Technical Difficulties: Protecting Privacy Rights in the Digital Age

Edward P. Sisk*

Whether we know it or not, our digital privacy rights are swiftly eroding. We live in a highly computerized society, where a majority of our meaningful conduct is chronicled through the usage of high-tech services or devices. Our fixation with technological conveniences has come at the expense of our digital privacy rights, and technology has outpaced the law. Many of the laws protecting our privacy rights in the digital age are archaic, confusing or completely non-existent, and as technology continues to grow, so too does the need for stronger privacy rights. Many individuals have sought to strengthen these attenuated rights, but judicial and legislative intervention has been lethargic at best. Although certain fixes to these problems may exist, many are too complex or unrealistic, while others fail to go far enough. Meanwhile, we continue to divulge vast amounts of highly personal information in the digital realm as naively as possible, enjoying almost no security in the privacy of that information.

I. INTRODUCTION

Technology is an inextricable feature of our daily lives, instantly providing an unprecedented amount of access to information. High tech amenities have become so embedded within our society that it is difficult to imagine life without them. We live in the digital age where functioning properly is nearly impossible without regularly utilizing some form of technology. People's unyielding dependence on the Internet, cell phones, cloud-based services, and GPS has the unfortunate consequence of divulging vast amounts of personal data to third parties.[1]

---

* Candidate for Juris Doctor, New England Law | Boston (2016); B.A., Political Science at the University of Massachusetts-Amherst (2011). First and foremost, I would like to thank my older brother Billy, for his immeasurably significant revisions. Without his help much of this paper may have been lost in translation and still contain my hand drawn depictions of the law. I would also like to thank my parents, William and Regina, along with my sister, Sadie, for their unconditional love, support, and undeniable willingness to sacrifice so much on my behalf; my dear friend Ryan Balise for all of his encouragement and advice; and the entire New England Journal on Criminal and Civil Confinement staff for their diligent efforts.

[1] David Gray et al., *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 747 (2013).

Yet with all of this information casually dispersed in massive quantities, the laws protecting such information have struggled to adapt.[2] Although many people believe that the information they transmit online is private, that information is not especially well protected by law.[3] The laws currently protecting electronic privacy are anything but adequate.[4] Such laws have not been substantially updated since their creation nearly thirty years ago.[5] Technology is racing forward at a torrid pace, but our electronic privacy rights have been left behind in a cloud of dust.[6] Many legal scholars, politicians, and privacy advocates are deeply entrenched in an uphill battle, fighting to renovate these rights through massive legislative reform.[7]

This Note discusses the issues facing the persistent legislative efforts to redefine privacy rights in the digital age and why these efforts have consistently fallen short. A massive reconstruction of the Electronic Communications Privacy Act (ECPA) is burdensome and unrealistic, but a refined and narrowed approach may be a more expeditious and effective route in amending the ECPA. Part II of this Note consists of background information concerning society's current technological dependence, our rampant obsession with social media and the Internet in relation to our privacy rights, as well as the basic laws and legal theories governing electronic privacy. Part III provides an in-depth look inside the ECPA, including its creation and intended purpose, and the various inadequacies resulting from its lack of modernity. Part IV discusses alternative solutions to strengthening our electronic privacy rights, as well as critiques to those strategies. Part V concludes this Note.

II. BACKGROUND: SOCIAL MEDIA V. PRIVACY

A. Social Media, the Internet, and Society

Communication changes as society evolves, and the digital age has dramatically reshaped the societal landscape we live in.[8] Gone are the days where the dominant forms of communication are accomplished in person, as many people

---

[2] Press Release, Patrick Leahy, Chairman, Leahy, Lee Introduce Legislation to Update Electronic Communications Privacy Act (Mar. 19, 2013), http://www.leahy.senate.gov/press/leahy-lee-introduce-legislation-to-update-electronic-communications-privacy-act.

[3] *See About the Issue*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Mar. 13, 2015).

[4] Leahy, *supra* note 2.

[5] *Electronic Communications Privacy Act (ECPA)*, EPIC, https://epic.org/privacy/ecpa/ (last visited Feb. 9, 2015).

[6] *Id.*

[7] *See generally* Mark Daniel Langer, Note, *Rebuilding Bridges: Addressing the Problems of Historic Cell Site Location Information*, 29 BERKELEY TECH. L.J. 955 (2014) (describing the growing collection of parties concerned with amending digital privacy laws legislatively).

