NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FRIENDING BRANDEIS:
PRIVACY AND GOVERNMENTAL SURVEILLANCE
IN THE ERA OF SOCIAL MEDIA

by

Elizabeth S. Gaffin

June 2012

Thesis Co-Advisors: Robert Josefek
Rodrigo Nieto Gomez

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.		
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis
4. TITLE AND SUBTITLE Friending Brandeis: Privacy and Government Surveillance in the Era of Social Media		**5. FUNDING NUMBERS**
6. AUTHOR(S) Elizabeth S. Gaffin		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A____.		
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Today, individuals network and interact with each other in radically different ways by using social networking sites, such as Facebook and Twitter. Utilizing this new media, individuals are able to share intimate details of their lives, coordinate activities, and exchange ideas with friends, family and others in ways previously accomplished only in person, by telephone, or in written letters stored at home. At the same time, terrorist organizations and other criminal actors are increasingly utilizing social networking sites, for both recruiting purposes and for the planning, financing, and execution of nefarious acts. As such, social networks have become a valuable source of intelligence for the law enforcement and intelligence communities that enable the collection of information pertaining to individuals in ways not previously possible. However, the law pertaining to surveillance in cyberspace has failed to keep pace with society's adoption of social networking and other cloud computing technologies. This thesis examines the privacy and civil liberties safeguards inherent in the Fourth Amendment and the need to ensure that an appropriate balance is struck between an individual's reasonable expectation of privacy in online communications and the government's information gathering requirements necessary to combat emerging criminal and terrorist threats.

14. SUBJECT TERMS Privacy and Civil Liberties, Surveillance, Fourth Amendment, Social Media, Social Networking Technologies Cloud Computing	**15. NUMBER OF PAGES** 137
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FRIENDING BRANDEIS: PRIVACY AND GOVERNMENTAL SURVEILLANCE IN THE ERA OF SOCIAL MEDIA

Elizabeth S. Gaffin
Attorney, Department of Homeland Security
United States Citizenship and Immigration Services, Washington, D.C.
B.S., Brooklyn College, 1984
J.D., Brooklyn Law School, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
June 2012

Author: Elizabeth S. Gaffin

Approved by: Robert Josefek, PhD
Thesis Co-Advisor

Rodrigo Nieto-Gomez, PhD
Thesis Co-Advisor

Daniel Moran, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Today, individuals network and interact with each other in radically different ways by using social networking sites, such as Facebook and Twitter. Utilizing this new media, individuals are able to share intimate details of their lives, coordinate activities, and exchange ideas with friends, family and others in ways previously accomplished only in person, by telephone, or in written letters stored at home. At the same time, terrorist organizations and other criminal actors are increasingly utilizing social networking sites, for both recruiting purposes and for the planning, financing, and execution of nefarious acts. As such, social networks have become a valuable source of intelligence for the law enforcement and intelligence communities that enable the collection of information pertaining to individuals in ways not previously possible. However, the law pertaining to surveillance in cyberspace has failed to keep pace with society's adoption of social networking and other cloud computing technologies. This thesis examines the privacy and civil liberties safeguards inherent in the Fourth Amendment and the need to ensure that an appropriate balance is struck between an individual's reasonable expectation of privacy in online communications and the government's information gathering requirements necessary to combat emerging criminal and terrorist threats.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

ACKNOWLEDGEMENTS

I wish to thank my family for their unending support during the past 18 months. A special thanks to my own two *Digital Natives*, Jeremy and Benjamin, who kept me abreast of all new emerging social networking technologies, and put up with my many excursions to the West Coast and to the library. I owe a tremendous debt of gratitude to my husband Robert Cannon who shared my excitement for this significant topic, and without whose assistance, this thesis would not be possible. Most of all, I would like to thank Special Agent 437, a.k.a. Romeo Cannon, for standing by my side throughout my research, giving me the confidence to continue, and giving me joy when I was frustrated.

In addition, I would like to thank my wonderful committee members for their tutelage. To Dr. Rodrigo Nieto Gomes, for sharing his enthusiasm and inquisitiveness about social media and its impact on society. To Dr. Robert Josefek, who patiently provided insights about both the subject matter and the academic process, and always returned my phone calls.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Today, individuals, particularly those in the younger generations, network and interact with each other in radically different ways than prior generations by using online social networking tools, such as Facebook, Twitter and, Google+. These new technologies enable individuals to share intimate details of their lives, coordinate activities, and exchange ideas with friends, family and others in ways previously accomplished only in person, and perhaps more limitedly, by telephone or in written letters. At the same time, social networking sites are increasingly being utilized by terrorist entities for recruiting planning, financing and execution of terrorist acts,[1] as well as by individuals engaged in other criminal ventures. As such, the Internet has become a valuable source of intelligence for the law enforcement and intelligence communities that enables the collection of information on individuals in ways not previously possible. With the advent of social networking technologies, the ability to track an individual's activities online has increased exponentially. However, existing privacy and civil rights law has failed to keep pace with advancements in technology, which leaves individuals with little to no "reasonable expectation of privacy" nor legal protections of their communications occurring in social media or other cloud computing tools. It is becoming increasingly critical to update pertinent laws or adopt online privacy principles that establish an appropriate balance between the government's surveillance needs and an individual's privacy and civil liberties interests.

To gain a proper understanding of an individual's reasonable expectation of privacy in today's digital world, it is important to understand the development of privacy as a cherished value and as a civil right in the United States. The framers of the Constitution enacted the Fourth Amendment to the Constitution to

[1] EUROPOL, *TE-SAT 2010: EU Terrorism Situation and Trend Report*, 2010, http://www.consilium.europa.eu/uedocs/cmsUpload/TE-SAT%202010.pdf.

protect individuals from unwarranted governmental intrusion of homes and personal affects without the issuance of a warrant premised upon probable cause. Interestingly, the Constitution does not contain the word privacy nor does it expressly provide protections for individual privacy rights, as they have become known today, in large part because the framers could not have imagined the technology that exists today (or even the technology that existed 100 years ago) and the potential for widespread governmental intrusion. Thus, no conception of the need to create Constitutional protections for other than personal and physical property existed.

The right to individual privacy as a concept has evolved and continues to evolve through the development of common law, the passage of federal statutes, and societal expectations. Advancements in communication technologies have far outpaced existing laws that enable governmental access to an individual's digital communications and other personal data stored in the cloud, with little or no judicial oversight. Today, the ability to control access to communications and other online activities, and to be free from unwarranted governmental intrusions in cyberspace, has been greatly compromised.

At the same time, terrorist and other criminal actors are using digital technologies to plan, recruit, and raise funds, and to execute their nefarious aims, which make their communications a valuable source of intelligence for those governmental entities entrusted with keeping this country safe. As the law enforcement and intelligence communities see the need for increased online data collection, the tension between privacy and civil liberties on the one hand, and information gathering and sharing on the other, is growing, which is highlighting the need for a significant reevaluation of the Fourth Amendment's protections.

Privacy and civil liberties are at a crossroads. Will Constitutional protections against unwarranted search and seizures, previously enjoyed by individuals utilizing traditional means of communication, apply to their digital communications? As Microsoft Associate General Counsel Mike Hintze stated, "[m]any Americans take for granted the protections of the Bill of Rights that

prevent the government from coming into people's homes without a valid search warrant. The rise of cloud computing should not diminish these privacy safeguards."[2] As individuals begin to migrate more of their communications and information into the cloud, it is imperative that an appropriate balance be struck between privacy and civil liberties of the individual, with the post-September 11 intelligence gathering needs of the law enforcement and Intelligence communities tasked with keeping the United States safe from additional acts of terrorism and other harm.

B. RESEARCH QUESTIONS

1. What are an individual's reasonable expectations of privacy in concerning digital communications occurring in social media or stored in the cloud?
2. How can we determine what is the correct balance is between an individual's reasonable expectation of privacy and the law enforcement and intelligence communities' lawful ability to collect information it needs to protect this country from emerging criminal and terrorist threats and how can the balance be achieved?
3. How should the Electronic Communications Privacy Act be amended to strike an appropriate balance between today's evolved expectations of privacy with the law enforcement and intelligence communities' efforts to protect the United States, which incorporates traditional notions of due process, civil liberties and judicial oversight?
4. How can internal policies be implemented by the law enforcement and intelligence communities, and by third party service providers, to afford Fourth Amendment like protections to individuals in the absence of clear legal standards? If so, what oversight mechanisms should be put in place to ensure compliance?

C. METHODOLOGY

Development of a legal and policy archetype that strikes a balance between an individual's civil liberties and privacy, and the intelligence and law enforcement communities' post-September 11 surveillance needs requires an

[2] Mike Hintze, "Restoring Balance to American Surveillance Laws," March 30, 2010, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/03/30/restoring-balance-to-american-surveillance-laws.aspx.

understanding of the current state of the law. It is essential to understand the evolution of the application of the Fourth Amendment as it existed in the early days of this country, as it evolved with the advent of new communications mediums, such as the telegraph and the telephone, and as it is applied today when intimate details of an individual's personal, religious and political life are communicated and stored outside that person's physical custody, by third parties, in cyberspace. This analysis focuses on privacy and civil liberties safeguards provided by the Constitution and those conferred by statutes, such as the Electronic Communications Privacy Act enacted in the early days of the Internet. In particular, it is important to understand the shortcomings of this technology centered statute, and how it fails to address privacy considerations associated with new and emerging social networking and cloud computing technologies.

This policy analysis includes: 1) an examination of the evolution of law as it relates to an individual's privacy and civil rights in his communications; 2) an examination of the current state of the law as it relates to an individual's privacy and civil liberties in communications occurring in social media and stored in cloud computing services; 3) applicable standards for the law enforcement and intelligence communities seeking to engage in the surveillance of an individual's electronic communications; 4) an examination of an individual's expectation of privacy in electronic communications and methods individuals employ to assert control over their information in cyberspace; and 5) options for the reform of the current law or the formation of policy to provide clear and consistent standards for surveillance in cyberspace while extending Fourth Amendment like protections to an individual's digital conduct.

The evolution of Constitutional law pertaining to the surveillance of electronic communication has resulted in a patchwork of inconsistent outcomes. An analysis of the principal Supreme Court cases interpreting the Fourth Amendment and the protections afforded to an individual and personal communications is conducted. In particular, the implications of the judicially created "Third Party Doctrine" that negates the "reasonable expectation of

privacy" when an individual entrusts information to another is considered. The Third Party Doctrine has become extremely problematic in the modern world, in which an individual regularly provides financial information to banks and online merchants and/or uses a mobile communication device to post messages on Facebook.

Further, an analysis of the Electronic Communication Privacy Act (ECPA) of 1986 is undertaken. ECPA was Congress' attempt to remedy the limitations on an individual's reasonable expectation of privacy imposed by the Third Party Doctrine and provide Fourth Amendment like protections to communications occurring on the Internet. These protections include an examination of the technology centric provisions of the act to determine how they apply to today's social networking technologies and whether the statute still provides meaningful safeguards for an individual and personal electronic communications.

D. RECOMMENDATIONS FOR A WAY FORWARD

Privacy and civil liberty protections may be afforded through the adoption of policy guidance by law enforcement and intelligence communities, as well as by a third party service provider. Existing policies are examined to determine whether governmental efforts to impose internal standards, such as those contained in a 1999 Department of Justice guidance on the use of the Internet for criminal intelligence gathering, have been effective in ensuring that privacy and civil liberties are afforded to users of social networking and cloud computing technologies.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. INTRODUCTION

How an individual's privacy and civil liberties are balanced against the law enforcement and intelligence communities' need to detect and deter emerging threats as communicated in cyberspace is the subject of a growing debate being conducted in literature, in U.S. courts and legislature and in popular discourse. Today, in cyberspace, an individual engaging in a conversation with friends has a limited expectation of privacy, even if it occurs in private, with all privacy settings elected, and in particular, when none of the friends have consented to the release of the information. With more and more personal information being communicated electronically in social networking sites (a form of cloud computing) and stored outside of homes in the cloud, the nature of an individual's reasonable expectation of privacy in cyberspace is the subject of a growing body of literature that includes an analysis of the Fourth Amendment, judicial decisions interpreting the boundaries of an individual's reasonable expectation of privacy in the new digital environment, and interpretations of a number of federal statutes. Of particular interest to the discussion of an individual's reasonable expectation of privacy and the appropriate standard for access by the law enforcement and intelligence communities is ECPA, a 1986 statute enacted prior to the popularity of the Internet as known today. In addition, a myriad of scholarly articles address societal expectations of privacy in the digital age, the increased use of the Internet by terrorist organizations, and of the lack of clarity in the existing legal paradigm relating to surveillance of the Internet by the law enforcement and intelligence communities.

