN RESPONSE TO A LACK OF CONGRESSIONAL REFORM TO THE SCA

As technology has advanced and social networking has become more prevalent in society, it is important for Congress to ensure the SCA reflects current Fourth Amendment privacy protections.³²³ Since society has become more accustomed to sharing information on Facebook, the SCA no longer achieves a proper balance between the interests and needs of law enforcement and the privacy interests of the American people.³²⁴ This problem has led to a variety of solutions proposed by different individuals and organizations.

A. Congressional Hearings on ECPA and SCA Reform

The ECPA consists of a “patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies.”³²⁵ The statute has created a variety of conflicting standards, illogical distinctions, judicial criticism, and constitutional uncertainty.³²⁶ “[T]he reality today is that the ECPA increasingly falls short of a common sense test.”³²⁷

In an effort to reform the ECPA, the House Committee on the Judiciary has held several hearings to fully understand the growth of technology and receive suggestions for statutory amendments.³²⁸ U.S. Congressman Jerrold Nadler stated that it will be a challenge “to find the appropriate balance between privacy and law enforcement interests; to protect the public while preserving consumer privacy and confidence; and, to support rapid technological innovation and growth yet discern standards for law enforcement access that will not become outdated with each new generation of technology.”³²⁹ Within these Committee

323. See Matlach, *supra* note 287, at 457, 459.

324. See *ECPA Reform Hearing*, *supra* note 23, at 2 (statement of Rep. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, & Civil Liberties). See also *supra* Part II.E.

325. *About the Issue*, *supra* note 233.

326. *Id.*

327. *Weather Report: Cloud-E with a Chance of Privacy Law Changes*, JUSTIA.COM (Sept. 30, 2010), <http://onward.justia.com/2010/09/30/weather-report-cloud-e-with-a-chance-of-privacy-law-changes/> (quoting Microsoft’s general counsel Brad Smith) (internal quotation marks omitted).

328. See *ECPA Government Perspectives*, *supra* note 26, at 1 (statement of Sen. Patrick J. Leahy, Chairman, S. Comm. on the Judiciary); *ECPA Cloud Computing Hearing*, *supra* note 23, at 1 (statement of Rep. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, & Civil Liberties); *ECPA Location Technology Hearing*, *supra* note 23, at 1 (statement of Rep. F. James Sensenbrenner, Jr., Member, Subcomm. on the Constitution, Civil Rights, & Civil Liberties); *ECPA Reform Hearing*, *supra* note 23, at 1 (statement of Rep. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, & Civil Liberties). See also Press Release, Congressman Jerrold Nadler, *supra* note 18.

329. Press Release, Congressman Jerrold Nadler, *supra* note 18.

hearings, Congress considered “whether [the] ECPA still strikes the right balance between the interests and needs of law enforcement and privacy interests of the American people.”³³⁰ The Committee recognized that this was an enormous responsibility and that changes in technology have subverted the original intent of the statute.³³¹

The present state of the ECPA has caused confusion amongst customers, the government, and service providers about what data is subject to protection under the statute.³³² Today, “the status of a single email changes dramatically depending on where it is stored, how old it is, and even the district within which the government issues or serves its process.”³³³ This is because of the “fundamental shift in the amount of sensitive information that we now trust to third parties.”³³⁴ As a result, “the basic technological assumptions upon which [the] ECPA was based are outdated.”³³⁵ According to one witness, Congress “should consider not only the appropriate balance between the needs of law enforcement and protection of civil liberties, but also the effects of its decisions on the health of the Internet ecosystem.”³³⁶ One solution proposed was to develop a “clear set of rules for law enforcement access that will safeguard end-user privacy, provide clarity for service providers, and enable law enforcement officials to conduct effective and efficient investigations.”³³⁷

State and local law enforcement officers are concerned because criminals are communicating with thousands of people through different media, including social networking websites.³³⁸ Law enforcement

330. *ECPA Reform Hearing*, *supra* note 23, at 2 (statement of Rep. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, & Civil Liberties).

331. *Id.* Regarding the ECPA’s current protection of social networking websites, one witness testified: “One of the most striking developments of the past few years has been the remarkable growth of social networking. Hundreds of millions of people now use these social media services to share information with friends and as an alternative platform for private communications.” *Id.* at 11 (statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology).

332. *Id.* at 12.

333. *Id.* at 19 app. A.

334. *Id.* at 43 (statement of Annmarie Levins, Associate General Counsel, Microsoft Corporation).

