Volume 114 | Issue 1 Article 10

September 2011

An Illusory Expectation of Privacy: The ECPA Is Insufficient to Provide Meaningful Protection for Advanced Communication Tools

Sara E. Brown
West Virginia University College of Law

AN ILLUSORY EXPECTATION OF PRIVACY: THE ECPA IS INSUFFICIENT TO PROVIDE MEANINGFUL PROTECTION FOR ADVANCED COMMUNICATION TOOLS

I. INTRODUCTION

We are not surprised to find the government uses social networking sites to investigate crimes[1]—or are we? An American couple was arrested for eating an endangered species of iguana in the Bahamas in February 2009 after

[1] Jennifer Lynch, *Government Finds Uses for Social Networking Sites Beyond Investigations*, ELECTRONIC FRONTIER FOUNDATION (Aug. 10, 2010), http://www.eff.org/deeplinks/2010/08/government-finds-uses-social-networking-sites.

posting pictures on Facebook.[2] In September 2009, a woman was arrested for violating a protective order with a Facebook "poke."[3] During the same month, police executed a warrant on the home of a self-proclaimed anarchist for coordinating communications among protesters via Twitter at the Group of 20 summit in Pittsburgh.[4] In July 2010, police arrested a nineteen-year-old mother after she posted a photo of her infant son "smoking" from a bong.[5] In February 2010, a nineteen-year-old male got fifteen years in prison when he used Facebook to blackmail more than thirty male classmates into having sex with him.[6] These arrests raise a series of questions: Do individuals really understand their rights to privacy when they post information on social networks? Further, what are users' rights, and how does the government collect and utilize the information found on social networks?[7]

Although no one may be surprised by government agencies utilizing the plethora of information individuals make publicly available on social networks, individuals likely would be alarmed to learn that law enforcement agencies recover "'private' content only shared among those chosen by the page owner."[8] Hundreds of millions of users are logging on to social networks[9] and providing personal information under the guise that such information is only viewable by the people to whom they give access.

Privacy law has evolved as new forms of communications presented risks of intrusion. Beginning with no privacy in telephone communications,

---

2 Catharine Smith & Bianca Bosker, *Arrested Over Facebook: 19 Posts That Got Suspects Snagged*, HUFFINGTON POST (Aug. 16, 2010), http://www.huffingtonpost.com/2010/08/16/arrested-over-facebook-po_n_683160.html#s127052&title=undefinedcouple_arrested_after; *see also* Adam Monacelli, *Barbecuing and Eating Endangered Iguanas Will Get You Arrested*, COURIER POST ONLINE (Feb. 17, 2009), http://blogs.courierpostonline.com/fishhead/2009/02/17/barbecuing-and-eating-endangered-iguanas-will-get-you-arrested/.

3 Eric Miller, *Charges Against Alleged Facebook 'Poker' to be Considered by Grand Jury*, THE TENNESSEAN (Nov. 3, 2009, 4:16 PM), http://www.tennessean.com/article/20091103/HENDERSONVILLE01/112170001/2139/Charges+against+alleged+Facebook+%E2%80%98poker%E2%80%99+to+be+considered+by+grand+jury.

4 Paula Reed Ward, *Men Arrested for G-20 Twittering Says it's Free Speech*, PITTSBURGH POST-GAZETTE (Oct. 5, 2009), *available at* http://www.post-gazette.com/pg/09278/1003126-53.stm.

5 *Mom Arrested After Posting Baby with Bong on Facebook*, FOX 8 NEWS (Aug. 17, 2010, 3:01 AM), http://www.fox8.com/news/ktla-bong-baby-mother,0,6230425.story.

6 Dinesh Ramde, *Anthony Stancl, 19, Gets 15 Years for Facebook Sex Scam*, HUFFINGTON POST (Feb. 24, 2010, 7:11 PM), http://www.huffingtonpost.com/2010/02/25/anthony-stancl-19-gets-15_n_476214.html.

7 Lynch, *supra* note 1.

8 DRUG ENFORCEMENT ADMIN., *Communications of People that Share* Interests, U.S. DEP'T OF JUSTICE (May 14, 2010), *available at* http://www.eff.org/files/20100514_dea_socialnetworking.pdf.

9 Facebook.com reports 750 million active users. *See infra* Part III.A.

privacy law shifted to a reasonable expectation of privacy under *Katz v. United States*,[10] then to no expectation where a communication is disclosed to a third party,[11] and finally to a balance of privacy needs with the needs of law enforcement involving electronic communications divulged to a service provider during the course of transmission under the Electronic Communications Privacy Act of 1986[12] ("ECPA"). This Note discusses the lack of protection available to communications via social networks under the ECPA, using Facebook as the prime example of social network communications based on its ranking as the most popular social network site.[13]

Currently, the ECPA lacks clarity as presently applied to advanced online communication tools because Congress enacted the ECPA in 1986 at a time when individuals used dial-up modems to connect to the Internet, downloaded e-mail, and before services such as Gmail, Facebook, and Twitter developed. Because advanced communication tools were beyond congressional foresight, the careful balance of needs Congress sought under the ECPA no longer meets the needs of individuals, law enforcement, or the judicial system.

This Note argues that Congress must take legislative action and update the ECPA to allow for an expansion of privacy protection over advanced communication technology tools such as user-controlled social network activity because users' expectations meet the standards required both by the Supreme Court and Congress. The Act no longer meets the intended balance of needs between individuals and law enforcement. The ECPA is unclear and inconsistently applied by courts in an area of the law that requires uniformity. Communication tools have advanced beyond the ECPA capabilities rendering the Act's distinctions futile and its protection insufficient. Additionally, this Note argues that Congress has historically intervened when the common law struggled to keep up with the advancement of communication tools and that technological progress since 1986 requires nothing short of revising the ECPA to include such tools under its umbrella of protection.

II. BACKGROUND: THE EVOLUTION OF PRIVACY LAW

The United States Constitution does not provide an explicit guarantee of a right to privacy.[14] The Supreme Court interprets many amendments, particularly the Fourth Amendment, as providing protection for a number of specific types of individual privacy against government intrusion.[15]

---

10 389 U.S. 347, 351 (1967).

11 United States v. Miller, 425 U.S. 435, 443 (1976).

12 Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2006).

13 Andy Kazeniac, *Social Networks: Facebook Takes over Top Spot, Twitter Climbs*, COMPETEPULSE (Feb. 9, 2009, 2:01 PM), http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/.

14 FRED H. CATE, PRIVACY IN THE INFORMATION AGE 52 (1997).

15 *Id.*

Most of the Supreme Court's privacy jurisprudence centers on the Fourth Amendment of the United States Constitution,[16] which protects all persons from "unreasonable searches and seizures."[17] Specifically, the Fourth Amendment states that all persons shall "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," unless, on the basis of probable cause, a warrant is issued with "particularity describing the place to be searched, and the persons or things to be seized."[18]

Notably, Justice Louis Brandeis explained the right to privacy within the context of the Fourth Amendment in a famous dissenting opinion:

> The protection guaranteed by the [a]mendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the [g]overnment, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the [g]overnment upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[19]

Because the Constitution does not explicitly reference privacy, the Supreme Court's interpretation of individual privacy often is confusing, and the scope of protection is narrow.[20] Privacy is defined in a number of ways such as an expression of one's personhood; "the right of [an] individual to define his or her essence as a human being"; "autonomy . . . of the individual to engage in his or her own thoughts, actions, and decisions"; or a citizen's ability to regulate information about herself.[21]

The Supreme Court typically addresses issues of privacy on a case-by-case basis.[22] New technologies create new privacy problems, and the Court his-

---

16 *Id.* at 57.