Throughout this country's history, a constant cycle of technological developments have enabled the government to engage in more efficient means of conducting surveillance, while at the same time, challenging an individual's privacy and civil liberties. Often, in response, legislative attempts have been made to rectify gaps in the protections of those civil liberties, as well as judicial

efforts to align societal expectations of an individual's Constitutional rights with new and emerging technologies, especially when existing laws have failed to keep up with technological advancements. With the advent of social media and cloud computing, laws have once again failed to keep pace with the rapid advancements in technologies. Privacy and civil liberties are at a crossroad. As Microsoft Associate General Counsel Mike Hintze stated, "[m]any Americans take for granted the protections of the Bill of Rights that prevent the government from coming into people's homes without a valid search warrant. The rise of cloud computing should not diminish these privacy safeguards."[3]

B. EVOLUTION OF THE CONCEPT OF PRIVACY IN THE UNITED STATES AND THE APPLICATION OF THE FOURTH AMENDMENT TO COMMUNICATIONS

The framers of the Constitution enacted the Fourth Amendment to ensure freedom from unreasonable searches and seizures in response to three pivotal cases, two occurring in England, and the third in the colonies. The two English cases, *Wilkes v. Woods*, 19 Howelll's State Trials 1153 (1763), and *Entick v. Carrington*, 19 Howell's State Trials 1029 (1765), stemmed from the actions of an individual who had distributed pamphlets critical of the King and his ministers. The King issued a "writ," or general warrant to search the papers and other personal effects of the pamphleteer and his associates, to obtain evidence in support of a charge of seditious libel against the pamphleteer. The third case, known as the "Writ of Assistance" case, challenged the issuance of a general writ to permit the King's customs inspectors to obtain evidence of smuggling in the American colonies. The governmental intrusion stemming from these three cases so angered the Colonists that it further inflamed their growing opposition to British rule.[4] In response, the Founding Fathers sought to ensure that the powers of the newly created government were placed in check by providing an individual

[3] Hintze, "Restoring Balance to American Surveillance Laws."

[4] See Net Industries, "Search and Seizure-The Fourth Amendment: Origins, Text, and History," 2012, http://law.jrank.org/pages/2014/Search-Seizure-Fourth Amendment.

with freedom from unwarranted and unreasonable searches and seizures of home, person, papers, and effects. The Founding Fathers could not possibly have envisioned a world in which the details of an individual's personal, professional, political and religious life that, in their day, had been communicated or maintained in writings stored within their homes or made face-to-face with their associates, would now be communicated and stored outside of the home in the electronic manner to which Americans have become accustomed.

Initially, violations of the Fourth Amendment were redressed in trespass law. However, in 1890, two years after the introduction of the first widely available Kodak camera, two esteemed jurists Samuel Warrant and Louis Brandeis argued in a law review article entitled "Right to Privacy"[5] that an individual possesses a "right to be let alone" that may be redressed in tort law (the law of injury). Thirty years later, Justice Brandeis, now sitting on the Supreme Court, authored a pivotal dissenting opinion in *Olmstead v. U.S.,*[6] which would become the framework for today's constitutionally guaranteed privacy paradigm. In doing so, he argued that an individual possess a right to privacy in his telephonic communications, even if they travel outside of the physical walls of the home. Justice Brandeis envisioned a time when advancements in technology would enable the government to engage in extremely intrusive surveillance of citizens, and thus, argued for the recognition of an individual's right to be protected from unwarranted governmental searches and seizures in new and emerging technologies. The Supreme Court would not recognize this right for 40 more years.

In 1964, with computers in the embryonic stage of development and with the Internet still a dream of a few Department of Defense researchers and academics, Edward Bloustein in a law review article entitled "Privacy as an

[5] Louis D. Brandeis and Samuel Warren, "The Right to Privacy," *Harv. L. Rev. 4*, 193 (1890).

[6] *Olmstead v. U.S.*, 277 U.S. 438 (1928).

Aspect of Human Dignity: An Answer to Dean Prosser"[7] strongly advocated for a review of statute and common law to facilitate the development of privacy law that would ensure that an individual's privacy interests were protected in light of rapidly developing technologies. As Justice Brandeis had prognosticated, Bloustein called attention to the fact that:

> in our own day scientific and technological advances have raised the specter of new and frightening invasions of privacy. Our capacity as a society to deal with the impact of new technology depends, in part on the degree to which we can assimilate the threat it poses to the settled ways our legal institutions have developed for dealing with similar threats in the past.[8]

A few years later in 1968, in *Katz v. U.S.*,[9] the Supreme Court finally adopted the legal reasoning set forth in the legendary Justice Brandeis *Olmstead* dissent and held that an individual possesses a "reasonable expectation of privacy" in telephonic communications to include even those occurring outside of the home. Katz established a two-step test for determining whether an individual enjoyed a reasonable expectation of privacy. The test provides that an individual enjoys a reasonable expectation of privacy: 1) if the person exhibited an actual (subjective) expectation of privacy; and 2) if that expectation is one that society is prepared to recognize as reasonable. Conversely, the court noted that the reasonable expectation of privacy is negated when an individual confides in another, which gives rise to what is known as the "Third Party Doctrine."

The Third Party Doctrine is a judicially formulated doctrine that negates the reasonable expectation of privacy when information is communicated to a third party. Courts have held that:

> when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not

---

[7] Edward J. Bloustein, "Privacy As an Aspect of Human Dignity: An Answer to Dean Prosser," *39 N.Y.U. L. Rev* 962 (1964).

[8] Ibid.

[9] *Katz v. U.S.*, 389 U.S. 347 (1967).

> prohibit governmental use of that information. Once information is shared even with only one other, it is no longer "private"; the Fourth Amendment does not prohibit governmental use of the now non-private information.[10]

The Third Party Doctrine is particularly troubling today because most data residing in the digital world is transmitted or stored on third party intermediary sites. An individual may elect all possible privacy settings in an attempt to manifest a reasonable expectation of privacy. However, the application of the Third Party Doctrine to data transmitted and communicated in social media or stored in the cloud would arguably provide the government with such unfettered access that it would negate the protections envisioned by the Fourth Amendment.

Many scholars argue that the Third Party Doctrine, taken to its logical conclusion, has the potential to deprive all electronic communications occurring in social media and stored in the cloud of any Fourth Amendment protection,[11] and therefore, the Third Party Doctrine must be modified.[12] Prof. John Palfrey in "The Public and the Private at the United States Border with Cyberspace" has argued it is time to "rethink legal protections for citizens from state surveillance in a digital age as a result of this third-party data problem."[13] The concerns raised by both Brandeis and Bloustein regarding the need to adopt legal and procedural safeguards to ensure an individual's privacy and civil liberties in the face of new and emerging technologies are just as relevant today as they were in their times. Scholars, legislators, policy makers and the public are currently engaged in a fierce debates over whether an individual who utilizes the services of a third party social media provider is entitled to Fourth Amendment protections against

---

[10] *U.S. v. Miller*, 425 U.S. 435, 443 (1976).

[11] Katherine J. Strandburg, "Home, Home on the Web, and Other Fourth Amendment Implications of Technosocial Change," *Maryland L. Rev*. 70, no. 101 (2011), http://ssrn.com/abstract=1808071.

[12] See also Justice Sotomayor concurrence in *U.S. v. Jones*, 565 U.S. __, slip at 5-6 (January 23, 2012).

[13] John Palfrey, "The Public and the Private at the United States Border with Cyberspace." *Miss. L. J.* 78, no. 2 (2008): 241–292.

unwarranted searches and seizures, and if so, how best to create legal and policy safeguards to ensure an individual's privacy and civil liberties.

C. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

Katz v. U.S. held that individuals do possess a Fourth Amendment protected reasonable expectations of privacy in their telephonic communications regardless of where they may occur. However, a reasonable expectation of privacy is negated when communications are shared with another. With the growth in popularity and promise of computer network communications, including specifically electronic mail (e-mail), Congress saw the need to enact legislation that would embed Fourth Amendment like privacy safeguards into federal surveillance laws to protect the increased use of third party intermediaries (computer networks) entrusted with the transmission and storage of e-mail.

Therefore, in 1986, Congress enacted ECPA.[14] Enacted prior to the public use of the Internet, ECPA extended federal wiretap restrictions to new forms of electronic communications. ECPA protects electronic communications from being intercepted or disclosed to another absent a warrant or a specific exemption.[15] Title II of ECPA, known as the "the Stored Communication Act," provides protections for electronic communications in temporary storage as part of the store-and-forward computer communications process.[16] While Title I of ECPA, the Wiretap Act, covered the "forwarding" part of computer communications, Title II, the Stored Communications Act, covered the "stored" part, which is transitionally storage pending delivery or further transmission of the message (it is not storage of the content after it has been received). Thus, for example, the

[14] *The ECPA amended Title III of the Omnibus Crime Control and Safe Street Act of 1968* (The Wiretap Act).

[15] 18 USC § 2511(1)(a) proscribes "intentionally intercept[ing] . . . any wire, oral, or electronic communication," unless the intercept is authorized by a court order or by other exceptions.

[16] While not all electronic communications at the time followed the store and forward transmission protocol, the most dominant at the time, e-mail, did. Others, such as File Transfer Protocol, operated slightly differently.

Stored Communications Act covers e-mail transmitted to a recipient but not opened for a period of time not to exceed 180 days after which time it is considered abandoned.[17]

As forward leaning as the statute was in at the time of its passage, it codified Congress' understanding of computer networks as they existed at the time and failed to consider advancements in technology.[18] The dizzying array of access standards adopted by Congress reflected Congress' understanding of computer networks as they existed in 1986. Today, policy makers, legislators, judges, law enforcement and intelligence communities, and the general public are left with an antiquated statute that fails to provide clear standards for the application of the Fourth Amendment. These safeguards are ill suited for today's Web 2.0 social networking and cloud computing technologies. Accordingly, the Fifth Circuit described attempts to interpret ECPA as a "search for lightning bolts of comprehension [that] traverses a fog of inclusions and exclusions which obscures both the parties' burdens and ultimate goal."[19]

The USA Patriot Act amended portions of ECPA that greatly facilitated the government's ability to obtain access to telephone, e-mail communications, medical, financial, and other records. At the same time, it eased restrictions on the government's ability to engage in foreign intelligence gathering within the United States, and expanded the use of National Security Letters that enabled the Federal Bureau of Investigation (FBI) to search telephone, e-mail, and financial records without a court order.[20] Further, it permitted the delay in notification to the subject of the search, and in some cases, provided no notice at all.

---

[17] 18 U.S.C § 2510(17)(A).

[18] Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It." *Geo Wash L. Rev*. 72 (2004): 1208. Neither ECPA's statutory language nor its legislative history makes any reference to the Internet. Yonatan Lupu, "The Wiretap Act and Web Monitoring: A Breakthrough for Privacy Rights?" *VA. J. L. & Tech.* 9, no. 3 (2004).

[19] *Briggs v. Am. Air Filter Co.,* 630 F.2d 414, 415 (5th Cir. 1980).

[20] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001.*

ECPA "is famous (if not infamous) for its lack of clarity,"[21] in large part because of the differing standards that both private entities and the government must meet to obtain access to electronic records. Courts have had difficulty applying consistent readings within each title of the Act. Recently, the Sixth Circuit Federal Court of Appeals in *Warshak v. U.S*. went so far as to discard the Stored Communications Act as being unconstitutional. The Court concluded that to the "extent the [Stored Communications Act] purports to permit the government to obtain such e-mails without a warrant, the [Stored Communications Act] is unconstitutional."[22]

Courts are just now beginning to be confronted with cases in which they are being asked to determine whether or not an individual enjoys a reasonable expectation of privacy in digital communications occurring in social media or stored in the cloud. A district court in California encountered this issue for the first time in 2010 in a case between two private litigants. The Court held that private messages sent using Facebook or MySpace do in fact fall under the protections of the Stored Communications Act that limits the government's ability to force the internet service provider to "disclose information in their possession about their customers and subscribers." [23] Similarly, items posted on an individual's "wall" may also enjoy the protections of the Stored Communications Act, but only to the extent that an individual invoked the site's available privacy protections. It is extremely likely that in the coming days, courts will be confronted with additional

[21] *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994). The 5th Circuit held that "the seizure of a computer, used to operate an electronic bulletin board system, and containing private electronic mail which had been sent to (stored on) the bulletin board, but not read () by the intended recipients, did not constitutes an unlawful intercept under the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq*., as amended by Title I of the *Electronic Communications Privacy Act*, Public Law 99-508, *U.S. Statutes at Large* 100 (1986)"; See also *U.S. v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998) (stating that the 5th Circuit "might have put the matter too mildly"); Orin S. Kerr, "Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't." *NW. U. L. Rev*. 97, no. 2 (2003): 607. "The law of electronic surveillance is famously complex, if not entirely impenetrable."

[22] *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010). Although the *Warshak* holding may be persuasive in the other 11 federal circuit courts, it is not binding outside of the 6th Circuit.