[8] Commonwealth v. Augustine, 4 N.E.3d 846, 859 (Mass. 2014).

have opted to connect with others via satellite or high speed data connection.[9] An online realm exists where millions are conversing, networking, and logging everything from the most ordinary and mundane aspects of their lives to the most private and intimate ones.[10] Most of this communication is conducted through the usage of social media websites, "collective[s] of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration."[11]

For most Americans, access to computers and high-speed Internet connections is of the utmost importance. We use computers and the Internet to complete schoolwork, locate jobs, entertain ourselves, find relationships, and access healthcare information, to name a few.[12] As of December 2012, there were more than 326 million wireless cellphone subscriber connections in the United States alone.[13] In 2013, 83.8% of U.S. households reported computer ownership, with 78.5% of all households having a desktop or laptop computer and 63.6% having a handheld computer.[14] Moreover, "[a]s of January 2014, 74% of online adults use social networking sites."[15] Of those online adults, 71% use Facebook, 23% use Twitter, 26% use Instagram, 28% use Pinterest, and 28% use LinkedIn.[16]

Facebook, generally regarded as the first and most influential social media website, had 890 million daily users on average and 1.39 billion monthly active users as of December 2014.[17] Statistics from the Neilsen Group have revealed that "Internet users within the United States spend more time on Facebook than on any other website."[18] Not only does Facebook allow us to stay in touch with friends, but it also provides access to business endeavors in the form of corporate Facebook

---

9 Chandra Johnson, *Face Time vs. Screen Time: The Technological Impact on Communication*, DESERET NEWS NAT'L (Aug. 29, 2014), http://national.deseretnews.com/article/2235/face-time-vs-screen-time-the-technological-impact-on-communication.html.

10 Ken Strutin, *Social Media and the Vanishing Points of Ethical and Constitutional Boundaries*, 31 PACE L. REV. 228, 229 (2011).

11 *Definition: social media*, WHATIS, http://whatis.techtarget.com/definition/social-media (last visited Feb. 12, 2015).

12 THOM FILE & CAMILLE RYAN, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2013, 2-3 (2013), http://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf.

13 United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) (noting that, as of June 2011, "there were more than 322 million wireless devices in use in the United States"); *Wireless Quick Facts*, CTIA, http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts (last visited Mar. 3, 2015) (reporting that, as of December 2012, there were more than 326 million wireless subscriber connections in the United States).

14 FILE & RYAN, *supra* note 12, at 2.

15 *Social Networking Fact Sheet*, PEW RES. CTR., http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/ (last visited Feb. 10, 2015).

16 *Id.*

17 FACEBOOK NEWSROOM, http://newsroom.fb.com/company-info/ (last visited Feb. 10, 2015).

18 WHATIS, *supra* note 11.

pages.[19] If an individual likes a certain company, they can check out that company's Facebook page, "like" it, and subsequently follow and receive updates about the company.[20] Companies and businesses have understood the marketing power of social media for quite some time now, and have gone to great lengths to ensure they are properly harnessing that power.[21] One of those innovative strategies is known as "behavioral targeting."[22]

B. Behavioral Targeting

Behavioral targeting is an online advertising technique designed to deliver specific, targeted advertisements to consumers by collecting information about their browsing behaviors.[23] Companies that conduct behavioral targeting, known as advertising networks, can predict Internet users' interests by using certain sophisticated technology that tracks and gathers data about the users' online activity.[24] This in turn creates a user persona or profile that can be used to segment Internet users into certain groups.[25] The resulting targeted ads are approximately twice as effective as other forms of online advertisements, which make them far more valuable.[26] Online content providers can then fund their entire operations with revenues from selling online advertising space, making it possible for websites to essentially offer online content for free.[27]

Behavioral targeting has become increasingly prevalent amongst providers of online content.[28] Under current law, ad networks enjoy unlimited leeway to use the information they collect for whatever purposes they desire.[29] Facebook developed

---

19 *Facebook for Business: Marketing on Facebook*, FACEBOOK, https://www.facebook.com/business (last visited Mar. 29, 2015).

20 FACEBOOK NEWSROOM, *supra* note 17.

21 Ilya Pozin, *20 Companies You Should be Following on Social Media*, FORBES (Mar. 6, 2014, 11:05 AM), http://www.forbes.com/sites/ilyapozin/2014/03/06/20-companies-you-should-be-following-on-social-media/ (illustrating the need for companies to utilize social media).

22 *See generally* Elspeth A. Brotherton, *Big Brother Gets a Makeover: Behavior Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555 (2012) (describing the online marketing strategy known as "behavioral targeting").

23 *Id.* at 558.

24 *See generally* TRUEFFECT, ONLINE BEHAVIORAL ADVERTISING: POSSIBLE SELF-REGULATORY PRINCIPLES 2 (2008), http://www.ftc.gov/sites/default/files/documents/public_statements/online-behavioral-advertising-moving-discussion-forward-possible-self-regulatory-principles/p859900stmt.pdf (last visited Mar. 25, 2014) (discussing "key questions relating to behavorial advertising").

25 *Id.*

26 Brotherton, *supra* note 22, at 558.

27 *See generally* Howard Beales, *The Value of Behavioral Advertising*, NETWORK ADVERT. INITIATIVE 3, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (last visited Mar. 27, 2014) (detailing total revenue online content providers receive from selling advertising space).

28 *Id.*

29 *Id.*

a system to inspect the information users post in their profiles, including political affiliation and friend networks, in order to create a more targeted advertising system.[30] For example, if a Facebook user changed their relationship status from "in a relationship" to "single," they might go from seeing ads for engagement rings to seeing ads for dating services.[31] If an Internet user goes online and browses through an online women's magazine, the ad network can learn that she is female, within a particular age range, and interested in fashion.[32] On the surface, these appear to be relatively harmless or innocuous situations, and many people may even appreciate a more refined or precise form of advertising. Yet, one can only begin to imagine the types of issues that could arise when Internet users browse for information that is far more private or discreet.