17 U.S. CONST. amend. IV; CATE, *supra* note 14, at 57.

18 U.S. CONST. amend. IV; CATE, *supra* note 14, at 57.

19 Olmstead v. United States, 277 U.S. 438, 478–79 (1928).

20 U.S. CONST. amend. IV; CATE, *supra* note 14, at 52.

21 CATE, *supra* note 14, at 19.

22 *See id.* at 52.

torically has responded slowly to these problems.[23] The rapid spread of new information technologies into every day facets of life shed new light on privacy issues—more people are using unprotected communication tools at the risk of intrusion.[24] The issues arising from the development of online communications has not gone unnoticed, and the increased use of popular online communication tools "has spawned an astonishing array of industry and academic conferences, working groups, public interest and lobbying efforts, public surveys, and news stories."[25]

In the context of new information technologies, "privacy refers to controlling the dissemination and use of data, including information that is knowingly disclosed, as well as data that are unintentionally revealed as a by-product of the use of the information technologies themselves."[26] The Supreme Court generally finds violations of the constitutional right to privacy in the context of police searches or seizures of records without a warrant or without meeting an exception to the warrant requirement.[27] The Court typically reserves application of Fourth Amendment privacy rights to investigations and prosecutions of criminal activity; further, protection "does not extend to information controlled by a third party."[28] Put another way, if something must be seen by a third party, "it cannot really be private."[29]

A. The Katz *Standard: A Reasonable Expectation of Privacy*

Privacy is not determined by location or the method of intrusion, but rather the individual's intent to preserve his privacy, even in an area accessible by the public.[30] Because privacy is defined by a person's intent, an intrusion is not characterized by a physical trespass, but rather by a person's expectation.[31]

---

23 *See, e.g.*, Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1105 (codified as amended at 47 U.S.C. §§ 151–609 (2006)); Katz v. United States, 389 U.S. 347 (1967) (making the interception of any wire communications illegal and establishing federal regulations of telegraph, telephone, and radio communications); *Olmstead*, 277 U.S. 438 (holding that the Fourth Amendment does not forbid a non-physical intrusion); *Transmission*, ENCYCLOPEDIA BRITANNICA, http://www.britannica.com/EBchecked/topic/585993/telephone/279924/Transmission (last updated Aug. 10, 2010) (noting that Alexander Graham Bell first completed a transmission over the telephone in 1876).

24 CATE, *supra* note 14, at 1.

25 *Id.* at 1.

26 *Id.* at 13.

27 *Id.* at 98–99.

28 *Id.* at 99.

29 HARRY HENDERSON, PRIVACY IN THE INFORMATION AGE 15 (rev. ed. 2006).

30 Katz v. United States, 389 U.S. 347, 351 (1967).

31 *Id.*

The Supreme Court reached its decision to determine privacy on the basis of a person's expectation in *Katz v. United States*.[32] In a majority decision, the Supreme Court held that a warrantless wire tap in a telephone booth was unconstitutional.[33] The Supreme Court reasoned that a person using a public telephone has a reasonable expectation of privacy: "One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[34]

In overturning the lower court's decision, the Court recognized the importance of the telephone, stating that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[35] Courts utilize Justice John M. Harlan's two-pronged test as laid out in his concurrence to analyze privacy issues: 1) whether an individual has a reasonable expectation of privacy, and 2) whether society is willing to recognize the expectation as reasonable.[36] The two-pronged test essentially balances the importance of an individual's right to privacy with the needs of law enforcement—is society willing to recognize the expectation as reasonable enough to forego law enforcement's need to investigate?

The Supreme Court's decision in *Katz*[37] overturned, in part, its previous decision in *Olmstead v. United States*, which held that the Fourth Amendment does not forbid a non-physical intrusion.[38] *Katz* essentially clarified the congressional intent behind the Communications Act of 1934,[39] which made it illegal for anyone to intercept any wire communications; established federal regulations of telegraph, telephone, and radio communications; and created the Federal Communications Commission to implement the regulations.[40]

B. *Privacy, Party of Two: Third Party Disclosures Eviscerate Privacy Expectations*

One caveat to the reasonable expectation of privacy is the Third Party Doctrine[41] laid out in *United States v. Miller*.[42] The Third Party Doctrine limits

---

32 *Id.*

33 *Id.* at 353.

34 *Id.* at 352.

35 *Id.*

36 *Id.* at 361 (Harlan, J., concurring).

37 *Id.* at 351.

38 277 U.S. 438, 466 (1928).

39 47 U.S.C. §§ 151–609 (2006).

40 *Id.*

41 The rule established in *United States v. Miller*, 425 U.S. 435 (1976), is commonly referenced by scholars as the "Third Party Doctrine." *See generally* Orin S. Kerr, *The Case for the Third-party Doctrine*, 107 MICH. L. REV. 561 (2009); Stephen E. Henders, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011).

the scope of Fourth Amendment privacy to communications between two people.[43] In a 7–2 decision, Justice Lewis F. Powell, Jr., writing for the Court, stated that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[44]

In *Miller*, a case for tax fraud, the defendant appealed to the Supreme Court for a violation of constitutional privacy rights on the basis of a defective *subpoena duces tecum* to seize bank records.[45] The Court stated that the Fourth Amendment provides no privacy protection for 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 and the confidence placed in the third party will not be betrayed."[46] To determine whether the defendant had a legitimate expectation of privacy, the Court examined the nature of the communication and held that the documents were not confidential communications.[47] Instead, the Court stated that the documents contained "information voluntarily conveyed" to be used in a commercial transaction and exposed during the ordinary course of business.[48]

C. *A Digital Caveat to the Third Party Doctrine: Electronic Communications Privacy Act*

The ECPA essentially carves out an exception to the Third Party Doctrine for electronic communications by striking a balance between an individual's right to privacy and the needs of law enforcement to investigate.[49] Although the ECPA prohibits the interception of wire, oral, or electronic communications,[50] the Act provides for authorization of interception and disclosure of such communications, and provides procedures for interception.[51] When Congress enacted the Act in 1986, electronic communication tools had yet to become popular,[52] but Congress recognized the significance of tools such as e-mail,

---

42 *Miller*, 425 U.S. 435.

43 *Id.* at 443.

44 *Id.*

45 *Id.* at 436.

46 *Id.* at 443.

47 *Id.* at 442.

48 *Id.*

49 Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2006); S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

50 18 U.S.C. §§ 2510–2522.

51 *Id.*

52 Betsy Joyce, *The Importance of Electronic Communication: Where We've Been, Where We Are Now, and What's Coming*, PUBLIC ROADS, Jan.–Feb. 2002, at 43, *available at* http://www.fhwa.dot.gov/publications/publicroads/02janfeb/iwatch.cfm. Electronic mail and the Internet were still in early stages of development at the time Congress enacted the ECPA. *Id.* As the Internet grew in the 1990s, e-mail communication also became more popular. *Id.*

which signifies preparation for future privacy issues before individual privacy faced technological challenges.[53]

The problematic section of the ECPA affecting online privacy is the Stored Communications Act[54] ("SCA"), which creates an exception to the Third Party Doctrine established in *Miller* for third party network service provider users. The SCA governs issues of online privacy and was enacted as part of the ECPA[55] in 1986. The SCA protects the privacy rights of users and subscribers of two types of third party network service providers—electronic communication services ("ECS") and remote computing services ("RCS").[56]

III. BACKGROUND: SOCIAL NETWORKING DEFINED

Just as the courts have worked toward defining the scope of individual privacy, defining social networks is imperative to carving out a place for social media in privacy law. Definitions of social networks vary, but how a social network and the use of social networks are defined result in important legal implications. In *Doe v. Myspace*,[57] the Fifth Circuit defined social networking as "the practice of using a Web site or other interactive computer service to expand one's business or social network."[58] The court further defined social networking as an "online profile" created by and for each individual member "that serves as a medium for personal expression, and can contain such items as photographs, videos, and other information about the member that he or she chooses to share . . . . Members have complete discretion regarding the amount and type of information that is included in a personal profile."[59]

Facebook, which touts itself to be "one of the most-trafficked sites in the world,"[60] describes social networking as "a social utility that helps people communicate more efficiently with their friends, family and coworkers,"[61] with a special focus on "giving people control over their experience so they can express themselves freely while knowing that their information is being shared in the way they intend."[62] The *Doe* court vaguely suggested controlled communi-

---

53 *Id.*

54 18 U.S.C. §§ 2702–2711 (2006).

55 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.).

56 18 U.S.C. §§ 2701–2712 (2006); S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

57 528 F.3d 413 (5th Cir. 2008).

58 *Id.* at 415.

59 *Id.*

60 *Factsheet*, FACEBOOK, http://www.facebook.com/press/info.php?factsheet (last visited Sept. 14, 2011).

61 *Id.*

62 *Id.*

cation as a characteristic of social networking by discussing it in terms of discretionary disclosure.[63]

Furthermore, hundreds of millions of users depend on social networks, such as Facebook, to communicate with friends, family, and other acquaintances with similar interests. As the law stands, however, the ECPA does not provide any legitimate privacy protection from unreasonable searches or seizures for social network users.