335. *Id.*

336. *ECPA Cloud Computing Hearing*, *supra* note 23, at 89 (statement of Kevin Werback, Associate Professor, The Wharton School, University of Pennsylvania).

337. *ECPA Reform Hearing*, *supra* note 23, at 12 (statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology).

338. *ECPA Cloud Computing Hearing*, *supra* note 23, at 101 (statement of Thomas B. Hurbaneck, Senior Investigator, New York State Police Computer Crime Unit). Additionally, the general counsel for the U.S. Department of Commerce recognized:

The Internet-based digital economy has sparked tremendous innovation. During the past fifteen years, networked information technologies—personal computers, mobile

officials need to access the information stored on these media quickly to avoid potential deletion or corruption of evidence.³³⁹ As a senior investigator stated, “[t]ime is our enemy in Internet investigations.”³⁴⁰ Technological advancements have created a variety of new sources for law enforcement to assess and these entities “must be contacted to build information during an investigation.”³⁴¹ The Department of Justice is especially concerned that an amendment restricting law enforcement’s ability to obtain information quickly and efficiently could have “a very real and very human cost.”³⁴² Increasing standards for obtaining information under the ECPA may “substantially slow criminal and national investigations.”³⁴³ According to the executive director of the Chicago High Intensity Drug Trafficking Area Program, “law enforcement must preserve its ability to conduct lawfully-authorized electronic surveillance and must have reasonably expeditious access to stored information that may constitute evidence of a crime committed or about to be committed regardless of the technology platform on which it resides or is transferred.”³⁴⁴ Without this authority, public safety is at risk.³⁴⁵

B. *The Digital Due Process Coalition*

The need for Congressional reform of the SCA has sparked the formation of the Digital Due Process coalition.³⁴⁶ The Digital Due

phones, wireless connections and other devices—have transformed our social, political, and economic landscape. A decade ago, going online meant accessing the Internet on a computer in your home, most often over a copper-wire telephone line. Today, “going online” also includes smartphones, tablets, portable games, and interactive TVs, with numerous companies developing global computing platforms in the “cloud.”

ECPA Government Perspectives, *supra* note 26, at 52 (statement of Cameron F. Kerry, General Counsel, U.S. Department of Commerce). These developments have posed numerous problems for law enforcement. *Id.*

339. *ECPA Cloud Computing Hearing*, *supra* note 23, at 102 (statement of Thomas B. Hurbank, Senior Investigator, New York State Police Computer Crime Unit) (“Technology has created many new sources of information that may be accessed by law enforcement equalized by the very number of private sector entities that must be contacted to build information during an investigation.”).

340. *Id.*

341. *Id.*

342. *ECPA Government Perspectives*, *supra* note 26, at 40 (statement of James A. Baker, Associate Deputy Att’y Gen., U.S. Department of Justice).

343. *Id.*

344. *ECPA Cloud Computing Hearing*, *supra* note 23, at 114-15 (statement of Kurt F. Schmid, Executive Director, Chicago High Intensity Drug Trafficking Area Program).

345. *Id.* at 115.

346. Richard Salgado, *Our Stand for Digital Due Process*, GOOGLE PUB. POL’Y BLOG (Mar. 30, 2010, 12:09 PM ET), <http://googlepublicpolicy.blogspot.com/2010/03/our-stand-for-digital-due-process.html> (showing a video that outlines the purpose of the Digital Due Process coalition).

Process coalition was developed to “simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.”³⁴⁷ Some of the coalition members include Amazon.com, America Online, American Civil Liberties Union, eBay, Google, Microsoft, Apple, Intel, and Facebook.³⁴⁸ Although the members of the coalition disagree on several issues, they “all agree that this area of the law needs to be updated to reflect changes in technology.”³⁴⁹

The Digital Due Process coalition advocates four main methods to reform the ECPA.³⁵⁰ The coalition wishes to: (1) treat online communication documents “the same as if they were stored at home” by requiring a “search warrant before compelling a service provider to access and disclose the information”; (2) “[r]equire the government to get a search warrant before it can track movements through” cell phones or other mobile devices; (3) require service providers to disclose information about communications in real-time, making it easier for the government to identify specific information that is relevant to its investigation; and (4) require the government to demonstrate to a court that the information is needed for an investigation in order to obtain information regarding an entire class of users during a criminal investigation.³⁵¹ The members of Digital Due Process recognize that this is just the beginning of a long process that will require public discussion, the engagement of other stakeholders, and dialogue with law enforcement agencies.³⁵² Congress should evaluate the coalition’s search warrant proposal in light of a potential burden on the government and an individual’s lack of privacy on social networking websites.³⁵³

347. *Our Principles*, DIGITAL DUE PROCESS, <http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163> (last visited Apr. 20, 2012).