To illustrate that point, let's assume the female user described above accessed certain articles about depression and dieting in the online women's magazine. Based upon that information, an ad network might deduce that she is depressed and wants to lose weight.[33] The ad network might then uncover her real name, e-mail address, phone number, and possibly home address if she were to sign up for the magazine's online sweepstakes.[34] Thus, if the user is reading an article about weight loss on the website, the ad network might display any number of targeted ads, ranging from workout clothes, dietary supplements, or an ad for a nearby business based on the location information she provided.[35] Even the casual consumer, with a very limited understanding of how the Fourth Amendment works, would probably consider that highly personal information to be protected from the prying and watchful eyes of the government.[36] Yet in addition to using the Internet users' information for targeted ads, ad networks routinely trade and sell information to third parties, including the government.[37] Internet users have often felt the illusion of privacy, but in reality and without targeted advertising, once you post something on the Internet you do not know where it will end up or how it will

---

30 *See* Nicole A. Ozer, *Facebook Not as Private as You Might Think*, ACLU (Aug. 28, 2007), https://www.aclunc.org/blog/facebook-not-private-you-might-think.

31 *Id.*

32 Brotherton, *supra* note 22, at 561.

33 *Id.*

34 *Id.*

35 *Id.*

36 *See generally* JOSEPH TURROW ET AL., THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION (2015) (discussing how new survey results indicate that a majority of Americans are resigned to giving up their personal data).

37 Brotherton, *supra* note 22, at 558; *see also* Press Release, Network Advert. Initiative, Study Finds Behaviorally-Targeted Ads More than Twice as Valuable, Twice as Effective as Non-Targeted Online Ads (Mar. 24, 2010), http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf (quoting Howard Beales, former Director, FTC Bureau of Consumer Protection).

be used.[38] For example, although Facebook's privacy policy indicates that it limits the availability of your information to third parties, it also states that Facebook may share information with "other companies, lawyers, agents or government agencies" in order to follow the law.[39] According to pre-Internet Supreme Court jurisprudence, the Fourth Amendment does not apply to electronic information held by a third party, like Facebook.[40]

C. The Fourth Amendment and the Third-Party Doctrine

1. The Fourth Amendment of the United States Constitution

The Fourth Amendment of the United States Constitution states that people have the right to be free from unreasonable searches and seizures.[41] The Fourth Amendment is implicated when the government violates "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[42] It is said to protect people, not places or areas, meaning that what a person could reasonably expect to preserve as private, even in an area accessible to the public, is protected from unlawful invasion without a warrant.[43] The purpose of the Fourth Amendment is to deter law enforcement from violating people's right to privacy.[44]

The Supreme Court has held that the Fourth Amendment's protections extend to areas where an individual has a reasonable expectation of privacy.[45] "Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[46] In *Katz v. United States*, Justice Harlan created a two-part test to determine when a reasonable expectation of privacy exists.[47] There is both a

---

38 Ozer, *supra* note 30.

39 *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last visited Apr. 4, 2015).

40 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that the installation and use of a pen register was not a "search" within the meaning of the Fourth Amendment, and hence no warrant was required); *see also* United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities).

41 U.S. CONST. amend. IV.

42 *Id.*

43 *See generally "Search and Seizure" and the Fourth Amendment*, FINDLAW, http://criminal.findlaw.com/criminal-rights/search-and-seizure-and-the-fourth-amendment.html (last visited Oct. 3, 2014) (describing the general circumstances in which the Fourth Amendment protections apply to individuals).

44 *Id.*

45 Katz v. United States, 389 U.S. 347, 359 (1967).

46 *Id.*

47 *Id.* at 361 (Harlan, J., concurring) (explaining that the critical point is whether the defendant's subjective expectation of privacy is one that society would recognize as objectively reasonable, justifiable, or legitimate).

subjective and objective prong to the test.[48] Justice Harlan stated that a reasonable expectation of privacy exists when it is shown "that 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.'"[49]

Justice Harlan's Fourth Amendment test seems like it should prevent the government from examining information collected by ad networks.[50] Many consumers subjectively assume and expect privacy from the government when they use the Internet, and their expectation is one that society would accept or is at least prepared to accept as reasonable.[51] Yet, even when an individual has a reasonable expectation of privacy, that expectation ceases to exist when he or she shares information, including electronic information, with a third party.[52] This exception to a reasonable expectation of privacy is known as the "Third-Party Doctrine."[53]

2. The Third-Party Doctrine: Ask and You Shall Receive

The third-party doctrine is a judicially constructed Fourth Amendment exception governing the collection of evidence from third parties in criminal investigations.[54] Essentially, an individual forfeits his or her reasonable expectation of privacy to certain types of information when they disclose that information to a third party.[55] Such individual effectively assumes the risk that the disclosure of information to a third party could wind up in the hands of a governmental entity.[56] The third-party doctrine states that once a fact is disclosed to the public, that information is no longer entitled to privacy protection.[57] The Fourth Amendment offers minimal protection to advertising network databases because information gathered for behavioral targeting was volunteered to a third party.[58] Laws preventing those networks from selling or exposing that information to the government do not exist.[59] The government does not need to have a court-ordered

---

48 *Id.*

49 *Id.*

50 Brotherton, *supra* note 22, at 573.

51 *Id.* at 573–74.