A. How Social Networks Work

Mark Zuckerberg, Chief Executive Officer of Facebook, launched Facebook in 2004.[64] Upon its inception, Facebook primarily offered services to college students.[65] Facebook made its free services accessible to anyone with a registered e-mail address in 2006, and its popularity quickly exploded.[66] Facebook alone lauds more than 750 million active users, fifty percent of whom log on to the network daily via computer or cellular phone.[67] In just five years, Facebook left Zuckerberg's Harvard dorm room and entered the homes and pockets of hundreds of millions of users.[68]

Creating a Facebook account is simple. Prospective users visit the website and become a member in a matter of seconds by simply entering basic information—name, e-mail address, gender, and birthday—then creating a password.[69] After becoming a member, the initially entered information becomes the user's profile.[70] Users then can supplement the initial profile information by adding interests, education, and photos.[71]

Once a user creates his or her profile, she can add "friends" through a simple name or e-mail address search thereby extending her network by finding friends, family, and people with similar interests.[72] Users send a friend request and the recipient either accepts or rejects the request giving users control over

---

63 528 F.3d at 415.

64 *Executive Bios*, FACEBOOK, http://www.facebook.com/press#!/press/info.php?execbios (last visited Sept. 11, 2011).

65 *Timeline*, FACEBOOK, http://www.facebook.com/press#!/press/info.php?timeline (last visited Sept. 11, 2011).

66 *Id.*

67 *Statistics*, FACEBOOK, http://www.facebook.com/press#!/press/info.php?statistics (last visited Sept. 11, 2011).

68 *Timeline*, FACEBOOK, http://www.facebook.com/press#!/press/info.php?timeline (last visited Sept. 11, 2011).

69 *Sign Up for Facebook*, FACEBOOK, http://www.facebook.com/r.php (last visited July 9, 2011).

70 Richard M. Guo, *Stranger Danger and the Online Social Network*, 23 BERKLEY TECH. L.J. 617, 620 (2008).

71 *Id.* at 623.

72 *Id.*

who views their profiles.[73] By adding "friends," users essentially link their profiles to each other creating an online community,[74] and "[t]his linking creates a 'friendship' between any two users, and generally allows each user to access the other's profile."[75] Essentially, the more a user's profile grows the more her online community grows,[76] and, furthermore, "the more information the user supplies, the greater her ability to connect with others."[77]

Users who have access to other profiles generally have the ability to post comments on a friend's "wall" or on other items friends post like photos, video, or links to other websites.[78] In November 2010, Facebook introduced Facebook Message, which is a "unified messaging system" that allows users to send messages via the Web or mobile phone regardless of whether they are using online chat, text messages, or e-mail.[79] Facebook Message has been called a "bold move" by reviewers because Facebook is "expand[ing] from a social network into a full-fledged communications system. It could help the company chip away even more at Internet portals like Google, Yahoo, MSN and AOL, which have used e-mail as one of their main draws with consumers."[80]

Further, Facebook opened its services to third parties in May 2007 through Facebook Platforms.[81] Facebook Platforms invite third party software makers to create programs for the service and to make money on advertising alongside them.[82] The initiative stimulated the creation of hundreds of applications such as games, music, and photo sharing tools.[83] Facebook describes the process as necessary to help users "share expressive and relevant content."[84] Facebook pre-approves third party websites and applications using the Platform,[85] then provides the third parties with a user's general information at the time the user accesses them.[86]

---

73 Nathan Petrashek, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1499–1500 (Summer 2010).

74 Guo, *supra* note 70, at 620.

75 *Id.*

76 Petrashek, *supra* note 73, at 1500.

77 *Id.*

78 *Using Facebook*, FACEBOOK, http://www.facebook.com/help/?tab=browse (last visited Oct. 2, 2011).

79 Miguel Helft, *Facebook Offers New Messaging Tool*, N.Y. TIMES, Nov. 15, 2010, *available at* http://tech.mit.edu/V130/N54/long2.html.

80 *Id.*

81 *Facebook Unveils Platform for Developers of Social Applications*, FACEBOOK, http://www.facebook.com/press/releases.php?p=3102 (last visited Oct. 2, 2011).

82 Kevin Allison, *Facebook Spreads its Web Wider*, FINANCIAL TIMES, June 29, 2007, at 24.

83 *Id.*

84 *Facebook Platform Policies*, FACEBOOK, http://developers.facebook.com/policy/#principles (last visited Oct. 2, 2011).

85 *Id.*

86 *Id.* at § II.

In doing so, Facebook made user information available to another party—communications are now shared among user's friends, Facebook, and Facebook Platforms. However, most users are likely unaware of the implications most of these new applications have on their privacy[87] and "are, at best, confused about the security of their data . . . ."[88]

B. *The Privacy Policy:*[89] *User Control and Network Access*

Individuals, particularly young people, are beginning to lead their social lives online under the guise that their online conversations and communications are far more private than they are.[90] Social networks, like Facebook, allow users to actively control the information they share through privacy controls—"public," "friends," "only me," or "custom."[91] Privacy settings can be customized for contact information, user posts, gender, birthday, and other personal information.[92]

However, Facebook reserves the right to make a user's name, profile picture, and networks publicly available.[93] Such information remains under the "public" setting, which is accessible by anyone on the Internet, even those not logged onto Facebook.[94] Furthermore, information set to "public" also is accessible by "the games, applications, and websites" users and user's friends utilize.[95] Users can prevent application access by turning off all Facebook "Apps," but then "will no longer be able to use any games or other applications." [96] Facebook also notifies users in its policy that such information may be associated

---

87 *Comments of Digital Due Process*, DIGITAL DUE PROCESS 6 (June 14, 2010), http://www.digitaldueprocess.org/files/NTIA_NOI_061410.pdf (comments submitted in response to a Notice of Inquiry sent out by the United States Department of Commerce National Telecommunications and Information Administration).

88 *Id.*

89 Facebook refers to its privacy policy as a "Data Use Policy." *Facebook's Data Use Policy*, FACEBOOK, http://www.facebook.com/#!/full_data_use_policy (last visited Oct. 1, 2011). Although the author is using Facebook as a primary example of social networks, the use of "Privacy Policy" is a term used to generally refer to policies expressly regarding a user's control over information she posts to a social network.

90 JOHN PALFREY & URS GASSER, BORN DIGITAL 53–54 (2008).

91 *Id.* at 56; *see also Data Use Policy: Control Over Your Profile*, FACEBOOK, https://www.facebook.com/about/privacy/#controlprofile (last visited Oct. 2, 2011).

92 *Data Use Policy: Control Each Time You Post*, FACEBOOK, https://www.facebook.com/about/privacy/#controlprofile (last visited Oct. 2, 2011).

93 *Data Use Policy: Information We Receive and How It Is Used*, FACEBOOK, https://www.facebook.com/about/privacy/#howweuse (last visited Oct. 2, 2011).

94 *Id.*

95 *Id.*

96 *Id.*

with the user, including name and profile picture, outside of Facebook on public search engines and other sites users visit.[97]

Lastly, a user has the option to "deactivate" or "delete" her account.[98] Deactivating an account puts an "account on hold" by making the user's profile inaccessible by others, but the information is not deleted.[99] Deleting an account permanently removes all information from the network, but deleting takes a minimum of one month and up to ninety days.[100] Although Facebook's Privacy Policy makes certain information public by default, its controls are still better than most other social networks in this regard.[101]

Facebook's Privacy Policy also reserves the right to access information for a laundry list of uses such as service management, contacting the user, to supplement user profiles, friend searches, to make suggestions, and most importantly, targeted advertising.[102] Targeted advertising is referred to as a way "to measure or understand the effectiveness of ads."[103] Facebook does not share user information with advertisers; rather, advertisers choose user characteristics and Facebook accesses user information, including sensitive information set to private, to properly target advertising to users with the chosen characteristics.[104] Facebook explains that it uses the information "to provide Facebook as it exists today" and to allow the network to provide users with "innovative features and services" in the future.[105]

IV. APPLICATION OF THE ECPA LACKS CLARITY IN OUR FAST-PACED DIGITAL AGE

Because Congress enacted the ECPA long before the introduction of current electronic communication tools, the narrowly tailored distinctions for which the Act provides protection force courts to struggle to meet Congress's intended purpose in the balance of needs between individual privacy and law enforcement. The narrow distinctions laid out in the ECPA have resulted in difficulty because most current communication tools do not fit under the defined electronic communications covered by the ECPA.