348. See *Who We Are*, *supra* note 23.

349. Miguel Helft, *A Wide Call to Improve Web Privacy*, N.Y. TIMES, Mar. 31, 2010, at B1 (quoting Kevin Bankston, a senior staff attorney with the Electronic Frontier Foundation) (internal quotation marks omitted).

350. See *ECPA Cloud Computing Hearing*, *supra* note 23, at 22 (statement of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google Inc.). The coalition proposes that the SCA is simplified to reflect the “reasonable privacy interests of today’s online citizens, and to ensure that government has the legal tools needed to enforce the laws.” *Id.*

351. *Id.* See also *Our Principles*, *supra* note 347 (discussing the principles and ideas of the Digital Due Process coalition).

352. *ECPA Reform Hearing*, *supra* note 23, at 5-6 (testimony of James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology).

353. See *Our Principles*, *supra* note 347. See also *supra* Part II.D-E (discussing the different

C. *Electronic Communications Privacy Act Amendments of 2011*

On May 17, 2011, Senator Patrick J. Leahy introduced the Electronic Communications Privacy Act Amendments Act of 2011.³⁵⁴ The bill was introduced in an effort to bring federal electronic privacy laws into the digital age to conform with new technologies.³⁵⁵ Senator Leahy was the lead author of the original ECPA law adopted in 1986 and admits that no one could have predicted the current issues in digital privacy.³⁵⁶ While drafting the bill, Senator Leahy attempted to develop a careful balance of “the interests and needs of consumers, law enforcement, and our Nation’s thriving technology sector.”³⁵⁷

Some amendments specified within the bill include: (1) adding a geolocation information and RCS category; (2) deleting the current 180 day rule and substituting it with a warrant requirement based on probable cause in order to compel disclosure of electronic communications; (3) requiring the government to notify individuals within three days of obtaining electronic information and provide them with a copy of the search warrant; and (4) allowing the government to use an administrative or grand jury subpoena only when obtaining general subscriber information.³⁵⁸ The bill also requires law enforcement to obtain a search warrant or court order for all geolocation information “collected, stored or used by mobile devices and mobile applications, such as smartphones and tablets.”³⁵⁹ Additionally, the bill permits “a provider to voluntarily disclose content that is pertinent to addressing a cyberattack involving their computer network to either the government or to a third party.”³⁶⁰

methods and people users can share information with on Facebook).

354. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011) (as of May 17, 2011, the bill was referred to the Senate Committee on the Judiciary). *See also* 112 CONG. REC. S3054 (daily ed. May 17, 2011) (statement of Sen. Patrick J. Leahy).

355. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011) (as of May 17, 2011, the bill was referred to the Senate Committee on the Judiciary).

356. *Id.* *See also* Press Release, Senator Patrick Leahy, Leahy Introduces Benchmark Bill to Update Key Digital Privacy Law (May 17, 2011), http://www.leahy.senate.gov/press/press_releases/release/?id=b6d1f687-f2f7-48a4-80bc-29e3c5f758f2.

357. 112 CONG. REC. S3054 (daily ed. May 17, 2011) (statement of Sen. Patrick J. Leahy).

358. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011) (as of May 17, 2011, the bill was referred to the Senate Committee on the Judiciary). For a summary of the amended sections, see Press Release, Senator Leahy, *supra* note 356. General subscriber information includes the subscriber’s name, address, session time records, length of service information, subscriber number and temporarily assigned network address, and means and source of payment information. *Id.*

359. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011) (as of May 17, 2011, the bill was referred to the Senate Committee on the Judiciary). For a summary of the amended sections, see Press Release, Senator Patrick Leahy, *supra* note 356.

360. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011) (as of May 17, 2011, the bill was referred to the Senate Committee on the Judiciary). For a

Supporters of the bill believe that this is a significant step towards updating Internet privacy laws.³⁶¹

V. PROPOSED SOLUTIONS

Most scholars and privacy experts would agree that there is a pressing need to amend the SCA as it is outdated and difficult to apply to modern technology.³⁶² Although the Digital Due Process coalition and Electronic Communications Privacy Act Amendments Act of 2011 propose a warrant requirement to obtain content stored within electronic communications, this may be too burdensome on law enforcement.³⁶³ The purpose of the SCA was to establish Fourth Amendment statutory protections and “balance the privacy expectations of American citizens and the legitimate needs of law enforcement agencies” that can withstand rapid technological changes.³⁶⁴ Currently, the SCA fails to achieve a proper balance.³⁶⁵ By imposing a blanket warrant requirement for communications stored on social networking websites, law enforcement officials may be deprived of essential building blocks for criminal investigations.³⁶⁶