52 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that no "search" occurred within the meaning of the Fourth Amendment following the installation and use of a pen register); *see also* United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that information obtained and revealed to a third party and conveyed by him to Government authorities did not violate the Fourth Amendment).

53 Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

54 *Id.*

55 *Id.*

56 *Id.*

57 Richard M. Thompson II, CONG. RES. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 1 (2014), http://fas.org/sgp/crs/misc/R43586.pdf.

58 Brotherton, *supra* note 22, at 557–58.

59 *Id.*

warrant to obtain personal information held by Facebook or any other social media sites—it can merely ask for that information via subpoena.[60] The big question then, is what—if any—safeguards exist to protect our digital privacy?

III. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: A RELIC FROZEN IN TIME

A. Defining the ECPA

The ECPA primarily governs electronic surveillance in the United States, and was passed in 1986 in order to establish a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement.[61] Congress felt it was supporting the creation of new technologies by assuring consumers that their personal information would remain secure.[62] The ECPA includes the Wiretap Act, the Stored Communications Act, and the Pen-Register Act. Most of the ECPA's provisions date from 1986—before the public Internet, widespread mobile telephone service, cloud computing, or social networking existed.[63] The challenge of applying the ECPA's framework to advanced digital technologies has become a source of increasing frustration for courts, law enforcement agencies, service providers, and ordinary citizens.[64]

B. The ECPA's Critics and the Rationale Behind that Criticism

When the ECPA was first enacted it was viewed as a highly impressive feat.[65] Authors of the ECPA foresaw the potential issues created by rapidly developing wireless and Internet technologies and designed the statute to limit law enforcement access to electronic communications and data.[66] However, a quarter century later, the doctrine is widely viewed as archaic.[67] The statute has not undergone significant revision since it was enacted in 1986—given technology's dramatic advancement since then, the ECPA has been outpaced.[68] As a result, the

---

60 Ozer, *supra* note 30.

61 *Electronic Communications Privacy Act (ECPA)*, *supra* note 5.

62 *Id.*

63 *Id.*

64 *Id.*

65 Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 386 (2014).

66 *See generally* Jason Krause, *Prying Eyes: Unlikely Allies Are Collaborating in a Push to Require Warrants for Law Enforcement Access to Digital Communications*, AM. BAR ASS'N J. (Apr. 1, 2013, 10:10 AM), http://www.abajournal.com/magazine/article/unlikely_allies_join_in_a_push_to_require_warrants_for_access_to_digital (discussing the foresight of the ECPA's drafters and their legislative intent).

67 Kerr, *supra* note 65.

68 Krause, *supra* note 66.

ECPA's patchwork of confusing standards and inconsistent interpretation by the courts creates uncertainty for both service providers and law enforcement agencies.[69] The ECPA can no longer be applied in a clear and consistent way, and, consequently, the vast amount of personal information generated by today's digital communication services may no longer be adequately protected.[70]

Recently, a group of large and influential civil liberties organizations, Internet companies, and privacy scholars known as "The Digital Due Process Coalition" was assembled to advance the existing criticism of the ECPA and to advocate for reform.[71] The group includes nonprofit organizations such as the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation, as well as major Internet businesses, including Google, Apple, Facebook, Microsoft, and AT&T.[72]

This coalition is certainly not alone in its fight to amend the ECPA, as Senate Judiciary Committee Chairman, Patrick Leahy, and Utah Senator Mike Lee introduced bipartisan legislation in 2013 to strengthen the ECPA and better protect digital privacy rights.[73] Regarding the proposed bill, Senator Leahy professed:

> No one could have imagined just how the Internet and mobile technologies would transform how we communicate and exchange information today. . . . [P]rivacy laws written in an analog era are no longer suited for privacy threats we face in the digital world. Three decades later, we must update this law to reflect new privacy concerns and new technological realities, so that our Federal privacy laws keep pace with an American innovation and the changing mission of our law enforcement agencies.[74]

E-mail, mobile location, cloud computing, and social networking are just a few examples of the emerging technologies that the authors of the original ECPA could not possibly have foreseen.[75]

E-mail is now a ubiquitous mode of communication used by most Americans for personal or professional messages in confidence or otherwise.[76] Just as they previously saved hand-written letters and other correspondence, most Americans today save their e-mail communications indefinitely.[77] Today saving and retrieving messages is much simpler than it used to be, since e-mail software makes it virtually effortless to store, search and retrieve digital communications for little

---

69 *Id.*

70 *Id.*

71 *Who We Are*, DIGITAL DUE PROCESS, http://www.digitalddueprocess.org/index.cfm?objectid=df652ce0-2552-11df-b455000c296ba163 (last updated 2010).