---

97 *Id.*

98 *Data Use Policy: Deleting and Deactivating Your Account*, FACEBOOK, https://www.facebook.com/about/privacy/your-info#deleting (last visited Oct. 2, 2011).

99 *Id.*

100 *Id.*

101 PALFREY & GASSER, *supra* note 90, at 56.

102 *Data Use Policy: How We Use the Information We Receive*, FACEBOOK, https://www.facebook.com/about/privacy/your-info#howweuse (last visited Oct. 2, 2011).

103 *Id.*

104 *Data Use Policy: How Advertising Works*, FACEBOOK, https://www.facebook.com/about/privacy/your-info#personalizedads (last visited Oct. 2, 2011).

105 *Data Use Policy: How We Use the Information We Receive*, FACEBOOK, https://www.facebook.com/about/privacy/your-info#howweuse (last visited Oct. 2, 2011).

Courts struggle to define new communication tools and find it difficult to apply the ECPA—such difficulties have resulted in circuit splits in the ECPA application. These misapplications and circuit splits are a direct result of a narrowly defined act lacking foresight to predict communication advancements. In order to ensure uniformity in application and to supply courts with a clear workable act, Congress must intervene and amend the ECPA to establish clear distinctions and definitions applicable to advanced communication tools.

A. Legally Defining Social Networks

When individuals utilize privacy settings and limit access to their information on social networking sites, their communications should be deemed private under the ECPA. Defining a social network is of key significance in determining whether a user has an expectation of privacy in her communications or whether the communication falls under the protection of the ECPA. The *Doe* court's attempt was a good start at defining social networking,[106] but the opinion misses a key element of the online activity: social networking is a controlled communication knowingly shared in a specific manner to a specific person or a specific group of people.

The *Doe* court vaguely suggested controlled communication as a characteristic of social networking by discussing it in terms of discretionary disclosure;[107] however, the court missed an important component described by Facebook as a communication *knowingly shared the way the user intends.*[108] The user's intent is important because if the user takes advantage of the privacy tools available on social networks, the user essentially has an expectation of privacy by utilizing the available privacy controls to limit access to his or her information.

User control of privacy settings gives the illusion of privacy and *should* be protected under *Katz*. The Court in *Katz* overturned *Olmstead* and accepted the congressional intent behind the Communications Act of 1934, which moved away from the old view of privacy as a physical intrusion.[109] The new test for Fourth Amendment privacy was established, and now individuals can expect protection if they have a reasonable expectation of privacy at the time the communication is made.[110]

Users are led to believe that the details of their Facebook activity are private and likely have no intent to publish the information because "[m]ost users of Facebook treat it as a sort of online scrapbook for their lives—posting

---

106 528 F.3d 413, 420 (5th Cir. 2008).

107 *Id.* at 415.

108 *Factsheet*, FACEBOOK, http://www.facebook.com/press/info.php?factsheet (last visited Sept. 14, 2011).

109 Communications Act of 1934, 47 U.S.C. §§ 151–609 (1934).

110 *See* Katz v. United States, 389 U.S. 347, 351 (1967).

everything from basic information about themselves to photos to calendars of events they plan to attend."[111] However, by instinctively clicking "accept" to the network's Privacy Policy, a user *unknowingly* clicks away her rights because she "accepts" that the information she shares is being accessed and used for public purposes while eviscerating any reasonable expectation of privacy.

By accepting the Privacy Policy, users agree to allow Facebook to access and use information, and often to allow Facebook Platform access by using applications and playing games.[112] This third party access renders social network communications unprotected under the Third Party Doctrine established in *Miller* because communications revealed to a third party are not private "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[113]

Users, however, likely do not realize Facebook reserves such access rights to use their shared information regardless of privacy settings.[114] Evidence suggests that few users read privacy policies let alone change default settings.[115] Furthermore, "even for those who are aware of the choices, keeping track of privacy settings can be difficult . . . ."[116] Control settings effectively lead users to believe that their information is only viewable by the people they give access via personal privacy settings.

As it stands, the ECPA does not provide any protection for social networking communications contrary to congressional intent. Digital Due Process, a privacy advocates coalition, reasons that the ECPA meets none of the goals set forth by Congress prior to its enactment because "[a]s presently applied, the ECPA does not comport with user expectations, does not meet law enforcement or judicial needs for clarity, creates non-trivial costs for businesses seeking to comply with law enforcement requirements, and erects barriers to the adoption of innovating, productivity enhancing technology by American business."[117]

Specifically, individuals using social networks to communicate as an alternative to other traditional communications can expect little if any protection from the ECPA.[118] The ECPA provides only "weak protection" for information stored on social networks "[e]ven when private records, photos and other mate-

---

111 Vauhini Vara, *Facebook Gets Personal with Ad Targeting Plan*, WALL ST. J., Aug. 23, 2007, *available at* http://online.wsj.com/article/SB118783296519606151.html.

112 *See supra* Part III.B (discussing the access users grant Facebook by accepting the network's privacy policy).

113 425 U.S. 435, 443 (1976).

114 PALFREY & GASSER, *supra* note 90, at 57.

115 *Id.*

116 *Id.*

117 J. Beckwith Burr, *The Electronic Communications Privacy Act of 1986: Principles for Reform*, DIGITAL DUE PROCESS 3 (Mar. 30, 2010), http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

118 *Id.* at 16.

rials are shared only with a couple of friends . . . , allowing governmental access without a warrant."[119]

Congress intended the ECPA to be an exception for electronic communications, such as social networking activity, because although such communications are unprotected under the Third Party Doctrine, users do not intend to disclose information to another party. Although a user "accepts" a social network's Privacy Policy, she still intends for her communications to remain private when she limits access to her information because the service's privacy controls create an illusion of privacy. Whether the Privacy Policy maintains a user's privacy is irrelevant because the user herself intends the communication to be private, and the user has a reasonable expectation of privacy when she limits access through service-provided privacy controls.

Under *Miller*, disclosing a communication to a third party, even if for a limited purpose, deems that communication unprotected. However, the ECPA protects certain types of electronic communications disclosed to third parties for the limited purpose of transmission and maintenance.[120] As defined under the ECPA, transmission and maintenance do not include targeted advertising or Facebook Platforms utilized by social networks and other advanced communications like commercial e-mail.[121] Because these services depend on these practices to remain competitive and available to users, and because users do not intend to publish their communications, such disclosures should be folded into the current definition of transmission and maintenance to ensure the balance of needs among users, service providers, and law enforcement intended by Congress.

B. *Where* Warshak *Went Wrong—Why Case-by-Case Analysis Is Insufficient*

Third party access required by social networks diminishes Fourth Amendment protection under the Third Party Doctrine rendering a reasonable expectation of privacy immaterial once the information is disclosed. Because online communications such as social network activity fit the prerequisite requirements Congress intended the ECPA to protect, amending the ECPA is a more strategic and reasonable avenue to update the law to comply with advancements in online communications.

In *United States v. Warshak*,[122] however, the Sixth Circuit held that a user enjoys a reasonable expectation of privacy independent of the ECPA in the contents of e-mails "that are stored with, or sent or received through, a commercial ISP."[123] Further, the Court found portions of the SCA unconstitutional:

---

119 *Id.*

120 18 U.S.C. § 2702(a) (2006).

121 *Id.*

122 631 F.3d 266 (6th Cir. 2010).

123 *Id.* at 288 (citing Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)).

"Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[124] In holding the SCA unconstitutional, the court referred to the distinctions between an ECS and an RCS, and the 180 day time limit for electronic storage.[125] The court found support for finding a reasonable expectation of privacy in *United States v. Forrester* that suggested contents of an online communication *may* deserve Fourth Amendment protection.[126]

Warshak used the two-pronged *Katz* test[127] in finding that e-mail users have a reasonable expectation of privacy, stating first that the defendant "plainly manifested an expectation that his emails would be shielded from outside scrutiny."[128] Further, the court noted that given the "sensitive and damning"[129] contents of the e-mails, the idea that the defendant intended the communication to be public was highly unlikely because "people seldom unfurl their dirty laundry in plain view."[130] Analogizing to postal mail and the telephone, the court determined whether society was willing to recognize a reasonable expectation of privacy in e-mail, and explained that the "explosion of Internet-based communications" has replaced traditional methods of communication.[131] The court further stated that because of "the fundamental similarities between e[-]mail and traditional forms of communication, it would defy common sense to afford e[-]mails lesser Fourth Amendment protection."[132]

The court distinguished *Miller* on the basis that the possibility or risk of third party access does not extinguish an expectation of privacy, and that the communications at issue were inherently different.[133] The court stated that the e-mail communications at issue were inherently different compared to the banking records in *Miller* because e-mail contains highly confidential communications whereas banking records merely constitute business records used in the ordinary course of business.[134] Additionally, the court looked to *Katz* to determine that the "right" of access also does not affect the reasonableness of an expectation of privacy because at the time *Katz* was decided, telephone companies typically reserved a right to monitor calls for safety purposes.[135] Further, the court stated that in *Miller* the bank used information in the ordinary course of business, whe-

---

124 *Id.*

125 *Id.* at 282–83, 288.

126 512 F.3d 500, 511 (9th Cir. 2008).

127 Katz v. United States, 389 U.S. at 516 (J. Harlan, concurring).

128 *Warshak*, 631 F.3d at 284.

129 *Id.* at 284.

130 *Id.*

131 *Id.* at 286.

132 *Id.* at 285.

133 *Id.* at 287.

134 *Id.*

135 *Id.* at 286.

reas an Internet Service Provider ("ISP") acts as an intermediary in the transmission of communications, and the content of the communications is not intended for the ISP.[136]

The court's ruling in *Warshak* created a broad designation of privacy in e-mail, but neglected to take into account that Web-based e-mail services, like social networks, utilize targeted advertising, which authorizes an ISP access to the contents of communications for *use* in marketing campaigns.[137] The communications at issue in *Warshak* were stored on an ISP that had not expressed an intent to "'audit, inspect, and monitor' its subscriber's emails."[138] The court suggested that communications on ISPs with such express intent may not be private, but was unwilling to hold that a subscriber agreement would never be broad enough to diminish a reasonable expectation of privacy.[139]

Although the court took a much needed leap toward online privacy, a problem arises because it was just that—a leap. The court unnecessarily circumvented thirty years of precedent holding that an individual *does not* have a reasonable expectation of privacy in communications voluntarily turned over to a third party.[140] The court's broad stroke of constitutional interpretation likely will face strict scrutiny under the lens of established case law. The court should have taken a statutory approach by analyzing the communications under the SCA's distinctions to find that the SCA lacks clarity and is outdated in light of the advanced capabilities of communication tools, social acceptance, and importantly, the legislative intent behind the ECPA.

C. *Distinctions in the ECPA Are Futile in Our Digital World—Circuits Split on Application of the ECPA to Advanced Communication Tools*

As a forward-looking act, the ECPA no longer meets the needs of technologically savvy individuals because the language of the Act is specifically tailored to old technology. In order to understand the privacy issues facing social network users, understanding the complex concepts of the ECPA is imperative. Congress enacted the ECPA at a time when electronic communication was

---

136 *Id.* at 288.

137 *See supra* Part III.B (discussing the use of information for targeted advertising).

138 *Warshak*, 631 F.3d at 287.

139 *Id.*

140 *See* Smith v. Maryland, 442 U.S. 735 (1979) (holding that a pen register, a device used to record electronic information, such as a dialed telephone number, was not an unreasonable search because the dialed number is always available to the phone company, and thus, the user voluntarily turned the information over to third parties, assuming the risk of disclosure); United States v. Miller, 425 U.S. 435 (1976) (holding the Fourth Amendment provides no privacy protection for 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 and the confidence placed in the third party will not be betrayed").

in its early stages, and when comparatively fewer people utilized the technology than at present.[141] The ECPA since has become outdated:

> ECPA, which served us remarkably well for many years, is today unwieldy and unreliable as a law enforcement tool, immensely difficult for judges and investigators to apply, confusing, costly, and full of legal uncertainty for communications and other technology tools and service providers, and an unpredictable guardian of our country's long cherished privacy values.[142]

To put the concept of technological advancements into perspective, in 1984 Apple released the 128k Macintosh, which retailed at $2,495, with a nine-inch screen and a mouse.[143] Today, Apple's MacBook Notebook retails at $999 boasting an LED backlit widescreen display, a multi-touch track pad, a built-in camera, a built-in ten-hour battery, 2GB of memory, and a 500GB hard drive.[144] Furthermore, the Apple iPhone4 retails at $199[145] lauding 16GB capacity, 3.5-inch widescreen multi-touch display, video recording, a five megapixel still camera, and cellular and wireless access that all fit in your pocket.[146]

Twenty-five years after its inception, the ECPA no longer meets the needs of individuals who utilize these tools because the Act applies only to two distinct classifications of electronic communications that no longer apply to most communication tools used today. Specifically, the Act protects communications in an ECS, which allows for temporary storage in the course of transmission, and communications in an RCS, which are considered in permanent storage.[147]

At the time Congress enacted the Act, subscribers used electronic communication services to send and receive electronic communications, typically e-mail, and to outsource computing tasks for storage capacity on remote computing services.[148] During communication transmission in the 1980s, computers

---

141 *See infra* Part V.B.

142 Burr, *supra* note 117, at 3.

143 Jeremy Reimer, *Total Share: 30 Years of Personal Computer Market Share Figures*, ARS TECHNICA, http://arstechnica.com/old/content/2005/12/total-share.ars/4 (last visited Sept. 16, 2011).

144 *The MacBook*, APPLE, http://www.apple.com/macbook/features.html (last visited Sept. 16, 2011).

145 *Apple Store*, APPLE, http://store.apple.com/us/browse/home/shop_iphone/family/iphone (last visited Oct. 2, 2011).

146 *IPhone 4 Technical Specifications*, APPLE, http://www.apple.com/iphone/specs.html (last visited Oct. 2, 2011).

147 18 U.S.C. §§ 2510(12), (15), 2711 (2006).

148 *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 27 GEO. WASH. L. REV. 1208, 1213–14 (2004) (citing S. REP. NO. 99-541, at 3557 (1986)).

made copies of the message, and placed them in "electronic storage" pending delivery, which would often remain in the provider's storage space for several months.[149] Additionally, remote computing services received data from users for storage and processing, and also often retained the data in electronic storage for several months.[150] Both services allow for minimal third party access to private information while retaining privacy protection.[151]

The SCA defines "electronic communications" narrowly to tools available in the 1980s. According to the SCA, an "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence," and an electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[152] The Act is narrowly tailored to provide protection for the specifically defined communication in that an ECS is prohibited from divulging or giving unauthorized access to electronic communications of users while the information is in electronic storage (a third party disclosure)—temporary, intermediate storage, which is incidental to transmitting the communication or storage for the purpose of backup protection.[153] On the contrary, the SCA prohibits an RCS from divulging communications carried or maintained for the purpose of transmission or storage.[154] The Act defines an RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system."[155] An ECS is defined as a facility used for the "transmission of electronic communications, and any computer facilities used for storage of such communications."[156]

Notably, the SCA only provides Fourth Amendment privacy protection requiring a warrant for communications held in electronic storage for less than 180 days.[157] In contrast, combined with prior notice, a government entity needs only a subpoena or a court order based on "specific and articulable facts" to compel disclosure of electronic communications that are in electronic storage for more than 180 days.[158] The distinction is imperative in the analysis because privacy protection depends on whether a communication is found on an ECS in temporary storage, or an RCS for permanent storage.[159] One scholar describes the process: "when an e-mail sitting on a third-party server ages from 180 days

149 *Id.*

150 *Id.*

151 18 U.S.C. § 2703 (2006).

152 *Id.* § 2510(12), (15).

153 *Id.* §§ 2702(a)(1), 2510(17).

154 *Id.* § 2702(a)(2).

155 *Id.* § 2711(2).

156 *Id.* § 2510(14).

157 *Id.*

158 *Id.* § 2703(d).