[23] *Crispin v. Audigier, Inc*., "Order Granting Plaintiff's Motion for Review of Magistrate Judge's Decision Re Plaintiff's Motion to Quash Subpoena," United States District Court, Central District of California, filed May 26, 2010, CV 09-09509-MMM-JEM.

cases in which they will be called upon to strike a balance between an individual's Constitutional right to be protected from unwarranted searches and seizures, and the government's law enforcement and intelligence gathering needs.

D. DEVELOPMENT OF WEB 2.0 TECHNOLOGIES

Computer network communications have continued to technologically evolve from Web 1.0 technology, in which anyone could publish a webpage and communicate with everyone, to Web 2.0 technology in which anyone can publish a webpage and everyone can interact with, comment on, and share content on that web page, and currently to Web 3.0 technology, in which everyone can contribute, create, collaborate, and curate the content. Cloud computing has transformed information technology by moving both content and applications from the desktop computer secured within an individual's private home or business, to third party server farms located in undisclosed destinations. A new generation, referred to as Digital Natives, has grown up online that always has access to information technology.[24] Their social space has transformed from one restrained by distance and the need to be physically together to socialize, to an always on, always interactive, always with you social media experience. Facebook, the most popular social media site, reportedly has exceeded 845 million users worldwide.[25] Social media provides the opportunity to post and share information with everyone anywhere in the world, or, with the appropriate settings, only to a restricted select few.

E. PRIVACY AND SOCIAL MEDIA

Is an individual's reasonable expectation of privacy diminishing as more personal information is posted online, more confidences bared on social media,

---

[24] Marc Prensky, "Digital Natives, Digital Immigrants," *On the Horizon* 9, no. 5 (October 2010), http://www.marcprensky.com/writing/Prensky%20%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf.

[25] Facebook, "Statistics," (n.d.), http://www.facebook.com/ press/info.php?statistics.

and more information uploaded to third party services? Is there any merit to the notion attributed to Sun Microsystems CEO Scott McNealy that in cyberspace, an individual has "zero privacy anyway" and they should "just get over it."[26] Privacy has always been a difficult concept to define. Alan Westin in 1967 noted, "few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientist."[27] Professor Daniel Solove, who has written extensively on privacy issues declared, "the concept of privacy is in disarray. Privacy seems to be about everything and therefore it appears to be about nothing." However defined, privacy is a cherished value that is critical to a free society. As more and more individuals mediate their lives in social media, defining the notion of privacy has become even more difficult.

Despite the collaborative notion of social media, researchers have debunked the proverbial wisdom that users of social media have no expectation of privacy. A growing body of research suggests that individuals still retain some expectations of privacy, and especially, young people who have been dubbed "Digital Natives." danah boyd,[28] who has performed extensive research on the practices and attitudes of teens online, asserts that young people very much possess an expectation of privacy in their online postings that is manifested by the way in which they "manage" their online associations by limiting who may have access to their postings, as well as the use of codes to mask the meaning of their communications.[29]

---

[26] Polly Sprenger, "Sun on Privacy: 'Get Over It'," *Wired*, January 26, 1999, http://www.wired.com/politics/law/news/1999/01/17538.

[27] Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 7.

[28] danah boyd does not capitalize the first letter of her name. See danah boyd, (n.d.), "What's in a Name?" http://www.danah.org/name.html.

[29] danah boyd and Alice E. Marwick, "Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies: A Decade in Internet Time," *Symposium on the Dynamics of the Internet and Society*, September 2011, http://ssrn.com/abstract=1925128.

F. WEB 2.0 TECHNOLOGIES: AN ENGINE FOR CHANGE, GOOD AND BAD

The Internet promotes American ideals of participatory government, the corner stone to a sound democracy.[30] It has facilitated the spread of democratic ideals both within this country and around the world. At the same time, it can enhance national security by providing situational awareness about country conditions so that the United States is not blindsided when political upheavals occur. The recent events in the Middle East known as the "Arab Spring" were aided in part by the availability of social media technologies. Individuals in repressive regimes utilized social media to communicate with like-minded people in ways previously only possible at great peril to their well-being. It also enabled dissidents to focus international attention on these repressive regimes by transmitting news of atrocities committed by government forces.

At the same time, social networking sites are increasingly being utilized by terrorist entities for recruiting purposes, planning and financing, and execution of terrorist acts,[31] as well as by individuals engaged in other criminal ventures, such as the recent attacks on government websites by "hacktivists" like LulzSec and Anonymous? In "Terrorist Financing and the Internet," Michael Jacobson noted that terrorist organizations, such Al Qaeda, are increasingly relying on the Internet "to spread its toxic message and drum up support throughout the world." In addition, Al Qaeda has utilized the Internet to recruit, plan and execute terrorist activities and for fundraising.[32] In an attempt to identify and track terrorist activities on the web, the University of Arizona's Artificial Intelligence lab instituted the "Dark Web" project. As of 2007, the project estimated that between 7,000 and 8,000 web sites were "created and maintained by known international terrorist groups, including Al-Qaeda, the Iraqi insurgencies, and many

[30] *ACLU v. Reno*, 929 F.Supp. 825 (ED.Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

[31] EUROPOL 2010.

[32] Michael Jacobson, "Terrorist Financing and the Internet," *Studies in Conflict & Terrorism* 33, no. 4 (2010): 353–63.

homegrown terrorist cells in Europe."[33] Given the ubiquitous nature of the Internet, it has become a valuable source of intelligence for the law enforcement and intelligence community by enabling the collection of information in ways not previously possible.

However, some argue that the tracking of terrorist activity may result in degradation in civil rights. In "Terror on the Internet,"[34] Michael Weimann argues that although terrorist organizations take advantage of the largely "unregulated, anonymous and accessible nature of the Internet," surveillance of the Internet by the law enforcement and intelligence communities may result in an infringement of an individual's privacy. Mark Rotenberg, Executive Director of the Electronic Privacy Information Center, an online civil-liberties group, also cautioned that the tools utilized by projects like the Dark Web "to track terrorists can also be used to track political opponents,"[35] in contravention of the First Amendment.

Growing concern exists about the ease by which the government can aggregate the vast amounts of an individual's pertinent information pertaining to an individual that is now available electronically in social networking technologies or stored in the cloud, and create what is being called "digital dossiers." This concern is particularly great among "Digital Natives," defined by Palfrey and Gasser as young people, born after 1980, who have lived their lives on line "mediated by digital technologies."[36] Digital natives, as well as the general population, are finding it increasingly more difficult to protect their privacy as information pertaining to them is increasingly being compiled into digital dossiers. To date, no consensus exists as to the level of process necessary for the

[33] University of Arizona, Dark Web Project, "Scientists Use the "Dark Web" to Snag Extremists and Terrorists Online," Press Release 07-118.

[34] Gabriel Weimann, "Terror on the Internet: The New Arena, the New Challenge," *The United States Institute of Peace*, 2006.

[35] Steven Kotler, "'Dark Web' Project Takes on Cyber-Terrorism," October 12, 2010, http://www.stevenkotler.com/node/87.

[36] John Palfrey and Urs Gasser, *Born Digital* (New York: Basic Books, 2008), 53.

government to obtain information stored in these third-party digital dossiers that will ensure Fourth Amendment like protections to individuals' digital selves in cyberspace.

G. GROWING FRUSTRATION AND EFFORTS TO REFORM ECPA

Many believe that EPCA fails to provide sufficient clarity to govern today's transformed social media environment and are calling for a statutory revision.[37] In 2010, Congress held hearings in which it explored the possibility of reforming ECPA.[38] Testimony not only focused on the need to fix the legendary "lack of clarity" provided by ECPA but also on the need to bring the law into alignment with the development in technology and societal expectations of privacy. At the September 22, 2010, Senate Judiciary Committee hearing, Committee Chairman Patrick Leahy stated that:

> [b]ringing this privacy law into the Digital Age will be one of Congress's greatest challenges . . . the 'ECPA is a law that is often hampered by conflicting privacy standards that create uncertainty and confusion for law enforcement, the business community and American consumers.[39]

On May 19, 2011, Senator Leahy introduced the ECPA Amendments Act of 2011, S. 1011.

Similarly, scholars also have been grappling with determining how to achieve a reasonable expectation of privacy within personal e-mail accounts.

---

[37] The Digital Due Process Coalition, whose members include major giants in the technology and commerce sectors, such as Amazon, AOL, Microsoft, Center for Democracy and Technology, AT&T and Google, are seeking the amendment of ECPA so as "To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public." Digital Due Process Coalition, http://www.digitaldueprocess.org.

[38] *ECPA Reform and the Revolution in Cloud Computing. Hearing of the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights and Civil Liberties*, September 23, 2010, http://judiciary.house.gov/hearings/hear_100923.html.

[39] *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age. Hearing of the Senate Committee on the Judiciary* (Statement of Senator Patrick Leahy (D-Vt.), Chairman, Senate Committee on the Judiciary), September 22, 2010, http://judiciary.senate.gov/hearings/testimony.cfm?id=4776&wit_id=2629.

Professor Orin Kerr in “Applying the Fourth Amendment to the Internet: A General Approach” offers a possible approach to affording Fourth Amendment, protections to communications transmitted in e-mail.[40] He asserts that the Fourth Amendment should be applied in the digital world in the same manner in which it is applied in the physical world. In the physical world, the Fourth Amendment affords protections to the inside of an individual’s home but provides little to no protections outside the walls of said home. As such, he suggests that in the digital world, Fourth Amendment protections should be afforded to the inside of a person’s electronic communications, i.e., the contents, but not to the outside, i.e., the address and subject lines.[41]

The level of privacy protections that should be afforded to social media interactions, in which varying levels of privacy settings are invoked, is not well settled. In the absence of Congressional action to amend ECPA to keep it in line with the realities of today’s technological advancements, courts will have no choice but to attempt to provide some judicial interpretation and forge ahead that may result in inconsistent outcomes as cases work their way up to the Supreme Court. In addition, in the absence of legislative relief, executive agencies are also beginning to develop administrative guidelines for the collection of information obtained from social media.

Moreover, the lack of clear legislative standards has placed third party service providers squarely in the middle of this debate. It has become commonly accepted practice for social networking service providers to supply notice to its users if presented with “lawful requests” that they will provide content to law enforcement or intelligence entities. In the absence of clearer legislative and judicial standards, the determination of whether a request made pursuant to

[40] See Orin S. Kerr, “Searches and Seizures in a Digital World, George Washington Law School Pub. L. Research Paper No. 13, *Harvard L. Rev*. 119 (2005): 531; Kerr, “A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It”; Kerr, “Internet Surveillance Law After the USA Patriot Act”; Orin S. Kerr, “Lifting the “Fog” of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law,” *Hastings L. J.* 54 (2003): 805.

[41] Kerr, “Lifting the “Fog” of Internet Surveillance.”

other than a judicially issued warrant, is in fact, lawful is currently left to the companies and their legal counsel to determine, which has placed service providers at risk for legal action by the government, as well as by individuals.[42]

With the advent of social media and cloud computing, and society's rapid adoption thereof, once again society finds itself in a place in time in which laws affording the individual protections against unreasonable governmental searches and seizures are out of alignment with the realities of modern life. The need for additional scholarly work in these areas will likely grow as academics, the courts, service providers, legislators and the public continue to struggle to determine how the Fourth Amendment should be applied to communications occurring in e-mail and in social media.

[42] An example occurred in 2005, when the Department of Justice (DOJ) sought to obtain one week of searches from Google to help the DOJ defend its position on the Child Online Protection Act. Google held the position that the request was improper, overly broad, and refused to honor the request in the absence of a warrant as required by the Stored Communication Act of ECPA. Google was then forced to defend its position in court. This case and other subsequent cases highlight the ever increasing need to strike the correct balance between Fourth Amendment expectations of privacy with the law enforcement and intelligence communities' need to obtain pertinent information to detect, prevent and thwart potential terrorist and other criminal acts.

THIS PAGE INTENTIONALLY LEFT BLANK

III. HISTORICAL EVOLUTION OF COMMUNICATIONS PRIVACY JURISPRUDENCE

The concept of privacy as a cherished value and civil right in the United States has its roots in Colonial America and has continued to develop throughout this country's history. Fourth Amendment jurisprudence has evolved as communications networks have moved from the Pony Express to the Twitter Bird. Concern for the security and privacy of communications networks was born out of the colonists' rebellion against a King who executed arbitrarily searches and seizure of his subject's home and personal effects. Many years after the birth of this nation, it was revisited when the Supreme Court was confronted with the novelty of the telephone. Four decades later, when the telephone had become more of an annoyance than a novelty, and the early Internet was beginning to be built, the Supreme Court recognized that people possessed a "reasonable expectation of privacy" and that expectation extended to the person and not just property. Two additional decades passed and the Internet was becoming the Department of Defense's primary data network (although few outside the Department of Defense-academic community had been given access). Congress, anticipating the importance this new communications medium would play in modern society, extended privacy protections from analog phone lines to digital communications. Another two and a half decades have passed, during which time the Internet has become a fundamental mean's of communication. The Constitutional concern for the privacy of communications, and the access of the sovereign to those communications, has evolved over hundreds of years. It has occurred during a time in which the speed of communications networks have been measured in bits per week (pony express), bits per day (telegraph), bits per minute (telephone), and now gigabits per second (broadband Internet).