72 *Id.*

73 Leahy, *supra* note 2.

74 *Id.*

75 DIGITAL DUE PROCESS, *supra* note 3.

76 *Id.*

77 *Id.*

cost.[78] For this reason, these days it is not uncommon for individuals to have many years worth of e-mail stored on the computers of service providers.[79] One notorious problem under current ECPA rules is that any e-mail left on a server more than 180 days is considered abandoned and can be accessed by law enforcement without a warrant.[80] And storage is so inexpensive nowadays that many Internet providers leave e-mail and other communications on cloud storage indefinitely.[81]

The recent e-mail probe of Central Intelligence Agency (CIA) Director David Patreaus by the Federal Bureau of Investigation (FBI) is quite illustrative of the problem.[82] What began as a harassment investigation exposed unrelated personal information about Patraeus' affair with his biographer, effectively ending his career.[83] That such sensitive information could be obtained and disseminated without a warrant by law enforcement is deeply troubling.[84]

Law enforcement's ability to collect sensitive information without a warrant is certainly not limited to e-mail.[85] The locational data for cell phones and mobile devices that supports cloud computing and other services can be accessed in real time through log files.[86] Such locational data can be used to infer a wide range of personal information, from a person's use of medical facilities to their sexual activities.[87] Location data is augmented by very precise GPS data in many devices as well.[88] Additionally, as discussed earlier, "one of the most striking developments of the past few years has been the remarkable growth of social networking."[89] Hundreds of millions of people now use social media services to share information with friends, and as an alternative platform for private communications.[90]

In the face of these developments, the ECPA does not provide protection

---

[78] *Id.*

[79] *Id.*

[80] *See generally* Rainey Reitman, *Deep Dive: Updating the Electronic Communications Privacy Act*, ELECTRONIC FRONTIER FOUND. (Dec. 6, 2012), https://www.eff.org/deeplinks/2012/12/deep-dive-updating-electronic-communications-privacy-act (explaining how the ECPA's current determination that e-mails stored for 180 days on a server are considered abandoned, thus enabling law enforcement to access such information without a warrant based on probable cause).

[81] Krause, *supra* note 66.

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] DIGITAL DUE PROCESS, *supra* note 3.

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] *Id.*

suited to the way technology is used today.[91] The ECPA has created conflicting standards and illogical distinctions, setting inconsistent rules for governmental access to e-mail and stored documents.[92] A single e-mail is subject to multiple legal standards in its lifecycle, from the moment it is being typed, to the moment its recipient opens it, and all the way to the time it is stored with the e-mail service provider.[93] To take another example, a document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but the ECPA states that the same document stored with a service provider may not be subject to the Fourth Amendment's warrant requirement.[94] The ECPA does not clearly state the standard for governmental access to location information.[95]

As a result of these shortcomings, the ECPA has been the subject of substantial judicial criticism.[96] The courts have repeatedly criticized the ECPA for being confusing and difficult to apply.[97] In 2002, the Ninth Circuit said, "Internet surveillance was a confusing and uncertain area of law."[98] When U.S. Magistrate Judge James Orenstein in the Eastern District of New York denied a government request to intercept cellphone communications without probable cause in August 2005, Judge Orenstein opined that the Department of Justice was relying on a vague and confusing law, and noted that, based on anecdotal information, "magistrate judges in other jurisdictions are being confronted with the same issue but have not yet achieved consensus on how to resolve it."[99] There was little indication of how the ECPA was being used in federal investigations prior to Judge Orenstein's opinion.[100] These requests were typically placed before a judge without opposing counsel to argue against them.[101] Because the law does not explicitly defend privacy rights in existing contexts, law enforcement often took sweeping positions about the amount of data that could be collected without a warrant.[102]

These expansive issues and criticisms have enabled privacy advocates, trade associations, think tanks, legal scholars, start-ups, and major Internet and communications companies to develop a consensus around the notion of a core set

---

91 Krause, *supra* note 66.

92 *Id.*

93 *Id.*

94 *Id.*

95 *Electronic Communications Privacy Act (ECPA)*, *supra* note 5.

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

97 Krause, *supra* note 66.

98 *See Konop*, 302 F.3d at 874.

99 In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 384 F. Supp. 2d 562, 566 (E.D.N.Y. 2005).

100 Krause, *supra* note 66.

101 *Id.*

102 *Id.*

of principles intended to simplify, clarify, and unify the ECPA standards.[103] As one commentator denotes, "the differences between the facts of physical space and the facts of the Internet require courts to identify new Fourth Amendment distinctions to maintain the function of Fourth Amendment rules in an online environment."[104]

C. Reforming the ECPA: Examining the Various Roadmaps and Strategies in Amending the ECPA

Amending the ECPA has been an unvarying desire amongst many of its critics, but given the territory, the most prudent means of doing so remains complex.[105] The ECPA update must confront a number of separate but related issues. First and foremost, a series of conflicting court rulings on accessing electronic communications in criminal investigations has substantially complicated the process.[106] The Electronic Frontier Foundation (EFF)[107] has outlined at least thirty federal opinions reaching varying conclusions solely related to government access to cellphone location information.[108] Proponents of an update argue that because different jurisdictions have different standards, law enforcement can access data in some jurisdictions that would be ruled inaccessible in others.[109]