159 *Id.*

to 181 days, a user no longer has a reasonable expectation of privacy in its contents."[160] Electronic communications compelled disclosure rules also apply to subscriber information such as name, address, and session times.[161]

Many courts addressing privacy issues in light of advanced communication tools get caught up in the futile distinctions in the ECPA between an RCS and an ECS. Because the ECPA provides privacy protection only for temporarily stored electronic communications, the distinction is important to analysis, but futile in the context of advanced communications.[162] Communications on an ECS are in temporary storage during transmission and may only be accessed with a warrant, but once the communication is delivered to the recipient, and opened, the communication is considered discarded after 180 days and is no longer protected.[163] On the contrary, electronic communications stored on an RCS are essentially in permanent storage, and may be accessed by a trial subpoena.[164]

Problems arise, however, because of the nuances of advanced communication tools that allow users to communicate in a variety of ways, quickly, while providing unlimited storage capacity. Circuits are split in deciding how to analyze these nuances under the current state of the ECPA.[165]

More than a decade ago, the Ninth Circuit recognized the ECPA as a "complex, often convoluted, area of the law."[166] Upon addressing similar issues in 2002, the Ninth Circuit stated that difficulties are

> compounded by the fact that ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication . . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.[167]

In *United States v. Weaver*,[168] the Seventh Circuit held that a court could compel an ISP to comply with a subpoena ordering disclosure of the contents of a subscriber's opened e-mails that were less than 180 days old because

---

160 Achal Ozza, *Amend ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1057 (2008).

161 18 U.S.C. § 2703(c).

162 Kerr, *supra* note 148, at 1217.

163 *Id.* at 1216 (unopened communications are on an ECA and are protected for 180 days or until the recipient opens the communication then the message is considered to be on an RCS).

164 18 U.S.C. § 2703.

165 *See* Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004); *but see* United States v. Weaver, 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009). *See also* Kerr, *supra* note 148, at 1216–17.

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

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

168 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009).

the e-mails were not in electronic storage. The court held that the ISP, Microsoft Hotmail, was both an RCS and an ECS because once the defendant opened the e-mails, he left the e-mails on the ISP in order to return to the messages at a later date.[169]

The court further reasoned that the ECPA requires communications on an ECS be stored for backup purposes in order to be protected for 180 days after opening, whereas communications opened and stored on an RCS are being stored "solely for the purpose of storage or processing services" and are not protected by the warrant provision.[170] Because the Microsoft Hotmail subscriber opened the e-mails and saved the messages to return to them on "subsequent occasions," Microsoft went from an ECS to an RCS, and was maintaining the messages "solely for the purpose of providing storage or computer processing services to such subscriber or customer."[171] As electronic communications stored on an RCS, the court held the messages were accessible by subpoena.[172]

In *Theofel v. Farey-Jones*,[173] the court held that once a subscriber opens an e-mail, any version that is on the ISP is held for backup purposes on an ECS and is protected for 180 days.

> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.[174]

The court essentially qualified e-mail, as used today, as electronic communications in temporary, intermediate storage, on an ECS. The court explained that "[w]here the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages."[175]

As distinguished from *Weaver*, the *Theofel* court held that once a message in an ECS is delivered and opened, if the message remains, it is being held

---

169 *Id.* at 772.

170 *Id.*

171 *Id.*

172 *Id.*

173 359 F.3d 1066 (9th Cir. 2004).

174 *Id.* at 1070.

175 *Id.* at 1076.

for backup purposes and the content is protected until it "expire[s] in the normal course" and a warrant is required for access.[176] Whereas *Weaver* held that the ISP shifts from an ECS to an RCS once the message is opened because the ISP is then maintaining the message solely for the purpose of storage, and is accessible by a subpoena.[177]

The split in application occurs because when Congress enacted the ECPA in 1986 the communications it intended to protect were e-mails downloaded onto a personal computer (electronic communications delivered via an ECS), and data stored on a server (an RCS).[178] Now ISPs can easily store volumes upon volumes of e-mails providing easy and efficient access such that downloading an e-mail today would be not only inefficient, but also impractical.[179] Basically, it makes more sense to leave e-mail on the ISP because the messages are then accessible from anywhere via the Internet, and can be revised, revisited, and re-sent at any time.

The question arises, however, when an e-mail is sent, received, and opened. Once opened, if the user leaves the message on the ISP in order to store it for future access, is the message stored for ECS backup purposes or is it stored solely for the purpose of storage or computer processing services on an RCS? Furthermore, where do social networks fit in this distinction? The questions and issues the ECPA application raise could be remedied easily by an amendment that merely updates the definitions of the categorical distinctions for electronic communications.

D. Crispin *Carves Out a Place for Social Networks Under the ECPA*

The Ninth Circuit is the only Circuit to address the applicability of the ECPA to social networks,[180] and is a prime example of why the ECPA is unworkable. In *Crispin v. Christian Audigier, Inc.*, the court held that "wall posts" with limited access and private messages on social networking services constituted "electronic communication services" falling under the umbrella of protection found in the ECPA.[181] *Crispin* serves as an illustrative example of a court trying to fit a square peg in a round hole in order to implement the congressional intent behind the ECPA.

The court compared "wall posts" to private electronic bulletin board systems ("BBS"), which it previously held to be protected under the ECPA, stating

---

176 *Id.*

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

178 Ozza, *supra* note 160, at 1057.

179 *Id.*

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

181 *Id.* at 989.

> [b]ecause Facebook wall postings and MySpace comments, on the one hand, and bulletin postings on a website . . . cannot be considered to be in temporary, intermediate storage, . . . the postings, once made, are stored for backup purposes . . . As a consequence, . . . Facebook and MySpace are ECS providers as respects wall postings and comments and that such communications are in electronic storage.[182]

The court further reasoned that regardless of how many other users have access to the information (i.e., an individual user's Facebook friends), the information remains in electronic storage.[183] The court stated that the number of users with access is of "no legal significance" and to make a distinction "would result in arbitrary line-drawing and likely in the anomalous result that businesses such as law firms, which may have thousands of employees who can access documents in storage, would be excluded from the statute."[184]

Additionally, the court looked to *Theofel* for support holding that the Act does not require backup purposes be to the benefit of only the recipient user.

> In this regard, the court analogizes to *Theofel,* where the Ninth Circuit interpreted the "for purposes of backup protection" language in § 2510(17)(B), and concluded that any backup purpose was sufficient, whether for the benefit of the email user or for the benefit of the ISP. Applying this logic to the RCS definition, it does not matter that the stored Facebook wall postings and MySpace comments are available to hundreds or thousands of approved users.[185]

Although *Crispin* relied on a decision within its circuit, *Theofel* has not gone without its share of criticism. In *Weaver*, the Sixth Circuit stated that *Theofel* distinguished ECS backup storage and RCS backup storage "on the assumption that users download emails from an ISP's server to their own computers" and that the "distinction between web-based e[-]mail and other e[-]mail systems made *Theofel* largely inapplicable."[186]

Additionally, scholars find *Theofel* difficult to "square with the statutory test."[187] The *Theofel* test for determining whether an e-mail is an electronic communication stored for backup purposes on an ECS or an RCS depends on

---

182 *Id.*

183 *Id.* at 990.

184 *Id.*

185 *Id.* (internal citations omitted).

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

187 Kerr, *supra* note 148, at 1217.

whether the e-mail "has expired in the normal course."[188] And according to some, the Act already has express provisions determining the "lifespan" of such electronic communications:[189]

> The difficulty is that § 2703(a) already defines such a lifespan elsewhere in explicit statutory terms; the statute provides one set of rules for contents in electronic storage held "for one hundred and eighty days or less" and provides another set of rules for contents in electronic storage held for longer than 180 days.[190]

Further, the court in *Crispin*, just like the court in *Warshak*, failed to address the issues that arise when social networks utilize targeted advertising and Facebook Platforms, which allows the service provider to access the user's information for purposes other than those necessary to providing service.[191] In relying on *Theofel*, the court neglected to consider outside third party access to information utilized for purposes not addressed in *Theofel*. *Crispin* blindly relies on the premise that the purpose of backup storage is irrelevant as set forth in *Theofel* without analyzing the outside factors affecting a user's privacy beyond what he or she limits through privacy controls.[192]

V. SOCIAL DEPENDENCY REQUIRES CONGRESSIONAL INTERVENTION

Congressional intervention is necessary to ensure privacy rights for individuals utilizing advanced communication tools. In 1986, the narrowly tailored scope of the ECPA met the needs of the stated dual purpose set forth by Congress—to protect the privacy of citizens and to address the needs of law enforcement.[193] Congress based its reasoning for intervening on a report conducted by the Office of Technology Assessment that concluded "current legal protections for electronic mail [were] . . . 'weak, ambiguous, or non-existent,' and that 'electronic mail remains legally as well as technically vulnerable to unauthorized surveillance.'"[194]

When Congress enacted the ECPA, e-mail was in its early stages while the number of e-mail users in 1986 was comparatively lower than the number of

---

188 Theofel v. Farey-Jones, 359 F.3d 1066, 1070 (9th Cir. 2004).

189 Kerr, *supra* note 148, at 1217.

190 *Id.*

191 *See supra* Part III.B.