A. EARLY AMERICAN CONCEPTS OF PRIVACY—"A MAN'S HOME IS HIS CASTLE"

David Flaherty, in *Privacy in Colonial New England,* writes that colonists living in New England viewed their homes as "a heaven for solitude and intimacy as a barrier against intrusion by uninvited outsiders."[43] Legal justification for this view stemmed from the 1604 English *Semayne* case [44] that gave legal recognition to the age-old adage that "[a] man's home is his castle." The case challenged the Crown's ability to break into a subject's home unannounced, and gave rise to the requirement that prior to entering a subject's home to execute legal process, the Crown's representative was required to announce his impending entry and the justification for doing so, which established the importance of providing notice to the subject of governmental action.

In the period leading up to the Revolution, the age-old tenet came under attack both in England and in the colonies when the Crown, facing political pressure, increased its use of the "Writ of Assistance." Writs of Assistance granted representatives of the Crown virtually unlimited authority to enter an individual's home, and search and seize items found therein. Evidence obtained in these general searches was used to squash political discontent and to combat the burgeoning smuggling trade in the colonies. The General Writ was particularly arbitrary and enabled the holder to enter a private home or business without specific justification. General Warrants could be executed without warning and with little oversight to keep governmental abuses in check. As such, they greatly tested the bounds of the principle that an individual's home was indeed his castle. The use of the writ was challenged in three seminal cases: *Entick v. Carrington*, 19 Howell's State Trials 1029 (1765) (England); *Wilkes v. Wood*, 19 Howell's State Trials 1153 (1763) (England); and the *Writ of*

---

[43] David H. Flaherty, *Privacy in Colonial New England* (University of Virginia Press, 1967), 85.

[44] *Semayne's Case*, 5 Co. Rep. 91a, 91b, 77 Eng. Rep. 194 (K. B. 1603), 1604, http://www.law cornell.edu/ancon/html/amd4frag1_user.html.

Assistance Case (1761) (The Colonies). The outcome of these cases added fuel to growing colonial discontent with English rule, and ultimately, resulted in the passage of the Fourth Amendment.

Entick and *Wilkes* arose from the execution of a Writ of Assistance used to break into the homes of John Wilkes and his associates. Wilkes was a pamphleteer accused of seditious libel for printing materials adverse to the King and his practices. Agents of the King ransacked the homes of Mr. Wilkes and his associates and seized private books and papers. Lord Camden, the judge presiding over these defining cases, declared that the use of the writs to allow the removal of an individual's papers and other personal affects undermined the fundamental liberties of Englishmen. Personal papers, Lord Camden noted, are an individual's "dearest property" and "where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass."[45] The issuance of a general warrant not premised upon what has become known as probable cause, had no basis in English common law. More than 100 years later, the U.S. Supreme Court would comment on the significance of Lord Camden's ruling in the case of *Boyd v. U.S.*:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employee's of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence,—it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment.[46]

The *Wilkes* and *Entick* cases were quite influential in the colonies in which tensions were mounting over attacks on the individual liberties of the colonists.

---

[45] *Entick v. Carrington*, 19 Howell's State Trials 1030, 1066 (1765).

[46] *Boyd v. U.S.*, 116 U.S. 616, 630 (1886).

These tensions came to a feverish pitch when the Crown used a General Writ to enter the business of a Boston merchant accused of smuggling. Smuggling in the colonies was rampant at the time in large part as a way to avoid usurious taxation rates imposed by the Crown. James Otis, the former British Advocate General in the colonies, unsuccessfully challenged the Writ on behalf of the Boston merchant. Otis declared the actions of the Crown to be the "worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law that ever was found in an English law-book."[47] Otis' five-hour speech was witnessed by the impressionable young John Adams, who declared that "then and there, the child Independence was born."[48]

B. DRAFTING OF A NEW CONSTITUTION—A GOVERNMENT THAT SERVED AT THE WILL OF THE PEOPLE

As the revolutionary struggle played out, freedom from governmental intrusion as a precursor to the concept of privacy was deemed to be an essential element to a free society. This sentiment was enshrined in the Declaration of Independence that pronounced that all men are endowed with certain inalienable rights, and that "among these are life, liberty and the pursuit of happiness." The Founding Fathers sought to create a government that served at the will of the people and whose powers were limited to those bestowed upon it by the people. This aspiration is encapsulated in the United States Constitution which sets forth the structure of the three parts of the government, as well as the relationship of the citizen to the state.

The concept that the government served at the will of the people and not the other way around was the product of liberal thinkers of the Enlightenment period. Thomas Jefferson, one of the central drafters of the Declaration of Independence and of the Constitution, had been greatly influenced by the works

---

[47] James Otis, "Against Writs of Assistance," *National Humanities Institute*, February 1761, http://www.nhinet.org/ccs/docs/writs.htm.

[48] The Boston Society, "History of the Old State House Building," 2012. http://www.bostonhistory.org/?s=osh&p=history.

of the English Enlightenment philosopher John Locke and incorporated his principles into the documents that serve as the cornerstone to the American democracy. Locke, the father of liberalism writing in 1600s, had refuted the concept of the Divine Rights of Kings[49] in the *Two Treatises of Government.*[50] The principles contained within the Divine Rights of Kings had kept the European monarchy in power for generations. Locke argued that in a civil society, freemen who had been bestowed by god with natural rights, such as self-liberty, willingly relinquished to the government those liberties for the sake of the guarantee of safe peaceful enjoyment of person and property.[51] Government formed by "mutual agreement of men acting freely" served the interests of its citizens and when it ceased to do so, could be disbanded and a new government created in its stead that would do so. Locke also argued that the powers of a government should be divided among different branches of government to include a strong legislative branch, whose laws were to be reviewed by "authorized judges" and an executive that could not usurp the authority of the other branches of government.[52] It was in this spirit that the Founding Fathers sought to ensure that the powers of the newly created government were placed in check, for as Constitutional scholar Benno C. Schmidt Jr. reminds us, "privacy is absolutely essential to maintaining a free society. The idea that is at the foundation of the notion of privacy is that the citizen is not the tool or the instrument of government —but the reverse."[53]

Patriot George Mason set forth the basic requirements for lawful search and seizure in the Virginia Declaration of Rights, which was adopted shortly

---

[49] Robert Flemming, *Political Discourses, Viz. Patriachal, or the Natural Power of Kings: The Free-Holders Grand-Inquest* (Google Books, 1680).

[50] John Locke, *Two Treatises of Government* (Google Books, 1821).

[51] Peter Laslett, *John Locke, Two Treatises of Government* (New York: Mentor Books, 1963), 377–82.

[52] Locke, *Two Treatises of Government*, book II, ch. 11–12.

[53] Curtis Sitimore, "To Benno Schmidt Jr., There Can Be No Free Society Without Privacy," *Christian Science Monitor*, December 5, 1986, http://www.csmonitor.com/1986/1205/zfree3b.html#.ThRqspPmwIs.e-mail.

before the enactment of the Declaration of Independence, which ultimately provided the foundation for the Fourth Amendment that protects "persons, papers and effects" from such arbitrary invasion by requiring law enforcement to obtain warrants issued by a court upon a showing of probable cause. The Fourth Amendment's protections provide important safeguards against possible tyranny of government.[54] The Fourth Amendment, which provides limits on the government's ability to search and seize an individual's home and effects without a judicially issued warrant premised on probable cause, provides as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

As forward thinking as the Founding Fathers were in crafting a system of government that would protect the civil rights of its citizens, they could not have possibly anticipated advancements in technology that exist in today's networked world. David Flaherty in *Privacy in Colonial New England* opined that "[p]rivacy received as much protection in the Bill of Rights as was needed at the time; the various amendments have remained the starting point as the American legal system has sought to respond to the vastly increased number of serious challenges to personal privacy in modern American society."[55]

C. COMMON LAW PROHIBITION AGAINST "EAVESDROPPING"

Arguably, one of the first forms of surveillance recognizable in common law was the act of "eavesdropping." Blackstone's Commentaries on the Law of England described the offense as "[to] listen under walls or window or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and

---

[54] TechFreedom, "Letter to the Honorable Patrick J. Leahy Chairman United States Senate Committee on the Judiciary," April 6, 2011, http://www.scribd.com/doc/52390394/DLP-Coalition-Letter-on-ECPA.

[55] David H. Flaherty, *Privacy in Colonial New England* (University of Virginia Press, 1967), 249.

mischievous tales." It was an offense punishable by "fine and finding of sureties for good behavior."[56] Eavesdropping was a crime recognizable in early America, although perpetrators were rarely prosecuted. As such, the legal concept had "nearly faded from the legal horizon"[57] by the 19th century. However, with the advent of modern day means of communications, the principle embedded in this common law prohibition was codified in subsequently passed wiretap legislation.

D. FREEDOM FROM PRYING EYES, PRIVACY IN EARLY MAIL

During the colonial period, the mail system was the central means for communicating between England and the colonies and within the colonies. Benjamin Franklin was tasked by England in 1753 to run the mail system in the colonies.[58] Users of the mail system had very little expectation that their correspondence would arrive unopened.[59] In 1753, Franklin required mail carriers to take an oath not to open mail entrusted to them. Despite the administration of this oath, Robert Ellis Smith, in *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, asserts that "opening of the mail by authorities was neither unusual nor unexpected,"[60] especially during the Revolution. By 1775, Franklin had been dismissed as Postmaster by England "for sympathies to the cause of the colonies." William Goddard, the new colonial postmaster, warned patrons of the service:

---

[56] William Blackstone, "Commentaries on the Law of England," 1769, http://www.lonang.com/exlibris/blackstone.

[57] Joel P. Bishop, *Bishop Commentaries on Criminal Law*, 670, 1882.

[58] United States Postal Service, "Publication 100—The United States Postal Service—An American History 1775–2006: Colonial Times," May 2007, http://about.usps.com/publications/pub100/pub100_002.htm.

[59] Robert E. Smith, "Ben Franklin's Web Site: Privacy and Curiosity from Colonial America to the Internet," *Privacy Journal*, 2000, http://www.worldcat.org/title/ben-franklins-web-site-privacy-and-curiosity-from-plymouth-rock-to-the-internet/oclc/43615216, 49.

[60] Ibid.

> Letters are liable to be stopped & opened by ministerial mandates, & their contents construed into treasonable conspiracies; and newspapers, those necessary and important vehicles, especially in times of public danger, may be rendered of little avail for want of Circulation. . . .[61]

During the Revolutionary War, grave consequences occurred if the contents of patriot's written correspondence fell into the hands of representatives of the King. Individuals took great steps to protect their correspondence to include writing under a pen name (pseudonym) or using codes or ciphers, two early forms of encryption.[62]

Shortly after the birth of the United States, Congress passed the first of several laws prohibiting the opening of mail put into the custody of the newly formed U.S. mail service.[63] Congress passed an additional statue in 1825, which required letters and packages placed in the U.S. mail system to be free from "examination and inspection." The constitutionality of the statute was affirmed by the Supreme Court in the case of *ex parte v. Jackson*, which held that:

> the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.[64]

E. ADVANCEMENTS IN TECHNOLOGY AND "THE RIGHT TO BE LEFT ALONE"

With the introduction of a portable camera by Kodak in 1888 and other new technologies, the emphasis on privacy in America in the late 1800s shifted

---

[61] United States Postal Service, "Publication 100—The United States Postal Service—An American History 1775–2006: Colonial Times," May 2007, http://about.usps.com/publications/pub100/pub100_002.htm.

[62] Smith, "Ben Franklin's Web Site: Privacy and Curiosity from Colonial America to the Internet," 25.

[63] Ibid., 50.

[64] *Ex parte Jackson*, 96 U.S. 727 (1877).

from freedom from governmental intrusion of an individual's home and physical being, to an individual's concern about the publication of pertinent personal information that also concerns reputation, work product or the memorialization of thoughts. In a definitive 1890 Harvard Law Review article entitled *Right to Privacy*, two Harvard schooled attorneys, Samuel Warren and Louis Brandeis, questioned the fundamental legal values adversely impacted by the advent of emerging technology. They challenged the courts to use the instrument of common law to craft remedies that would afford legal protections to ensure an individual's privacy. Warren and Brandeis mused:

> the intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[65]

Brandeis and Warren argued that the ever-evolving instrument of common law needed to respond to "recent inventions and business practices" that enabled the intrusion of an individual's "thoughts, emotions and sensations," and bestow upon the individual legal recognition of "the right to be left alone."[66] "The Right to Privacy" was a stinging indictment of the newly emerging practices of journalists, in particular photojournalists, who were "invading the sacred precincts of private and domestic life and [whose] numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops."[67]

The two partners noted that initially, the law provided protections from physical intrusions of an individual's person and belongings and that liberty meant freedom from "physical restraint." As time went by, recognition of a

---

[65] Brandeis and Warren, "The Right to Privacy."