Different appellate court rulings have slowly undermined the legal framework for online law enforcement in the last decade.[110] As previously mentioned, in 2002, the Ninth Circuit Court of Appeals noted that Internet surveillance was a confusing and uncertain area of the law.[111] In a 2010 ruling, *United States v. Warshak*, the Sixth Circuit directly challenged the validity of portions of the law, saying, "to the extent that the [Stored Communications Act, hereby SCA] purports to permit the government to obtain such e-mails warrantlessly, the SCA is unconstitutional."[112] As a result, law enforcement has inconsistently interpreted their ability to seize data and communications.[113] Google says it will not respond to requests for data without a warrant because it is headquartered in the Ninth Circuit, where the court

---

103 Kerr, *supra* note 65.

104 *See* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007 (2010).

105 Krause, *supra* note 66.

106 *Id.*

107 Founded in 1990, "[t]he Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world." *About EFF*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/about (last visited Feb. 10, 2015).

108 Krause, *supra* note 66.

109 *Id.*

110 *Id.*

111 *See Konop*, 302 F.3d at 874; Krause, *supra* note 66.

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

113 Krause, *supra* note 66.

has restricted law enforcement's access to digital records.[114] Although more and more jurisdictions have ruled against an expansive ECPA interpretation, rulings against the ECPA have sometimes relied on very different legal reasoning, and many privacy advocates agree that a legislative solution would be the best way to resolve these differences.[115]

This unclear legal landscape does not serve the government, customers, or service providers well.[116] Customers are confused about the security of their data in response to an access request from law enforcement, while companies are unable to assure their customers that subscriber data will be uniformly protected.[117] Law enforcement consistently wastes resources on litigating applicable standards, and prosecutions are in jeopardy should the courts ultimately rule on the Constitutional questions.[118] With all of this in mind, what exactly can be done?

IV. WHAT CAN BE DONE TO PROTECT OUR DIGITAL PRIVACY RIGHTS

A. Guiding Principles for ECPA Reform

The overarching goal of many privacy scholars' reform is to balance, with certainty, efficiency, and public confidence, the law enforcement interests of the government, the privacy interests of users, and interests of communication service providers.[119] Although, many of the concepts providing guidance in this area have sought to answer every particular question about the ECPA, a more focused and practical approach is better suited to handle the ECPA's current problems.[120] A handful of the most important issues continuously arising under the current law are more important to address at the moment, and probably easier to modify than a more comprehensive overhaul of the ECPA.[121]

The first practical suggestion amending the ECPA is relatively straightforward: the Government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online.[122] This principle extends privacy safeguards that the law has traditionally applied to similar non-digital letter correspondence to digital communications transmitted through systems like private

---

114 *Id.*

115 *Id.*

116 *Electronic Communications Privacy Act (ECPA)*, *supra* note 5.

117 DIGITAL DUE PROCESS, *supra* note 3.

118 *Id.*

119 *See generally* Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129 (2011) (discussing the predominant themes of reform advanced by privacy scholars today).

120 DIGITAL DUE PROCESS, *supra* note 3.

121 *Id.*

122 Krause, *supra* note 66.

e-mails, text messages, word processing documents, spreadsheets, photos, Internet search queries and private posts made on social networks.[123] This change is congruent with the bi-partisan legislation introduced by Senator Patrick Leahy discussed earlier.[124] Additionally, it is consistent with appeals court decisions holding that e-mails and SMS text messages stored by communications providers are protected by the Fourth Amendment, and is consistent with the leading legal scholarship on the issue.[125]

The next recommendation would require government to obtain a search warrant, based on probable cause before it can, prospectively or retrospectively, track the location of a cell phone or other mobile communications device.[126] This principle addresses the treatment of the growing quantity and quality of data based on the location of cell phones, laptops, and other mobile devices, which is currently the subject of conflicting court decisions.[127] It proposes the conclusion reached by a majority of the courts requiring a search warrant for real-time cell phone tracking, and would apply the same standard to access to stored location data.[128] Recently, the Supreme Judicial Court (SJC) of Massachusetts determined that in order to obtain historical cell site information from a user's mobile carrier, law enforcement officials were required to obtain a search warrant.[129] This holding is certainly consistent with this proposed change to the ECPA, and is an important building block in the fight for electronic privacy rights.

Another proposed amendment to the ECPA would require the government to display to a court that certain real-time transactional data about when and with whom an individual communicates using communications technology is relevant to an official criminal investigation.[130] In 2001, the law governing "pen registers and 'trap & trace' devices"[131] was expanded to allow monitoring of communications made over the Internet.[132] In particular, the data at issue includes information relating to whom individuals e-mail, instant message, text, and the Internet Protocol addresses of the Internet sites individuals visit.[133] This principle would enable judicial review of surveillance requests for this data based on a

---

123 *Id.*

124 *Id.*

125 *Id.*

126 *Id.*

127 *Id.*

128 *Id.*

129 *See* Commonwealth v. Augustine, 4 N.E.3d 846, 849-50 (Mass. 2014).