Just as the ECPA “treats addressing information associated with email and other electronic communications differently from addressing information associated with phone calls,” the ECPA should also treat Facebook and other social networking websites differently.³⁶⁷ Achieving a proper balance requires Congress to consider an appropriate level of privacy protection that “flow[s] from an assessment of . . . factors, including the expectation of privacy surrounding the mode of communication used in connection with the content, who has access and use of that information, and the interest of law enforcement and national security.”³⁶⁸

summary of the amended sections, see Press Release, Senator Patrick Leahy, *supra* note 356.

361. 112 CONG. REC. S3054.

362. *See id.* (demonstrating that even Senator Leahy, a drafter of the SCA, believes that it must be reformed); Helft, *supra* note 349, at B8. *See also ECPA Location Technology Hearing*, *supra* note 23, at 4 (statement of Rep. Henry C. “Hank” Johnson, Jr., Member, Subcomm. on the Constitution, Civil Rights, & Civil Liberties).

363. *See* discussion *supra* Part IV.

364. S. Rep. No. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

365. Kattan, *supra* note 215, at 652.

366. *ECPA Government Perspectives*, *supra* note 26, at 49 (statement of Sen. Chuck Grassley, Member, S. Comm. on the Judiciary).

367. *See id.* at 44 (statement of James A. Baker, Associate Deputy Att’y Gen., U.S. Department of Justice).

368. *See id.* at 59 (statement of Cameron F. Kerry, General Counsel, U.S. Department of Commerce).

The SCA should reflect privacy considerations that are consistent with the Fourth Amendment.³⁶⁹ Therefore, it is important to assess whether individuals have any reasonable expectation of privacy on Facebook when considering how to properly amend the SCA.³⁷⁰ The SCA should not impose heightened warrant requirements on the government where individuals have relinquished any reasonable expectation of privacy. It is inconsistent with the Fourth Amendment to impose a warrant requirement when individuals are knowingly disclosing their information to “friends” on Facebook.³⁷¹

Although the Supreme Court in *Quon* was hesitant in determining whether an individual had a reasonable expectation of privacy in electronic equipment, the Court was not troubled by the potential SCA violation.³⁷² The Court held that the employer’s search was reasonable under the Fourth Amendment even though this search would have been impossible had the wireless provider not violated the SCA by turning over the transcripts.³⁷³ The existence of statutory protection under the SCA did not make the search per se unreasonable under the Fourth Amendment.³⁷⁴

As Justice Scalia noted in *Kyllo*, “[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”³⁷⁵ Moreover, as Justice Samuel Alito discussed in *United States v. Jones*,³⁷⁶ technological change may reform what the “reasonable person” assumes is private.³⁷⁷ As a result, technology “may provide increased convenience or security at the expense of privacy and many people find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.”³⁷⁸

369. See *id.* at 66 (joint letter dated Apr. 6, 2011 to Sen. Patrick J. Leahy and Sen. Charles E. Grassley from Tech Freedom et al.).

370. See *id.*

371. See *United States v. Miller*, 425 U.S. 435, 443 (1976) (“[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . .”).

372. See *City of Ontario v. Quon (Quon II)*, 130 S. Ct. 2619, 2629, 2632 (2010). See also *supra* text accompanying notes 304-12.

373. *Quon II*, 130 S. Ct. at 2626, 2633. See also discussion *supra* Part III.C.

374. *Quon II*, 130 S. Ct. at 2632.

375. *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001).

376. 132 S. Ct. 945 (2012).

377. *Id.* at 962 (Alito, J., concurring).

378. *Id.*

Several lower courts have made it clear that individuals do not have a reasonable expectation of privacy in information posted on Facebook and similar websites.³⁷⁹ Existing social norms inherent in Facebook demonstrate that users feel comfortable sharing information on the Internet.³⁸⁰ Facebook's "mission is to give people the power to share and make the world more open and connected."³⁸¹ Users are voluntarily revealing information on Facebook and, therefore, lack any reasonable expectation of privacy.³⁸² By disclosing information to a third party, users risk that this information may be conveyed to the government.³⁸³

Additionally, Facebook's data use policy warns its users, amongst other things, that "if [they] share something on Facebook, anyone who can see it can share it with others."³⁸⁴ This policy and other policies are conditions users must agree to in order to access Facebook's services.³⁸⁵ Lower courts have correctly accepted that these privacy policies sufficiently warn users that they have no right to privacy in the information posted on these websites.³⁸⁶

Moreover, other social networking websites warn users to be careful about what they post, since the general public may view their information.³⁸⁷ By knowingly disclosing information to a third party, individuals risk that their information may be conveyed to the government. As a result, individuals do not maintain a reasonable expectation of privacy under the Fourth Amendment in information posted on social networking websites.³⁸⁸ If an individual wishes to maintain a reasonable expectation of privacy, they should not place their life on the Internet.