[66] Ibid.

[67] Ibid.

person's "spiritual nature" and of "feelings and intellect" emerged. Accordingly, the "right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" have grown to comprise every form of possession—intangible, as well as tangible."[68]

Warren and Brandeis' work is generally regarded as being the impetus behind the creation of the four invasion of privacy torts set forth in the Restatement (Second) of Tort: [69] (1) intrusion upon the seclusion; [70] (2) appropriation of name or likeness;[71] (3) publicity given to private life;[72] and (4) publicity placing person in false light.[73] Courts began to apply the principles set forth in Warren and Brandeis' "The Right to Privacy" in cases asserting injuries in tort and defamation.[74] Gradually, the four torts were recognized by the courts and became part of American jurisprudence. Although they created private causes of actions and not rights against the government, they were instrumental in shaping the concept of privacy in America.

F. PASSAGE OF THE FIRST WIRETAPPING STATUTE

The first wiretapping statute was passed as a temporary measure to prevent disclosure of government secrets during World War I.[75] However, with the invention and adaption of telegraph and telephones, states began enacting legislation to protect their citizens from unwarranted interception of their

---

[68] Brandeis and Warren, "The Right to Privacy."

[69] See Ben E. Bratman, "Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy," *Tennessee L. Rev.*, 69, 623 n. 10, *U. of Pittsburgh Legal Studies Research Paper*. 2002. SSRN: http://ssrn.com/abstract=1334296.

[70] Restatement of the Law, Second, Torts, Sec. 652, *The American Law Institute*, 1977.

[71] Ibid., Sec. 652C.

[72] Ibid., Sec. 652D.

[73] Ibid., Sec. 652E.

[74] Daniel J. Solove, "A Brief History of Information Privacy Law," *Proskauer on Privacy, PLI, GWU Law School Pub. L. Research Paper No. 215* (2006): 1–11, SSRN: http://ssrn.com/abstract=914271. The torts of libel and slander provided a remedy for the publication of false information and not for the publication of private information.

[75] 40 Stat. 1017-18 (1918).

telegraphic and telephonic communications. By 1928, 41 of the 48 states had "banned wiretapping or forbidden telegraph employees and officers from disclosing the content of telephone or telegraph or both."[76]

G. EARLY APPLICATION OF THE FOURTH AMENDMENT TO TELEPHONIC COMMUNICATIONS—*OLMSTEAD V. U.S.*

Judicial analysis of Fourth Amendment protections in a communications network dates back to 1928, long before the World Wide Web or social media. In 1928, telephone service was still in its infancy. The Federal Communication Commission had yet to be established. Telephone service had not been universally deployed and was largely a tool for business. When initially confronted with a challenge to the propriety of wiretapping of private conversations occurring on this novel service, the Supreme Court, in a 5-4 split decision, concluded that the Fourth Amendment did not apply to telephonic transmissions once they existed an individual's home. In *Olmstead*, police officers had tapped defendant Ray Olmstead's phones and intercepted a transmission that exited his home and his office. In doing so, the police had not trespassed on the defendant's property at home or in the office, but attached equipment to the network nearby.[77] The Supreme Court's ruling that there was no expectation of privacy in a phone call remained the law of the land for four decades.

Traditionally, searches were deemed to have occurred only when the government engaged in a physical trespass of an individual's property. In this first Supreme Court decision addressing wiretapping by federal law enforcement officials of a bootlegger's home and office, the court did not deviate from the physical trespass view and declared that an individual had no Fourth Amendment protected right of privacy in communications that exited the home by telephone.

---

[76] Charles Doyle and Gina Stevens, "Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping," *Congressional Research Service*, Order Code 98-326, 2008.

[77] *Olmstead v. United States*, 277 U.S. 438 (1928) (J. Brandeis, Dissenting Opinion).

The Court based its holding on the fact that "there was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only."[78]

In a defining dissent, Louis Brandeis, co-author of *The Right to Privacy* and now a Supreme Court Justice, challenged the majority approach by declaring:

> in the application of a constitution, our contemplation cannot be only of what has been, but of what may be. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may someday 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.[79]

Brandeis argued that the Court in *Olmstead* failed to recognize the Constitution as a living document. The framers of the Constitution could not have anticipated the advancements that had occurred in technology since the colonial era nor did they intend for the protections afforded by the Bill of Rights to be limited to those threats that existed in the early days of this nation. Brandeis envisioned a time when surveillance apparatuses the size of a pin could be planted within one's home by the government, with the effect to chill civilized man's greatest possession, the right to have his own independent thought free from the judgmental eyes of the government.

Brandeis explored the essence of the liberty interests the Founding Fathers were attempting to bestow:

> When the Fourth and Fifth Amendments were adopted, 'the form that evil had theretofore taken,' had been necessarily simple. Force and violence were then the only means known to man by which a Government could directly effect self-incrimination. It could compel the individual to testify—a compulsion effected, if need be, by

[78] *Olmstead v. United States*, 277 U.S. 438 (1928), 464.

[79] Ibid., 474

> torture. It could secure possession of his papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language. But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[80]

Brandeis' dissent laid the foundation for what has become modern day privacy law.

In 1934, six years after *Olmstead*, Congress attempted to rectify the adverse holding in *Olmstead* in the Federal Communications Act of 1934 by statutorily creating Fourth Amendment like protections for an individual's telephonic communications. In addition to drafting a comprehensive regulatory scheme to address emerging telecommunications technologies, it also included a prohibition on wiretapping by any person including the government, thus bringing the law into alignment with advancements in technology. Section 605 of the Act provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person..."[81]

H. JUDICIAL RECOGNITION OF A REASONABLE EXPECTATION OF PRIVACY

Olmstead remained the law of the land until 1967, when the constitutionality of wiretaps was once again challenged in two defining cases. In *Berger v. U.S.*, the Fourth Amendment's protections were held to extend to a "conversation," and the use of electronic devices to capture it was a "search"

---

[80] Ibid., 473.

[81] 47 U.S.C. § 605 (1946). *Nardone v. U.S.*, 302 U.S. 379 (1938). The statute did not apply to action of the states nor did it provide any penalty for evidence obtained by wiretaps not introduced into evidence. See Daniel J. Solove, "Surveillance Law Reshaping the Framework," *Geo. Wash. L. Rev.* 72, no. 1264 (2004): 1272–73.

within the meaning of that Amendment.[82] In *Katz v. United States*,[83] the Supreme Court determined that Fourth Amendment protections extend to the person and not just home and property. In these two cases, the Supreme Court adopted the arguments asserted by Brandeis in the *Olmstead* dissent, and brought the common law into alignment with prevailing societal expectations by holding that the Fourth Amendment protects people, and not merely places.[84] Thus, the court recognized that an individual does enjoy a Fourth Amendment protected expectation of privacy in telephonic communications occurring outside of the home.

The Court in *Katz* established a two prong test to determine whether an individual possesses a "reasonable" or "legitimate" expectation of privacy.[85] The test provides that an individual enjoys a reasonable expectation of privacy if conduct reflects "an actual (subjective) expectation of privacy," that is, "one that society is prepared to recognize as 'reasonable.'"[86] Accordingly, when a person enters a public telephone booth, shuts the door and makes a call, this conduct reflects a reasonable expectation of privacy, and as such, the government must obtain a warrant to seize an individual's conversations occurring in a communications network. However, the Supreme Court caveated its finding by noting that "what a person knowingly exposes to the public, even in his own home or office is not a subject of Fourth Amendment protection,"[87] which gave rise to what has become known as the "Third Party Doctrine."

Many legal procedures exist to search and seize items by law enforcement and intelligence communities. They include warrants, court orders

---

[82] *Berger v. U.S*. 388 U.S. 41, 51 (1967).

[83] *Katz v. U.S*. (Justice Harlan, concurring). The FBI placed a wiretap on a public telephone and recorded Katz's conversations without obtaining a warrant. The evidence was used to convict the defendant of transmitting wagering information out of state.

[84] Ibid., 351.

[85] Ibid., 361

[86] Ibid.

[87] Ibid., 350.

and subpoenas. Each method requires differing levels of judicial oversight, with warrants requiring the maximum level and subpoenas requiring little to none.

- Warrants—There are many types of warrants but as a general manner, a warrant is a judge's written order authorizing a law-enforcement officer to conduct a search of a specified place and to seize evidence. The government must demonstrate that it has probable cause to believe that the evidence of a certain crime will be located at the place to be searched. A warrant premised upon probable cause is per se constitutional.
- Court Orders—A court order is a command, direction, or instruction. A court order is a court's mandate to compel an action. It can be to compel testimony, compel the disclosure of an items or to compel that action be taken. It can be issued in writing or orally and may or may not require the signature of a judge.
- Subpoena—Latin for punishment, is a method to compel the production of an item or a person. Subpoenas can be issued by administrative agencies with no judicial oversight. The use of a subpoena does not afford the Constitutional protections afforded to a warrant.

I. THIRD PARTY DOCTRINE

An individual's reasonable expectation of privacy concerning information is not absolute. Information loses its Fourth Amendment protections when it is "knowingly" exposed to another, which enables the government to obtain access without the need for a warrant. Courts have held:

> when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now non-private information.[88]

The Third Party Doctrine codified a proverb attributed to Benjamin Franklin that "three may keep a secret, if two of them are dead."[89]

---

[88] *King v. U.S.*, 55 F.3rd 1193, 1195-96 (6th Cir. 1995).

[89] Benjamin Franklin, Wikiquote, (n.d.), http://en.wikiquote.org/wiki/ Benjamin_Franklin.

The Third Party Doctrine is particularly troubling today since most data residing in the digital world is transmitted and stored on third party intermediary sites. Taken to its logical conclusion, the Third Party Doctrine has the potential to deprive an individual of any reasonable expectation of privacy he may have in his digital communications, which has led many to call for a reevaluation of the Constitutional protections afforded an individual in cyberspace. Recently, Supreme Court Justice Sotomayor, concurring in a pivotal Fourth Amendment challenge to the government's warrantless use of Global Positioning System (GPS) on a suspect's car, opined that it may be time to reevaluate the "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[90] She further declared, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[91] Although the Court did not decisively resolve the issue of the applicability of the Third Party Doctrine to today's digital communications, it is without doubt that the issue will come before the Court in the near future.

J. THREE CATEGORIES OF ONLINE INFORMATION CREATED BY *KATZ* AND THE THIRD PARTY DOCTRINE

For purposes of government investigations, *Katz* creates three categories of information: (1) open source—information freely accessible from public sources, such as newspapers and libraries; (2) Third Party Doctrine—information an individual has shared with a third party, and thus, has given up an expectation of privacy; and (3) private communications. On the Internet, these three categories of information would be (1) first person voluntarily disclosure, in which an individual voluntarily makes information available by positing it on a publicly

[90] *U.S. v. Jones*, 565 U.S.__, slip at 5-6 (2012, January 23).

[91] Ibid.

available Internet site; (2) third party disclosure in which an individual discloses information to a third party, such as a provider of financial services; and (3) private online communications, in which an individual either stores personal data online or attempts to have a private conversation with others online.

It is safe to say that that an individual who openly posts personally identifiable information so as to be publicly available on the Internet has demonstrated no reasonable expectation of privacy and the information is "open source" material. In recognition of the growing availability of "open source" information on the Internet, the Department of Justice in 1999 issued guidance to its investigators and prosecutors entitled "Online Investigative Principles for Federal Law Enforcement Agents"[92] that set forth 11 principles governing the collection of information online. Generally, the principles provided that agents may obtain information without a warrant, "from publicly accessible online sources and facilities under the same conditions as they may obtain information from other sources generally available to the public."[93] Access did not require special legal authority or permission. In addition, agents are permitted to "passively observe . . . real-time electronic communications open to the public under the same circumstances in which the agent could attend a public meeting."[94] The guidelines also provided principles for undercover operations, including specifically prohibiting an agent from acquiring or using another person's identity without first obtaining the consent of the individual. Although the

[92] United States Department of Justice, DOJ-The Online Investigations Working Group, "Online Investigative Principles for Federal Law Enforcement Agents," November 1999, http://publicintelligence.net/department-of-justice-online-investigative-principles-for-federal-law-enforcement-agents/.

[93] United States Department of Justice, DOJ-The Online Investigations Working Group, "Online Investigative Principles for Federal Law Enforcement Agents," 10.