130 DIGITAL DUE PROCESS, *supra* note 3.

131 Pen registers and "trap & trace" are technologies used to obtain transactional data in real time about when and with whom individuals communicate over the phone. Marcus M. Baldwin, Note, *Dirty Digits: The Collection of Post-Cut-Through Dialed Digits Under the Pen/Trap Statute*, 74 BROOK. L. REV. 1109, 1113 (2009).

132 DIGITAL DUE PROCESS, *supra* note 3.

133 *Id.*

factual showing of reasonable grounds that the information sought is relevant to a crime being investigated, thus updating the law to reflect modern technology.[134]

Lastly, the government should first demonstrate to a court that the data is needed for its criminal investigation before securing transactional data about multiple unidentified users of communications or other online services when tracking a suspect.[135] This principle addresses the circumstance when the government uses subpoenas to get information in bulk about broad categories of telephone or Internet users, rather than refining their search and seeking the records of specific individuals that are relevant to an investigation.[136] For example, there have been reported cases of bulk requests for information about everyone that visited a particular web site on a particular day, or everyone that used the Internet to sell products in a particular jurisdiction.[137] Because such bulk requests for information on classes of unidentified individuals involve unique privacy interests, this principle applies a standard that requires a showing to the court that the bulk data is relevant to an investigation.[138]

B. Critiques of the Proposed ECPA Modifications

Much debate surrounds the attempts to fix the ECPA. Some individuals and organizations feel that certain attempts, such as Senator Leahy's proposed bill, fail to go far enough.[139] Others believe that legislative approaches to amending the ECPA are inherently faulty altogether.[140]

1. Free-Market Regulation

Free-market advocates might argue that protecting privacy can lead to higher costs for goods and services as well as a reduction in the quality of services.[141] As an alternative, free-market scholarship could argue that Internet Service Providers (ISPs) and customers should be encouraged by government entities to enter into private contracts with respect to e-mail privacy.[142] Legal requirements of notice and consent, enforced by federal law, could provide necessary privacy protections without passing on large regulatory costs to customers.[143] With that said, such an approach is not above reproach, and many have pointed to the limits of self-

---

134 *Id.*

135 *Id.*

136 *Id.*

137 *Id.*

138 *Id.*

139 Krause, *supra* note 66.

140 *See* Katherine A. Oyama, Note, *E-Mail Privacy After* United States v. Councilman*: Legislative Options For Amending ECPA*, 21 BERKELEY TECH. L.J. 499, 525 (2006).

141 *Id.* (citing FRED H. CATE, PRIVACY IN THE INFORMATION AGE, at ix (1997)).

142 *Id.*

143 *Id.*

regulation with respect to privacy protection.[144] Professor Paul Schwartz discussed the failures in the privacy market and stated:

> The emerging verdict of many privacy scholars is that existing markets for privacy do not function well. Due to such market failures, which are unlikely to correct themselves, propertization of personal information seems likely to lead to undesired results—even to a race to the bottom as marketplace defects lead competitors to take steps that are increasingly harmful to privacy.[145]

According to Schwartz, the main concern with allowing ISP industry self-regulation is that many individuals do not know how their information is processed.[146] Schwartz references a report from the Annenberg Public Policy Center finding that "the overwhelming majority of U.S. adults who use the Internet at home have no clue about data flows—the invisible, cutting-edge techniques with which online organizations extract, manipulate, append, profile and share information about them."[147] Schwartz contends that the lopsided balance of information available to consumers and industry participants, in addition to the relative vulnerability of consumers within the larger market, requires close scrutiny of and skepticism about the commodification of personal data.[148]

In the case of e-mail privacy, economic incentives alone will not pressure ISPs to adequately protect consumer privacy.[149] Private markets do not provide consumers with a meaningful choice concerning the issue of ISP e-mail monitoring because potentially invasive activities are invisible to the decision-making consumer when he or she is selecting a service provider.[150] In addition, consumers have little insight into or oversight of ISP activity once they commence using a company's service.[151] Furthermore, the major ISPs explicitly reserve the right to monitor their customers' e-mail.[152] Even if a customer decides to change ISPs, the switching costs are high including the hassle of changing one's e-mail address and contractual commitments with an ISP.[153]

---

144 *Id.*

145 Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2076 (2004).

146 *Id.* at 2075–76.

147 *Id.* at 2078 (citing JOSEPH TUROW, AMERICANS AND ONLINE PRIVACY: THE SYSTEM IS BROKEN 4 (Univ. Pennsylvania 2003), http://www.annenbergpublicpolicycenter.org/wp-content/uploads/20030701_online_privacy_report2.pdf); *see also* Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CALIF. L. REV. 395, 476 (2000).