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

193 S. REP. NO. 99-541, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3558.

194 *Id.* at 3558 (quoting Federal Government Information Technology: Electronic Surveillance and Civil Liberties (Washington, D.C.: U.S. Congress, Office of Technology Assessment, OTA-CIT-293, Oct. 1985)).

users at present.[195] To send an e-mail, a subscriber connected to the Internet via dial-up modem, and downloaded e-mail correspondence to his or her personal computer.[196] Service providers acted as temporary storage mediums and typically deemed correspondence that went unopened for six months abandoned.[197] In addition, download speed was excessively lower in 1986. In 1985, the industry standard for modems was 2400 bits per second; it would take 2.5 minutes at that speed to download the United States Constitution.[198]

Today, however, service providers such as Gmail offer more than 7500 megabytes of free storage space,[199] and Internet service providers such as Comcast offer download speeds up to 15 megabytes per second.[200] The efficiency and practicality advanced communication tools offer have created a societal dependency both for personal and economical purposes. Such technological strides in just a couple of decades since the ECPA was enacted could not have been in congressional foresight making the call to reform necessary based on historical congressional policy.

A. Congress's Historical Policy of Intervening

Based on the historical policy of Congress stepping in when technology outpaces the law, the ECPA should be amended to include advanced communication tools such as social networks. In what is dubbed the "Digital Age,"[201] new technologies have advanced expediently compared to the law, and social dependency on these tools requires congressional intervention.

The judicial system historically has addressed similar issues of technological advancements sluggishly; however, upon recognizing and addressing the issues, the Supreme Court made hasty, and sometimes, improper decisions.[202]

---

195 Ozza, *supra* note 160, at 1045.

196 *Id.*

197 *Id.* at 1072.

198 *Id.* at 1045.

199 *Gmail*, GOOGLE, https://www.gmail.com (last visited Sept. 16, 2011).

200 *Xfinity Internet from Comcast*, COMCAST, http://www.comcast.com/Corporate/Learn/HighSpeedInternet/highspeedinternet.html (last visited Sept. 16, 2011). To clarify, eight bits comprise one byte, and one megabyte is composed of one million bytes. University Information Technology Services, *What Are Bits, Bytes, and Other Units of Measure for Digital Information?*, IND. UNIV., http://kb.iu.edu/data/ackw.html (last modified Sept. 15, 2011). At 15 megabytes per second, Comcast's download speed consists of 120,000,000 bits per second compared to the standard in 1985. *Id.*

201 *See generally* PALFREY & GASSER, *supra* note 90.

202 See *Olmstead v. United States*, where the Supreme Court initially held an individual has no expectation of privacy in communications over the telephone. 277 U.S. 438 (1928). In 1934, Congress enacted the Communications Act of 1934, which stated the contrary. 47 U.S.C. §§ 151–609 (1934). Further, the Court revisited the same privacy issue in *Katz v. United States*, holding an individual does enjoy an expectation of privacy in telephone communications. 389 U.S. 347 (1967).

The Supreme Court addresses issues of privacy on a case-by-case basis, making the judicial system incapable of addressing privacy problems involving technological advancements until issues arise, and even then the Court is constrained by the specific facts of each case.[203] In the past when technology developed too quickly for the Court to keep up, Congress typically established a statutory framework reflective of societal needs.[204]

Congressional intervention is necessary because typically when communication tools advance, risks of privacy intrusion develop almost simultaneously, creating exigent circumstances for protection.[205] For example, wire tapping developed practically contemporaneously with the telephone, and presented high risks of intrusion to personal privacy as the telephone became integrated into everyday life.[206]

Olmstead v. United States is a prime example of the Supreme Court adopting a narrow interpretation of privacy in the context of new technology on the basis of specific facts.[207] The Court affirmed a conviction based on evidence "obtained by intercepting messages on the telephone . . ."[208] by differentiating between telephone calls and writing correspondence. The Court deemed such interceptions constitutional because no physical trespass took place.[209]

In his famous dissenting opinion, Justice Louis Brandeis recognized a broader scope of constitutional protection afforded to telephone conversations.[210] Justice Brandeis warned against the limited scope adopted by the majority, stating that

> [w]ays may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.[211]

Congress recognized the issues Justice Brandeis foreshadowed and in 1934, just six years after the *Olmstead* decision, Congress enacted the Commu-

---

203 CATE, *supra* note 14, at 52.

204 *See* Communications Act of 1934, 47 U.S.C. §§ 151–609 (2006); Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 197, 21225 (1968) (codified as amended at 18 U.S.C. §§ 2510–2522 (2000)); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2006).

205 CATE, *supra* note 14, at 52.

206 *Id.*

207 277 U.S. 438.

208 *Id.* at 456.

209 *Id.*

210 *Id.* at 478.

211 *Id.* at 571.

nications Act.[212] The Communications Act was the first act of Congress to require a warrant for phone conversations, contrary to the ruling in *Olmstead*.[213] Specifically, the Act prohibited unauthorized publication or use of communications by common carriers stating that "no person shall intercept . . . divulge, or publish" such communications.[214] Further, the Act required common carriers to establish policies and procedures for authorizing interception of communications or access to call-identifying communication, and for preventing unauthorized interception or access.[215] The shift in policy came as the telephone became more popular and ingrained in everyday life,[216] but interpretation of the Act was controversial.[217] Government agents found loopholes and argued ambiguities.[218] Further, the Attorney General's office assured government agencies it would not prosecute violations of the Act.[219] Arguably, the Act did very little to restrict wiretapping.[220]

Nearly forty years after *Olmstead* and more than thirty years after the Communications Act of 1934, the Supreme Court finally reached a majority decision in *Katz v. United States*,[221] holding a warrantless wire tap in a telephone booth unconstitutional on the basis of an individual's reasonable expectation of privacy and society's willingness to accept such an expectation. The Supreme Court adopted the "reasonable expectation of privacy" test in *Katz* on the basis that privacy is not determined by location or method but rather the person's intent.[222] The Court further stated that the importance of innovations, such as the telephone, called for a broader interpretation of the Constitution and Fourth Amendment privacy.[223]

---

212 Communications Act of 1934, Pub. L. No. 73–416, 48 Stat. 1105 (codified as amended at 47 U.S.C. §§ 151–609 (2006)).

213 *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Judiciary Comm.*, 111th Cong. (2010) (statement of James Dempsey, Vice President for Public Policy, Center for Democracy and Technology).

214 47 U.S.C. § 605 (1996).

215 *Id.*

216 *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Judiciary Comm.*, 111th Cong. (2010) (statement of James Dempsey, Vice President for Public Policy, Center for Democracy and Technology).

217 *See* Nardone v. United States, 302 U.S. 379 (1937).

218 *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 592 (2011).

219 *Id.*

220 *Id.*

221 389 U.S. 347 (1967).

222 *Id.*

223 *Id.* at 352.

Just one year after *Katz*, Congress enacted the Federal Wiretap Act,[224] which furthered its policy of striking a balance between the privacy needs of individuals with the needs of law enforcement. The Act prohibited willful interception of wire or oral communications, and authorized government officials to seek judicial approval to conduct wiretapping investigations.[225] Congress enacted the Federal Wiretap Act years before the cusp of electronic communications—Ray Tomlinson introduced electronic mail sent via the Internet in 1971 while the Act was introduced in 1968.[226] Further, the Court established the Third Party Doctrine in *Miller* in 1976, just five years after the introduction of e-mail.[227] During this time and for several years following the decision, "e-mail remained mostly private, [and was] used only by computer scientists, the military, and then colleges and universities."[228] The general public did not truly realize the significance of Tomlinson's invention until the 1990s when the Internet became more accessible to more users.[229]

Once again, Congress responded to the disparities in applying the Federal Wiretap Act and the Third Party Doctrine to advanced electronic communications by creating the ECPA.[230] When Congress enacted the ECPA, it had the same two goals: to protect the privacy of citizens and to address the needs of law enforcement.[231] Congress stated its purpose on the basis that the Framers of the Constitution could not have foreseen such "dramatic changes" in methods of intrusions:

> When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses, papers, and effects" protected by the [F]ourth [A]mendment. During the intervening 200 years, development of new methods of communication and devices for surveillance

---

224 Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001,* 94 LAW LIBR. J. 601, 602 (2002); Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 197, 212–25 (1968) (codified as amended at 18 U.S.C. §§ 2510–2522 (2000)).