[94] Ibid., 22.

guidelines were written prior to the popularity of social networking, these guidelines are still relevant to today's environment and have been adopted by the Department of Homeland Security.[95]

K. ENACTMENT OF THE FEDERAL WIRETAP LEGISLATION IN LIGHT OF *KATZ*

In response to the Supreme Court rulings in *Berger* and *Katz* and the creation of the Third Party Doctrine, Congress attempted to strike a balance between the protections afforded an individual by the Fourth Amendment with the government's needs to obtain evidence lawfully by enacting Federal Wiretap legislation. The ensuing Federal Wiretap Act regulated federal law enforcement's ability to engage in the interception and electronic capture of oral and wire communications in a manner that ensured an individual's reasonable expectation of privacy. Title III of the Omnibus Crime and Safe Streets Act of 1968, The Wiretap Act, [96] prohibited the interception or acquisition of data through wiretapping, electronic eavesdropping of face-to face conversations, telephone conversations, or other wire communications in the absence of a court order.[97] The Wiretap Act provided the authority to perform electronic surveillance in a limited number of enumerated crimes when no less restrictive means was available.[98]

L. THE ELECTRONIC COMMUNICATION PRIVACY ACT

With the growth in popularity and promise of computer network communications, and the increased use of electronic mail (e-mail), Congress saw the need to enact legislation that would embed Fourth Amendment like privacy

---

[95] *See DHS monitoring of social networking and media: Enhancing intelligence gathering and ensuring privacy*: *Hearing before Committee on Homeland Security, Subcommittee Counterterrorism and Intelligence*. 112th Cong. (Feb. 16, 2012) (Testimony of Department of Homeland Security Privacy Officer Mary Ellen Callahan) http://homeland.house.gov/hearing/subcommittee-hearing-dhs-monitoring-social-networking-and-media-enhancing-intelligence

[96] Public Law 90-351, 42 U.S.C. § 3711; 18 U.S.C. §§ 2510-2522.

[97] 18 U.S.C. § 2511.

[98] Ibid.

safeguards into federal surveillance laws. The ensuing Electronic Communications Privacy Act sought to afford protections to communications that were increasingly occurring on third party intermediaries computer networks entrusted with the transmission and storage of e-mail.[99] Enacted prior to the widespread public use of the Internet, ECPA extended federal wiretap restrictions to new forms of electronic communications. ECPA protects electronic communications from being intercepted or disclosed to another absent a warrant or a specific exemption.[100] Title II of ECPA, known as the "the Stored Communication Act," provides protections for electronic communications not in transmission but in temporary storage as part of the communications process.

Although the term "e-mail" was not mentioned in the statute, Congress attempted to afford privacy protections to e-mail in part in response to an Office of Technology Assessment's 1985 report entitled "Electronic Surveillance and Civil Liberties." The report concluded "current legal protections for electronic mail are 'weak, ambiguous, or non-existent,' and that 'electronic mail remains legally as well as technically vulnerable to unauthorized surveillance."[101] Shortly thereafter, Congress took legislative action to afford electronic communications Fourth Amendment like protections noting:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations . . . But there are no comparable Federal statutory provisions to protect the privacy and security of communications transmitted by new non-common carrier communications services or new forms of telecommunications and computer technology . . . This gap [between postal privacy protections and new technology

[99] ECPA amended Title III of the Omnibus Crime Control and Safe Street Act of 1968 (The Wiretap Act).

[100] 18 USC § 2511(1)(a) proscribes "intentionally intercept[ing] . . . any wire, oral, or electronic communication", unless the intercept is authorized by court order or by other exceptions.

[101] Congress of the United States, Office of Technology Assessment, "Electronic Surveillance and Civil Liberties," NTIS Order #PB86-123239, 39, 1985, http://www.fas.org/ota/reports/8509.pdf.

> protections] results in legal uncertainty . . . It may also discourage American businesses from developing new innovative forms of telecommunications and computer technology.[102]

ECPA amended the federal Wire Tap Act to afford Fourth Amendment like protections to the fledgling realm of electronic communications. It did so by bestowing differing levels of procedural protections depending on the age of the communication, whether or not it has been "retrieved" or opened by the recipient, or whether it was in "electronic storage." The statute also required that notice be provided to the intended target depending on the level of legal process obtained or the age of the communications.

1. Confounded By ECPA

The enactment of ECPA reflects the evolution of Fourth Amendment and privacy jurisprudence to emerging communications networks. It, however, is the last major milestone of that evolution. More than 25 years have passed since ECPA; the Internet, which at that time was a toy of the Department of Defense, went public in the early 1990s, and society has embarked upon the Information Revolution. ECPA is antiquated. It is antiquated not only due to the tremendous passage of time moving at "Internet speed," but also because ECPA was antiquated the day it was enacted. The technological developments in Internet technologies, occurring at a brilliant speed, have created a conundrum for Fourth Amendment jurisprudence.

ECPA "is famous (if not infamous) for its lack of clarity,"[103] in large part because of the differing standards that both private entities and the government must meet to obtain access to electronic records. Courts have had difficulty applying consistent readings within each title of the Act. For example, while most courts agree that a lawful intercept of e-mail under Title I must be

---

[102] S. Rep. No. 99-541, Reprinted in 1986 U.S.C.C.A.N. 3555, 3564-65, 1986.

[103] *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994). *See also U.S. v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998) (stating that the 5th Circuit "might have put the matter too mildly"); Kerr, "Internet Surveillance Law After the USA Patriot Act. ("The law of electronic surveillance is famously complex, if not entirely impenetrable").

contemporaneous with the transmission of the communication, they have disagreed on whether an e-mail residing in 'transient electronic storage' prior to delivery is afforded procedural protections. Different federal courts of appeal have applied ECPA differently to an e-mail in storage while waiting to be downloaded from an e-mail server, while sitting in the cloud of a web based e-mail service, after being downloaded onto an individual's personal computer, after the e-mail has been opened, or when the e-mail is delivered by a commercial Internet service provider as opposed to a private corporate in-house e-mail service. Moreover, courts are just beginning to grapple with whether or not ECPA affords protections to communications occurring in social media and other cloud computing technologies that did not exist at the time of ECPA's enactment, and if so, how.

As forward looking as the statute was in 1986, it codified Congress' understanding of computer networks as they existed at the time, and has failed to consider advancements in technology.[104] Today, policy makers, legislators, judges, the law enforcement and intelligence communities, and the public are left with an antiquated statute that fails to provide clear standards for the application of Fourth Amendment. These safeguards contained within the statute are ill suited for today's Web 2.0 social networking and cloud computing technologies. Accordingly, the 5th Circuit described attempts to interpret ECPA as a "search for lightning bolts of comprehension [that] traverses a fog of inclusions and exclusions which obscures both the parties' burdens and ultimate goal."[105]

Many pages have been dedicated by experts to unpuzzle ECPA, and such, an exegesis does not need to be replicated in this thesis. In the following sections, the author provides a brief exploration of the statute to demonstrate its limitations and the quandary it has created for the modern digital environment.

---

[104] Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It." Neither ECPA's statutory language nor its legislative history makes any reference to the Internet. Lupu, "The Wiretap Act and Web Monitoring."

[105] *Briggs v. Am. Air Filter Co.*, 630 F.2d 414, 415 (5th Cir. 1980).

2. Title I: The Wiretap Act

Prior to the passage of ECPA, the federal Wiretap Act covered the interception of voice and wire communications. ECPA expanded the definition of communications to electronic communications including "signs, signals, writings, images, sound, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectric or photo-optical systems."[106] E-mail and web browsing are examples of electronic communications covered under this provision.

Generally, the statute prohibits the disclosure of a communications to anyone other than the intended recipient while it is in transmission. The intentional interception of a communication is also prohibited. The Wiretap Act is a law governed by exceptions; in this case, the relevant exceptions are that law enforcement may obtain access after first obtaining a court order, and parties to the communications can consent to disclosure (this becomes relevant to the Third Party Doctrine).[107]

3. Title II: The Stored Communications Act

The Stored Communications Act is the most complex of the three statutes. It governs how the government can obtain electronic communications in electronic storage with Internet service providers, such as Google, AOL and Yahoo. It provides standards for access by federal and state law enforcement, articulates permissible voluntary disclosure by Internet service providers for such things as routine network maintenance,[108] and establishes criminal penalties for

[106] 18 U.S.C. § 2510.

[107] See, generally, Robert Cannon, "ECPA Title I: The Wiretap Act: Exceptions," *Cybertelecom*, 2012, http://www.cybertelecom.org/security/ecpaexception.htm.

[108] An Internet service provider may voluntarily disclose non-content information to non-governmental entities. 18 U.S.C. § 2702(c)(6). However, voluntary disclosure to a governmental entity of content or non-content information is expressly prohibited. 18 U.S.C. § 2702(a).

the unlawful access to certain types of information.[109] The Stored Communications Act applies different standards to content, opened versus unopened communications, and two types of non-content data (basic subscriber[110] versus transactional).[111] The Stored Communications Act provides maximum protection to the content of electronic communications stored in public computing services reflecting Congress's judgment "that users have a legitimate interest in the confidentiality of communications in electronic storage."[112] The Stored Communications Act, however, does not apply to an "electronic communication [that] is readily accessible to the general public."[113]

As mentioned above, ECPA reflected Congress' mid-1980s understanding of computer networks. For example, ECPA reflects computer networks' "store-and-forward" architecture. While Title I of ECPA, the Wiretap Act, covers the "forwarding" part of computer communications, Title II, the Stored Communications Act, covers the "stored" part.[114] An e-mail could be transmitted across the network (Title I, Wiretap Act) and could be stored on a receiving e-

---

[109] See United States Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, "Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," 2009.

[110] Basic subscriber data includes: (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address (temporarily assigned network addresses would include IP numbers); and (F) means and source of payment for such service (including any credit card or bank account number). 18 U.S.C. § 2703(c)(2).

[111] Transactional data is the catch-all category for non-content data and includes: historical data, websites visited by user, or e-mail addresses with whom the user communicated.

[112] *Theofel v. Farley-Jones*, 341 F.3d 978, 982 (9th Cir. 2003) in which the court analogized the protections provided by the Stored Communications Act to those afforded by the law of trespass as follows: Like the tort of trespass, the Stored Communications Act protects individuals' privacy and proprietary interests. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, cf. Prosser and Keeton on the Law of Torts § 13, at 78 (W. Page Keeton ed., 5th ed. 1984), the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.

[113] 18 U.S.C. § 2511(2)(g). See e.g., Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 1220.

[114] This is a transitional storage pending delivery or further transmission of the message (it is not storage of the content after it has been received).

mail server (Title II, Stored Communication Act) pending download by the recipient. E-mail that remains stored but not accessed by the recipient for less than 180 days requires a warrant for access by law enforcement. After 180 days, an unretrieved e-mail is deemed abandoned and only an agency level subpoena is required.[115] If the e-mail is accessed by the recipient, but the e-mail remains on the Internet service providers' servers, law enforcement may obtain the e-mail with a mere subpoena provided that the subscriber receives prior notification; no notice is required if a warrant is obtained. If the message was downloaded and opened by the recipient, and resided on the recipient's personal computer, the government would be required to obtain a warrant premised upon probable cause to search and seize the physical personal computer in which the e-mail was stored. The convoluted contours of the Stored Communications Act's applicability to e-mail and Internet communications confounds even the most well versed ECPA experts.

Disclosure of non-content to anyone other than the government is permissible. A governmental entity may obtain basic subscriber information with a subpoena issued by a federal grand jury, a federal trial court, or where permitted by statute, an administrative subpoena.[116] No notice is required. Whereas, transactional data may be obtained by court order provided that the requestor can "offer specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic information or the records or other information sought are relevant and material to an ongoing investigation."[117] No prior notice is required.

ECPA also distinguishes between Electronic Communications Services (ECS) and Remote Computing Services (RCS), which creates additional technology centric procedural requirements. An ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic

[115] 18 U.S.C § 2510(17)(A).

[116] 18 U.S.C § 2703(c)(2).

[117] 18 U.S.C § 2703(c)(d).

communications."[118] Providers of e-mail (Internet Service Providers), telephone and text messaging services[119] that provide the ability to send and receive communications generally act as ECSs; whereas, RCS means the provision to the public of computer storage or processing services by means of an electronic communications system.[120] Generally, an RCS is provided by an off-site computer that stores or processes data for a customer.[121] A service provider that allows customers to use its computing facilities in "essentially a time-sharing arrangement" provides an RCS. Services that allow users to store data for future retrieval also provide an RCS.[122] However, an entity that operates a website and the services associated with it are not an RCS, unless it also offers storage or processing. In any case, an entity is only an RCS if it provides services to the public.