As a result of the social norms established with Facebook, the SCA should not impose strict and often confusing regulations protecting

379. See discussion *supra* Part III.A.2.

380. See discussion *supra* Part II.E.

381. *About*, *supra* note 82.

382. See *United States v. Miller*, 425 U.S. 435, 443 (1976); *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 656 (Sup. Ct. 2010) ("[A]s neither Facebook nor MySpace guarantee complete privacy, Plaintiff has no legitimate expectation of privacy.").

383. *Miller*, 425 U.S. at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

384. *Data Use Policy*, *supra* note 21.

385. See generally *id.*; *Statement of Rights and Responsibilities*, *supra* note 8.

386. See discussion *supra* Part III.A.2.

387. See *supra* text accompanying notes 130-36 (describing Twitter and Myspace's privacy policies).

388. See discussion *supra* Part III.A.2.

privacy rights that may not exist under the Fourth Amendment. Although the SCA has had difficulty keeping pace with technology in order to maintain Fourth Amendment protections,³⁸⁹ Facebook users should not be given additional statutory protection they would not otherwise receive under the Constitution.

VI. CONCLUSION

Social networking websites have helped individuals communicate and share information quickly and efficiently. Facebook bases its principles on trying to make the world more open and transparent by giving individuals greater power to share and connect with one another.³⁹⁰ With the simple click of a button, individuals may display their deepest secrets on the Internet. Current social norms reflect that people feel comfortable reporting their daily thoughts and moods on Facebook—often with people they have never even met. However, individuals do not realize that “[t]he Internet’s not written in pencil . . . it’s written in ink” and the “ink” may be easily stored and later retrieved.³⁹¹

Information stored on social networking websites such as Facebook is extremely valuable in the legal realm. These websites provide detailed information about a person or entity. However, if a user chooses to “delete” or “deactivate” his or her account, this information may be difficult for attorneys or law enforcement officials to retrieve during discovery.³⁹² Facebook claims that the SCA prohibits it from disclosing the content of communications even if a valid subpoena or court order is issued.³⁹³

The SCA has not been amended since its enactment in 1986 to encompass the overwhelming changes in technology. The current state of the SCA has presented a challenge for law enforcement officials and attorneys when attempting to obtain necessary evidence from social networking websites for discovery. When reforming the SCA, Congress should consider the current social norms that have been established with Facebook and the privacy protection available under the Fourth Amendment. At bottom, Facebook should be required to turn over

389. See discussion *supra* Part III.B.

390. *Facebook Principles*, FACEBOOK, <http://www.facebook.com/principles.php> (last visited Apr. 20, 2012).

391. See THE SOCIAL NETWORK, *supra* note 70.

392. Wilson, *supra* note 11, at 1207-08.

393. *Information for Law Enforcement Authorities*, *supra* note 160.

information pursuant to a discovery request, since users consent via the website's terms and conditions that their information may become public.³⁹⁴

*Lindsay S. Feuer**

394. See *supra* text accompanying notes 124-30.

* J.D. candidate, 2012; Hofstra University School of Law. This Note would not have been possible without the endless encouragement and guidance of Professor Frank Gulino. Thank you for always believing in me and pushing me to take risks in my legal career. Over the past three years, you have molded me into a better writer, advocate, and future attorney. I would also like to thank Professor Andrew H. Lupu for his thoughtful suggestions and insight. Thank you Sarah Wieselthier, David Gerardi, and Emily Harper for your meticulous editing throughout all of my 394 footnotes. A special thank you to Allana Grinshteyn, Simone Hicks, and Gabrielle Blum for your patience, moral support, and friendship. Thank you to all of my friends and family members who have not “defriended” me over the past three years. You have all been my number one cheerleaders and have never stopped supporting me. Finally, I dedicate this Note to my parents. Mom and Dad—thank you for always reminding me that there is a light at the end of the tunnel and for believing in me when I sometimes failed to believe in myself. Thank you for making sacrifices in your lives so that I could pursue my dreams. I love you both.