225 *Id.*

226 Joyce, *supra* note 52, at 43. Congress enacted the Federal Wiretap Act as part of the Omnibus Crime Control and Safe Streets Act of 1968. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 197, 212–25 (codified as amended at 18 U.S.C. §§ 2510–2522).

227 *Id. See generally* Miller v. United States, 425 U.S. 435 (1976).

228 Joyce, *supra* note 52, at 43.

229 *Id.*

230 *Id.*

231 S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

has expanded dramatically the opportunity for such intrusions.[232]

Congress, quoting Justice Brandeis's famous dissenting opinion in *Olmstead*, accepted a broad interpretation of the Constitution stating that existing law was "hopelessly out of date,"[233] and that "[i]t has not kept pace with the development of communications and computer technology. Nor has it kept pace with changes in the structure of the telecommunications industry."[234]

B. *Outdated and Outpaced: Expediency of Technological Advancements and Popularity Require Reform of the ECPA*

In just thirty years, the ECPA is similarly "hopelessly out of date." Technology has made sweeping advancements since 1986, and the introduction of social networking sites and other advanced communications could not have been in *congressional* foresight at the time the ECPA was enacted.[235] Advancements in technology since have resulted in an increase in individual usage. According to the United States Census Bureau, only 8.2 percent of households had a personal computer in 1984 compared to 61.8 percent in 2003.[236] Furthermore, only 18 percent of households maintained Internet access in 1997 compared to 54.7 percent in 2007.[237]

Digital Due Process, a privacy advocates coalition, reasons that the ECPA meets none of the goals set forth by Congress prior to its enactment because "[a]s presently applied, ECPA does not comport with user expectations, does not meet law enforcement or judicial needs for clarity, creates non-trivial costs for businesses seeking to comply with law enforcement requirements, and erects barriers to the adoption of innovating, productivity enhancing technology by American business."[238]

With the ECPA, Congress recognized the need for an exception to the Third Party Doctrine for electronic communications at a time when electronic communications had not fully developed—e-mail was in its beginning stages, and access to personal computers and the Internet was limited. Just as the tele-

---

232 *Id.* at 3555.

233 *Id.* at 3556.

234 *Id.*

235 *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Judiciary Comm.*, 111th Cong. (2010) (statement of James Dempsey, Vice President for Public Policy, Center for Democracy and Technology).

236 Jennifer Cheeseman Day, Alex Janus & Jessica Davis, *Households With a Computer and Internet Access: 1984 to 2003*, U.S. Census Bureau (Oct. 2005), *available at* http://www.census.gov/prod/2005pubs/p23-208.pdf. Respondents have not been asked any questions about computer access or ownership since 2003. *Id.*

237 *Id.*

238 Burr, *supra* note 117, at 3.

phone and e-mail play integral roles in facets of everyday life, social networking is fast approaching the same essential communication role for millions of individuals.

As new ways of collecting, analyzing, and integrating data develop, the economy is becoming more and more dependent on massive exchanges of information, such as targeted advertising.[239] Computer databases have grown exceptionally since the beginning of the 1960s, which in turn "increased the threat to privacy by creating large amounts of information about the details of peoples' lives while providing little control over how this information might be used."[240]

The increase in the number of users and the multifaceted communicative utilities of social networking makes the activity worthy of the ECPA privacy protection. Individuals are leading their social lives online, and the demographic is shifting from young people to people of all ages.[241] For example, of Facebook's touted 750 million users, thirty-seven percent of those users are within the thirty-five to fifty-five age range.[242] The increase in Facebook popularity among all ages makes privacy issues all the more important because very few people are thinking ahead to realize the consequences of the information they leave behind.[243] Congressional intervention is warranted because "[a]t no time in history has information . . . been more freely and publicly accessible to so many others."[244]

Communication via social networks is quickly taking an integral role in personal and business communication. Facebook alone is growing at an exponential rate with more than 750 million users.[245] With Facebook's Private Messages, users can communicate with other users from a personal computer or a cell phone regardless of whether they are using instant messaging, e-mail, or private messages.[246] Although Facebook allows for access beyond practical service management or usage, the marketing genius behind targeted Facebook ads makes social networking an imperative tool for business owners.[247] Targeted advertising directs marketing efforts toward the most applicable groups of people, efficiently resulting in more successful advertising campaigns.[248] And

---

239 HENDERSON, *supra* note 29, at 15.

240 *Id.*

241 Matthew Ingram, *Facebook vs. Twitter: An InfoGraphic*, GIGAOM (Dec. 20, 2010, 7:14 AM), http://gigaom.com/2010/12/20/facebook-vs-twitter-an-infographic/.

242 *Id.*

243 PALFREY & GASSER, *supra* note 90, at 53–54.

244 *Id.* at 54.

245 *Facebook, Inc.*, N.Y. TIMES, http://topics.nytimes.com/top/news/business/companies/facebook_inc/index.html (last updated Aug. 31, 2011).

246 *Id.*

247 Vara, *supra* note 111; *see generally* CATE, *supra* note 14, at 14–15.

248 Vara, *supra* note 111; *see generally* CATE, *supra* note 14, at 14–15.

social networks are not the only online communication companies utilizing targeted advertising; commercial e-mail servers also are taking advantage of the strategy.[249] Furthermore, targeted advertising allows these companies to maintain the service at no cost to its users.[250]

Additionally, social networks offer a number of personal benefits as well such as encouraging self-expression and socialization, providing the ability to stay connected with friends and family who are separated by geographical distance, and the ability to meet new people with similar interests.[251]

> The answer is that people have social reasons to participate on social network sites, and these social motivations explain both why users value Facebook notwithstanding its well-known privacy risks and why they systematically underestimate those risks. Facebook provides users with a forum in which they can craft social identities, forge reciprocal relationships, and accumulate social capital. These are important, even primal, human desires, whose immediacy can trigger systematic biases in the mechanisms that people use to evaluate privacy risks.[252]

Increased popularity and dependency on social networks, and the invaluable benefits derived from the use of social networks makes the call to reform all the more notable.

VI. CONCLUSION

At a minimum, Congress must amend the ECPA to include social network communications by users with strict privacy settings on the basis that social networks perform a vital role in everyday life comparable to the telephone and e-mail. When Congress enacted the ECPA, it accepted a broader interpretation of the Constitution on the basis that the law at the time was outdated, and had not kept pace with current technology. The ECPA as it currently stands does not protect most personal e-mail let alone social network communications, leaving private communications, which are increasingly made via the Internet, at risk to unreasonable intrusions.

Under *Katz*, social network users have a reasonable expectation of privacy, but that expectation is diminished by the provider's third party access and utilization of user information. The ECPA distinctions are becoming increasing-

---

249 *Privacy Policy for Google Ads and the Google Display Network*, GOOGLE, http://www.google.com/privacy/ads/privacy-policy.html (last visited Oct. 2, 2011).

250 Vara, *supra* note 111.

251 Petrashek, *supra* note 73, at 1519–20.

252 James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1151 (2009).

ly more difficult to apply to advanced communication tools such as social networks, and these changes require revision of the ECPA. Case-by-case application of the ECPA to advanced communication tools creates disparity in the law in an age when communication tools are advancing beyond the ECPA capabilities at an exponential rate.

Congress historically has intervened when communication tools advance, become integrated into everyday life, and outpace the common law. Society's dependency both economically and personally requires expansion of the ECPA to ensure national uniformity that Congress historically has provided. Leaving these decisions to judicial discretion has created and will continue to create disparity in the law on a case-by-case basis.

Sara E. Brown[*]

[*] Executive Notes Editor, Volume 114 of the *West Virginia Law Review*; J.D. Candidate, West Virginia University College of Law, 2012; Bachelor of Science in Communications, Ohio University, 2007. The author would like to thank Professor William Rhee for his insight, Michelle Green for her guidance, her colleagues on the *West Virginia Law Review*, and her friends and family for their patience and support.