Although cloud computing services were not the norm at the time of ECPA's passage, many of the services provided by and stored in today's cloud would arguably be considered RCS for purposes of ECPA. However, how today's social networking technologies would be classified and what level of review is necessary to access transactional data or content may not be so easy to determine. For example, would an individual's Facebook profile be considered a communication transmitted by an ECS or rather would it be considered a computing service, and therefore, protected under the RCS? The tech centric provisions of ECPA make it difficult to apply to new and emerging social network technologies. Courts are just beginning to grapple with whether or not ECPA

---

[118] 18 U.S.C. § 2510(15).

[119] *See Quon v. Arch Wireless Operating Co*., 529 F.3d 892, 902-03 (2008) (holding that a text messaging service provider was an ECS, and therefore, not an RCS).

[120] 18 U.S.C § 2711(2). An electronic communication system is defined in the statute as: any wire, radio, electromagnetic, photooptical or phototelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

[121] See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564-65.

[122] See *Steve Jackson Games, Inc.,* 816 F. Supp. at 442–43.

affords protections to communications occurring in social media and other cloud computing technologies that did not exist at the time of ECPA's enactment.

In the case of *Quon v. Arch Wireless Operating Co*., the Federal Court of Appeals for the Ninth Circuit articulated its belief that a service provider could only be an ECS or an RCS, but not both.[123] The court's "either/or approach" is in contravention to Congressional intent.[124] The definitions provided in the statute were independent of each other. While no one will argue that a provider of e-mail services is an ECS, the legislative history suggests that since e-mails stored after transmission would be protected by the provisions of the Stored Communications Act that protect the contents of communications stored by an RCS, an ECS could become an RCS as well.[125] In *Flagg v. City of Detroit*, a federal district court adopted this reading of legislative intent by finding that a service provider "may be deemed to provide both an ECS and an RCS to the same customer."[126] The key to determining whether a social networking or cloud computing service provider is an ECS or an RCS is to ascertain what role it has played or is playing with respect to the electronic communication.

The government can compel disclosure of the contents of an electronic communications in the storage of an RCS or in the storage of an ECS for greater than 180 days in a number of ways: (a) with a warrant, no notice is required; (b) an administrative subpoena; (c) a grand jury subpoena; (d) a trial subpoena; or (e) a court order issued under Section 2703(d) if the government offers "specific and articulable facts showing reasonable grounds to believe" that the communications sought are "relevant and material" to an ongoing criminal investigation. The government's ability to obtain content information in the absence of a warrant premised upon probable cause negates an individual's

---

[123] *Quon*, 529 F.3d at 904-08 (finding reasonable expectation of privacy in pager messages stored by provider of communication service).

[124] See United States Department of Justice, 2009.

[125] See H.R. Rep. No. 99-647, at 65 (1986).

[126] *Flagg v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008).

reasonable expectation of privacy, which prompted Professor Orin Kerr to note, "[t]he most obvious problem with the current version of the Stored Communications Act is the surprisingly weak protection the statute affords to compelled contents of communications under the traditional understanding of ECS and RCS."[127]

4. Title III: Pen Register Act

Traditionally, a pen register would capture telephone numbers called from a specific number. The Supreme Court in *Smith v. Maryland* held that no actual expectation of privacy in phone numbers dialed exists.[128] Congress enacted the Pen Register Act to provide standards for access of transactional data associated with telephone calls and required the government to obtain a court order premised upon a showing that the information obtained is relevant to an ongoing investigation. Initially, the statute failed to state specifically that it applied to electronic communications transmitted on the Internet, which left many to struggle with ascertaining Congressional intent. Subsequently, Section 216 of the 2001 Patriot Act expanded the scope of a pen register to encompass Internet communications more clearly.[129] The Pen Register Act as amended, defines pen registers as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication."[130]

---

[127] Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 1233.

[128] 442 U.S. 735 (1979).

[129] 18 U.S.C § 3122(c).

[130] 18 U.S.C. § 3127(3).

A court order must be obtained to use a pen register or a trap and trace device. The application for the order must be made by "an attorney for the government" and not the individual law enforcement office. The application must demonstrate that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency.[131]

The Pen Register Act has failed to keep pace with advancements in technology with respect to locational data generated by cell phone and other mobile devices. Cell phones generate locational data transmitted to the nearest cell phone towers. Cell phones towers capture location data in the course of providing service to users. As more and more individuals use their cell phones to access social networking technologies, a constant record of their geographical whereabouts is created. The Pen Register Act did not adequately articulate a standard for governmental access to this type of information, in part because at the time of the Act's passage, cell phone use was extremely limited. At the time of the passage of the Act, only 913 cell phone towers existed as compared to approximately 251,000 today.[132] Currently, a cell phone can be used as a tracking device capable of recording the coming and goings of an individual. Many, therefore, believe that governmental access to locational data generated by cell phones amounts to a search and seizure necessitating a warrant and further illustrating the need to update ECPA to account for the advancement in cell phone technologies.[133]

---

[131] 18 U.S.C § 3122(b).

[132] See *In re Application of the United States of America for Historical Cell Phone Data Site Data*, 747 F.Supp.2d 827 (S.D. Tex. 2010).

[133] Ibid. District Court ruling that warrant is necessary to obtain cell phone location as it is more intrusive than mere GPS data. This ruling is not universally followed throughout the United States However, the recent Supreme Court ruling in *U.S. v. Jones*, January 23, 2012, that law enforcement's use of a GPS tracking device on a suspect's car without a warrant is unconstitutional, it is likely to be persuasive in future law enforcement requests for access to cell phone locator information.

M. THE USA PATRIOT ACT

The USA Patriot Act amended portions of ECPA and greatly facilitated the government's ability to obtain access to telephone, e-mail communications, medical, financial, and other records, eased restrictions on foreign intelligence gathering within the United States and expanded the use of National Security Letters that allows the FBI to search telephone, e-mail, and financial records without a court order.[134] Further, it permitted the delay in notification to the subject of the search, and in some cases, no notice at all.

Note that unlike other milestones in the history of Fourth Amendment jurisprudence, the Patriot Act did not increase privacy protections, nor did it increase restrains or checks on governmental access and gathering of information.[135]

[134] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001.*

[135] See, generally, Robert Cannon, "The Patriot Act," *Cybertelecom*, 2012, http://www.cybertelecom.org/security/patriot.htm.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. "SUBTLER AND MORE FAR-REACHING MEANS OF INVADING PRIVACY"[136]

In the 25 years since ECPA was enacted, the World Wide Web was invented, the Internet was made public by the National Science Foundation, Google was invented, the Dot Com boom and bust occurred, and social networks and interactive media have exploded. Most significantly, sufficient time has transpired that a new generation known as Digital Natives has lived their entire lives online. These revolutions in communications have rendered antiquated a Fourth Amendment jurisprudence developed in the era of the AT&T telephone monopoly.

A. WEB 2.0—SOCIAL MEDIA

Technological enhancements of Internet technologies have occurred at break neck speed. Initially, Web 1.0 technology enabled anyone with minimal technical ability to publish to a webpage and communicate the message to everyone. Web 2.0[137] revolutionized the way people communicated with one another by permitting individuals to interact with Internet sites in a collaborative

[136] Justice Brandeis in the pivotal *Olmstead* dissenting opinion foreshadowed a time when developments in technology would enable far reaching means of governmental surveillance: Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. Moreover, 'in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be.' The progress of science in furnishing the government with the means for espionage is not likely to stop with wiretapping. Ways may someday 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. *Olmstead v. United States*, 277 U.S. 438 (1928).

[137] The Pew Internet and American Life Project defines Web 2.0 as "an umbrella term used to refer to a new era of web-enabled applications built around user-generated or user-manipulated content, such as wikis, blogs, podcasts, and social networking sites." Aaron Smith, "Web 2.0," *The Pew Internet and American Life Project*, November 15, 2011, http://www.pewinternet.org/topics/Web-20.aspx. The term Web 2.0 was coined during a braining storming conference between Tim O'Reilly and Media Live International. Initially, it signified a resurgence of the Internet after the Dot.com boom and had nothing to do with the emerging technological capabilities. However, the term quickly took hold. See Tim O'Reilly, "What is Web 2.0. O'Reilly Media," September 30, 2005, http://oreilly.com/web2/archive/what-is-web-20.html.

manner and enabling the creation of “user generated content.” With the advent of Web 2.0 technology, everyone can contribute, create, collaborate, and curate content. Finally, the growing popularity and adaption of cloud computing has transformed information technology, moving both content and applications from the desk top computer, secured within an individual’s private home or business, to third party server farms located in undisclosed destinations.

Social networking technologies allow participants to meet others online and form communities with individuals who possess similar interests. Just as importantly, research has demonstrated that social media is also an effective tool to maintain connections with existing friends and family.[138]

The first modern day social networking services that enabled users to create profiles, to accumulate friends and to surf their friends profiles was launched in 1997. SixDegrees.com attracted millions of users but failed to maintain itself as a business.[139] Friendster was the next major social networking service to come on the scene in 2002. Friendster only permitted users to gain access to profiles of people no more than four degrees away, which resulted in users friending people they did not know to expand their access. However, technical difficulties due to its rapid growth in popularity and a rumor that it would soon collect fees caused users to jump ship to the emerging Myspace.com. By 2004, MySpace gained popularity with teenagers with its policies that permitted minors to use its services.[140] Also in 2004, Facebook came on to the scene with its introduction to students on the campus of Harvard. In 2005, Facebook

[138] The Pew Internet and American Life Project found that “two-thirds of adults online use social media like Facebook, Twitter, MySpace and LinkedIn, primarily to maintain connections to friends and family.” Further, 91% of teens use social networking technologies to connect with existing friends. Amanda Lenhart and Mary Madden, “Teens, Privacy & Online Social Networks.” *Pew Internet and American Life Project,* April 18, 2007, http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx.

[139] danah boyd and Nicole Ellison, “Social Network Sites: Definition, History and Scholarship,” *Journal of Computer-Mediated Communication* 13, no. 1, (2007): art. 11, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.htm.

[140] Ibid., art. 8.

became available to high school students around the country. Today, Facebook is the most popular social networking service with more than 845 million users worldwide.[141]

Social media is an umbrella term that includes many different technologies. The following is a brief discussion of some of the more popular types of technologies and services in use today. Technologies may provide multiple functionalities.

1. Content Sharing—Allows participants to share different types of media. These tools enable users to generate and share "User Generated Content." [142] Examples include Youtube for sharing videos, Flickr for sharing photos and Deviant Art for sharing art.
2. Discussion—Text messaging, video chatting/ conferencing. Examples include Yahoo messenger, Google talk and Skype.
3. Social Networks-—perhaps the most commonly used social networking technology. Examples include Facebook, MySpace, Linkedin and Google+.
4. MicroBlogging—Mini publishing that enables quick and frequent sharing and has helped to provide officials and the public with on the ground situational awareness during natural emergencies, such as the earthquake and tsunami in Japan, as well in man-made emergencies, such as the uprisings in Iran and Egypt. Examples include Twitter, which is limited to 140 characters and Tumblr.
5. Location-based networks—Used for reviewing businesses, as well to report and track an individual's attendance at a site. Examples include Four Square and Yelp.
6. Social Games—Stand-alone or applications on other social network platforms. Examples include Farmville and Mob Wars.
7. Virtual Worlds—Online environments that make it possible to create personalities or avatars, and interact with other personalities or avatars. Examples include Second Life, There and Imvu.

---

[141] Facebook, (n.d.). "Statistics," http://www.facebook.com/press/info.php?statistics.

[142] According to the Organization of Economic Cooperation and Development, User Generated Content must possess three salient characteristics: (1) It must be published on a website or social networking site available to selected group of people; (2) it needs to show a certain amount of creative effort; and (3) it needs to have been created outside of professional routines and practices. Organization of Economic Cooperation and Development, "Participative Web: User-generated content. OECD Committee for Information, Computer and Communications Policy report, DSTI/ICCP/IE(2006)7/FINAL," April 2007, http://www.oecd.org/dataoecd/57/14/38393115.pdf.

8. Massive Multiplayer Online Games—Combination of social games and virtual worlds. Usually a common goal or community exists in which participants can interact with one another. Examples include World of Warcraft, Webkinz and Club Penguin.[143]

Social networking services typically permit individuals to create profiles for themselves. These profiles may contain personal information, as well as the lists of "friends" or others that they maintain contact with online. Many services enable users to exercise some measure of control over those they chose to share their profiles by invoking available privacy settings. Regardless of the privacy settings a user selects, service providers, pursuant to their "terms of use" agreements, often retain the ability to access and collect user's data so that they can deliver targeted advertising to the user, and thus, can raise revenues to sustain its operations. Typically, these agreements are lengthy, complicated, and difficult to understand, which casts doubt on whether users are providing meaningful consent.[144] Prof. Lorrie Cranor noted, "[o]nline privacy policies are difficult to understand. Most privacy policies require a college reading level and an ability to decode legalistic, confusing, or jargon-laden phrases."[145] Buried within the terms of use agreements is frequently language in which providers include their policies for responding to requests from law enforcement.[146] Privacy disclosure policies vary from site to site.