148 Schwartz, *supra* note 145, at 2078–79.

149 *Id.*

150 *Id.*

151 *Id.*

152 *Id.*

153 *Id.*

2. Relationships of Trust: Why They Matter and How They Affect the ECPA and the Third-Party Doctrine

It has never been easier for the government to engage in surveillance of individuals.[154] Concerning governmental invasions of privacy, there is a disjunction between a citizen's expectation of privacy and what the federal constitutional law actually protects.[155] Professor John Palfrey states that, "[w]hat matters from the citizen's perspective is whether he or she has a reasonable expectation that the activities under surveillance are taking place in public or private."[156] The problem the digital age presents is that the line separating public and private information has become hazy, and the public-private distinction is less likely to trigger constitutional protections, as the government collects information from third parties who independently gathered the data.[157]

Professor Lawrence Friedman opines, "[u]nder existing law, the public-private distinction is defined by an individual's non-disclosure of personal information: in other words, only what we keep to ourselves is private."[158] This understanding flows from a series of pre-Internet Supreme Court cases previously discussed,[159] where the Court held that individuals hold no reasonable expectation of privacy in information they provide to third parties.[160] The problem is that the Court's understanding ignores the social presumption of discretion in normal relationships of trust.[161] We do not simply entrust a bank with our money out of convenience but also assume that information pertinent to our accounts, from our balances to our pin numbers, will not be disclosed to others.[162] A bank either unwilling or unable to protect such information should not reasonably expect to retain its customers.[163] Professor Friedman points out, we could choose to store our money or other valuables underneath our mattresses or in a safe at home, but the more productive route is to place those valuables in a bank account or safety deposit box.[164] We do so on the understanding that the bank will not disclose information about our

---

154 John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241 (2008).

155 *Id.*

156 *Id.* at 283.

157 *Id.*

158 Lawrence Friedman, *The Fourth Amendment in the Digital Age*, 79 MISS. L.J. SUPRA 41, 41 (2009), http://mississippilawjournal.org/wp-content/uploads/2014/11/Friedman_79MissLJSupra041.pdf.

159 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442–43 (1976).

160 *See Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 442–43.

161 Friedman, *supra* note 158, at 42.

162 *Id.*

163 *Id.*

164 *Id.*

account to anyone else.[165]

Relationships of trust are based on a common understanding that information disclosed between parties should not be shared with other outside parties.[166] If someone shares personal and private information with the bank, no one involved in that relationship has a basis for considering that information as being of public record.[167] Likewise, electronic communications are such that when correspondence is sent from a home computer, there is a reasonable expectation that such correspondence is private and the ISP should not enjoy the authority to disclose it to any outside parties, including the government.[168] The Supreme Court adopted an unnecessarily and dangerously broad view of what should be considered public.[169] By ruling that something is private only to the extent that we do not share it with anyone else, it mostly precludes the possibility of any relationship based on confidence and trust.[170] Any information disclosed between one person to another under such precedent would no longer enjoy the assumption of privacy.[171] Such an interpretation of the Fourth Amendment seems obtuse, as it would suggest that any and all information about ourselves we are either obligated to keep to ourselves or expect that everyone should know.[172]

Professor Friedman believes that until the reasoning of cases establishing that there exists no reasonable expectation of privacy in information given to third parties is replaced by a model that recognizes that privacy may subsist in relationships of trust, the digital age will be one in which the government has an ever-freer hand to acquire personal information about citizens.[173] The best method in ensuring that a paradigmatic shift concerning what is considered private information online is to amend the ECPA so that the government is required to obtain a search warrant based on probable cause to access information individuals expose online. Doing this on a federal level would ensure uniformity and clarity, and would certainly help to alleviate many of the issues keeping the ECPA's critics up at night.

V. CONCLUSION

Given the extreme influx of technology in our society, it has become almost impossible to avoid its regular utilization. Sacrificing the usage of technology in order to protect one's privacy can be alienating and unproductive. It would be both

---

165 *Id.*
166 *Id.*
167 *Id.*
168 *Id.*
169 *Id.*
170 *Id.*
171 *Id.*
172 *Id.*
173 *Id.* at 43.

unrealistic and unfair to assume that anyone who wishes to retain a certain level of privacy should completely refrain from using particular forms of technology or divulging personal information digitally. The laws need to be adjusted so that individuals can retain a reasonable expectation of privacy in the information that they provide to third parties through the usage of the Internet, cell phones, e-mails or other technological services. By simply amending the ECPA so that law enforcement officials are required to obtain a search warrant based on probable cause to obtain that information, society as a whole would benefit greatly. As Professor Lawrence Friedman expounds, "the [F]ramers would not likely believe it too much to require that the government continue to abide by the requirements of the Fourth Amendment, even as the means by which we communicate with each other and develop relationships of trust proliferate."[174] Friedman believes that, "In many circumstances, after all, the government's ability to articulate an individualized suspicion of wrongdoing may be all that stands between it and our personal information."[175] In light of the way we live our lives in the digital age, the current understanding of the public-private distinction may eventually work to completely undermine even that modest constitutional protection.[176] We need laws that protect our privacy in the digital context, and amending the ECPA in such a way as to essentially proliferate the third-party doctrine would be a simple step in the right direction.

174 Friedman, *supra* note 158 at 43
175 *Id.*
176 *Id.*