---

[143] O'Neill Communication, "All the Different Types of Social Media," (n.d.), http://www.oneillcommunications.com/2010/04/all-the-different-types-of-social-media/.

[144] See Aleecia M. McDonald and Lorrie F. Cranor, "The Cost of Reading Privacy Policies," *ACM Transactions on Computer-Human Interaction* 389, no. 3 (2008): 1, http://www.mendeley.com/research/the-cost-of-reading-privacy-policies/. Calculating that if all the privacy policies encounter in a year are read, it would take 76 work days, or on a national basis of work hours, a cost in terms of work hours $54 billion.

[145] Lorrie F. Cranor, Patrick Gage Kelley, Aleecia M. McDonald, and Robert W. Reeder, "A Comparative Study of Online Privacy Policies and Formats," *Lecture Notes in Computer Science*, 5672/2009, 37-55, DOI: 10.1007/978-3-642-03168-7_3, 2009, http://www.springerlink.com/content/e2640gw68436054k/.

[146] See Facebook, "Information for Law Enforcement Authorities," 2012, https://www.facebook.com/safety/groups/law/guidelines/.' See also Google, "Privacy Policy," 2012, https://www.google.com/intl/en/policies/privacy.

Both Facebook and Google provide notice of their policy with respect to disclosure to the government:

- For legal reasons: We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
    - meet any applicable law, regulation, legal process or enforceable governmental request.
    - enforce applicable Terms of Service, including investigation of potential violations.
    - detect, prevent, or otherwise address fraud, security or technical issues.
    - protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

The control and collection of data pertaining to an individual is an aspect of the expectation of privacy in cyberspace that is the subject of a huge debate currently occurring in Congress, academia, corporate boardrooms, and homes across this country.[147] Although the Third Party Doctrine would arguably negate an individual's reasonable expectation of privacy in communications occurring in social media, courts are beginning to consider whether or not an individual has invoked available privacy settings in determining whether an individual intends personal communications to be private.[148]

[147] Although not considered within this thesis, it should be noted that currently a raging debate is going on about whether an individual is entitled to consumer privacy or control over personal information in the custody of third party service providers. This debate prompted the White House to propose a privacy framework for consumer data. It should be noted that unlike like the government, third party service providers are not bound by Constitutional restraints. See The White House, "Consumer Data Protection in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Digital World Economy," February 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[148] *Crispin v. Audigier*, 717 F.Supp.2d 965 (2010). In a case of first impression, a district court held that the Stored Communications Act does afford protections to private communications occurring in social media and shielding the contents from disclosure in a civil matter. The court dismissed the suit pending an examination of whether the generator of the content provider invoked available privacy protections, and thus, evidenced an expectation of privacy. The district court decision is not binding on other courts

Finally, in the very near future, Internet technologies will evolve to a new level with the advent of Web 3.0 technologies and "the semantic web,"[149] a term coined by one of the original pioneers of the Internet, Sir Ted Berners-Lee. The extent of the new functionalities that will become available with Web 3.0, or the semantic web, is still unknown. However, they will most likely enable machines to read web pages to better tailor the computing experience for the user. While some theorize that if constructed properly, privacy considerations can be can embed into emerging Web 3.0 technologies (privacy by design), others fear that the consolidation of so much data will make surveillance much easier.

1. Cloud Computing

Social media is enabled by the availability of remote computing resources owned and operated by third party service providers. The concept of cloud computing or the ability to leverage computer services and storage on remote systems is not a new concept. The developers of the ARPANET, the first packet switched network that evolved into the early Internet, envisioned the concept. Larry Roberts, one of the early pioneers of the ARPANET, predecessor to the Internet, described the ARPANET as follows:

> The data sharing between data management systems or data retrieval systems will begin an important phase in the use of the Network. The concept of distributed databases and distributed access to the data is one of the most powerful and useful applications of the network for the general data processing community. As described above, if the Network is responsive in the human time frame, databases can be stored and maintained at a remote location rather than duplicating them at each site the data is needed. Not only can the data be accessed as if the user were

[149] The Semantic Web, a collaborative effort of W3C and industry partners, "provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries." See W3C, "W3C Semantic Web Activity," 2011, http://www.w3.org/2001/sw/.

> local, but also as a Network user he can write programs on his own machine to collect data from a number of locations for comparison, merging or further analysis.[150]

Internet protocols were developed to enable ARPA-funded researchers to share computer resources and research. Web 2.0 technologies merely created a new demand for bigger and better remote servers that gave birth to a new market of private and public sector services.

The National Institute for Standards and Technology has defined cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[151] It provides "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction."[152]

Cloud computing has enabled individuals to store more and more data on remote third party services located in "the cloud," as well as to perform computing tasks remotely. Today, individuals conduct their banking online utilizing services located in the cloud. In addition, graduate and other students can compose and store their work product remotely in the cloud. The storage of data on third party servers has resulted in new challenges to an individual's ability to maintain control of data, which calls into question privacy concerns not addressed by outdated laws.

---

[150] Lawrence G. Roberts and Barry D. Wessler, "Computer Network Development to Achieve Resource Sharing," *Proceedings of AFIPS*, 1970, http://www.packet.cc/files/comp-net-dev.html.

[151] Tim Grance and Peter Mell, "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," *National Institute of Standards and Technology, Special Publication 800-145*, September 2011.

[152] Tim Grance and Wayne Jancen, "Guidelines on Security and Privacy in Public Cloud Computing," *National Institute of Standards and Technology, National Institute of Standards and Technology, Special Publication 800-144,* December 2011.

Pursuant to the Third Party Doctrine, from the 1968 *Katz* Supreme Court case, should the privacy protection for what used to be contained in an individual's private papers be diminished because they are now stored in the desk of another, i.e., a cloud provider? Or does an individual's actions (establishing password protections and setting privacy settings) manifest the content owner's reasonable expectation of privacy as envisioned in *Katz*? David A. Couillard in "Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing" suggests that cloud service providers should be viewed as "virtual landlords."[153] Although a user may be interacting with a service provider when utilizing online calendars, photo storage, document storage, or blogging services, it is not the intent of the user to provide access to the content with the provider. "The provider is merely providing a platform for using and storing the content via the cloud." In the same way that a tenant does not expect that a lock will keep out a landlord, neither will the use of a password; rather, it is the operation of applicable law that ensures the privacy of an individual.[154]

Nonetheless, in light of the judicially recognized Third Party Doctrine, an individual's expectation of privacy for computing activities occurring and stored in third party cloud computing services is all but non-existent. While an e-mail stored on a home computer would be fully protected by the Fourth Amendment warrant requirement, an e-mail or other digital communications stored on a remote, cloud computing server may not be.[155] In an era in which more and more commercial entities are storing their clients' information in the cloud or inviting their clients to do so, some have asserted that the diminished expectation of privacy that comes from the ease by which authorities or others can access

---

[153] David A. Couillard, "Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing," *Minnesota L. Rev., 93, 101*, June 2009, SSRN: http://ssrn.com/abstract=1832982.

[154] Kristopher Nelson, "Applying the United States Fourth Amendment to Data in the Cloud," *Social Media Today*, January 20, 2010, http://socialmediatoday.com/index.php?q=all/14232.

[155] EPIC, "Electronic Communications Privacy Act-Reform," (n.d.), http://epic.org/privacy/ecpa/default.html.

personal information may have a chilling effect on societal tolerance of having their data stored by commercial entities in the cloud. In Congressional testimony on the need to amend ECPA, Professor Kevin Werbach remarked that "cloud computing represents a new stage in the evolution of that economy" and for it to be successful, "a smooth transition to cloud computing requires users to continue feeling a sense of trust online." He noted further, "though it is fashionable to assert that today's young people are unconcerned about privacy, research shows that in many ways they feel even more strongly about the need to control their personal information than their elders."[156]

2. Privacy and Social Media

Privacy as a concept has always been difficult to define. As history has demonstrated, societal notions of privacy are not always in alignment with Constitutional notions of privacy. Little consensus exists on an exact meaning.[157] In 1967, Prof. Alan Westin declared "few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists."[158] Prof. Daniel Solove declared, "[p]rivacy is a concept in disarray."[159] "Privacy seems to be about everything and therefore it appears to be about nothing."[160] While danah boyd asserts that privacy "is about how people experience their relationship with others and with information. Privacy is a sense of control over information, the

[156] *ECPA Reform and the Revolution in Cloud Computing*.

[157] Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania L. Rev.* 154, no. 3 (January 2006): 477–479, *GWU Law School Pub. L. Research Paper No. 129.* SSRN: http://ssrn.com/abstract=667622.

[158] Westin, *Privacy and Freedom*, 7.

[159] Solove, "A Taxonomy of Privacy," 477.

[160] Ibid., 479.

context where sharing takes place, and the audience who can gain access. Information is not private because no one knows it; it is private because the knowing is limited and controlled."[161]

However defined, privacy is a cherished value critical to a free society. With the advent of the Internet, and subsequently, with social networking technologies, the concept of privacy and an individual's "reasonable expectation of privacy" as recognized in *Katz* are on a collision course. Despite the collaborative nature of social networking technologies, researchers have debunked the notion that users of these services have no reasonable expectation of privacy, ala, the first prong of the *Katz* test. Young people, as early adopters and the most active users of social media,[162] have demonstrated their desire to shield their information from unwanted attention by employing a variety of methods, while others of all ages have chosen to engage in anonymous activities online or have elected to use pseudonyms and encryption techniques to effectuate privacy. It has become commonplace to achieve some level of privacy by concealing personal information, avoiding providing information pursuant to unnecessary inquiries, or, when forced to provide answers, simply lying. While courts struggle to determine what level of protections communications occurring in social media should be afforded, individuals have worked hard at creating walls around information in an attempt to exclude unwanted eyes.

3. Digital Natives and Privacy

One segment of the population worthy of note is that which has become known as the "Digital Native. ""Digital Natives" are those who were born into and raised in a digital world and who are "native speakers' of the digital language of

[161] danah boyd, "Facebook's Privacy Trainwreck," *Convergence: The International Journal of Research into New Media Technologies* 14, no. 1 (2008): 13, http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf.

[162] Mary Madden and Aaron Smith, "Reputation Management and Social Media," *Pew Internet and American Life Project*, May 2010, http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx. .

computer, video games, and the Internet."[163] Today, young people are living their lives in cyberspace mediated by social networking technologies. danah boyd, an ethnographer and social media researcher, has conducted extensive research on the online habits of today's youth, has written about their online practices, social behaviors, and expectations of privacy, and how they attempt to manage it as they navigate through cyberspace. In a two and half year ethnographic study of American teens' engagement with social network sites, she examined their habits online, how they socialized with their peers and how they navigated their way through adult society. She observed that teens used social media to gossip, flirt, joke around, share information, and to simply hang out.[164] Their activities in social networking site created a "networked public" defined as: (1) the space constructed through networked technologies, and (2) the imagined community that emerges as a result of the intersection of people, technology, and practice.[165] Further, she asserts that the networked public supports many of the same activities as "unmediated publics." Further, boyd notes that four unique properties and three dynamic properties emerge from their structure, which are persistence, searchability, replicability, and scalability of information posted in social media sites and three dynamics that arise from online social interactions, which are invisible audiences, collapsed contexts, and the blurring of public and private.[166] These attributes test the notion of privacy in ways not previously imaginable.

boyd's research has debunked the prevailing notion that young people do not care about privacy, for if they did, why would they portray so much information about themselves on Facebook? She argues that young people very much care about their privacy and have developed elaborate strategies to create

---

[163] Prensky, "Digital Natives, Digital Immigrants."

[164] danah boyd, "Taken Out of Context: American Teen Sociality in Networked Publics," *Dissertation, University of California, Berkeley*, 2008, http://www.danah.org/papers/TakenOutOfContext.pdf.

[165] Ibid.

[166] Ibid.

a sense of privacy in the networked world. “All teens have a sense of privacy, although their definitions of privacy vary widely.”[167] “They believe that privacy has to do with their ability to control a social situation, how information flows and where they can be observed by others.”[168] boyd notes that young people accept that they are being watched.[169] Many even enjoy the attention they receive. Nevertheless, they are concerned about the ability of others to hold any control over them and struggle to maintain agency over their online presence.

Young people employ various techniques to effectuate a semblance of control over information pertaining to them generated, communicated and stored in social media. boyd notes the complexities involved with doing so in cyberspace declaring:

> privacy is not about structural limitations to access; it is about being able to limit access through social conventions. This approach makes sense if you recognize that networked publics make it nearly impossible to have structurally enforced borders. However, this is not to say that teens do not also try to create structural barriers.[170]

Young people have adopted ingenious methods to restrict access by fabricating pertinent personal information, as well as by controlling with whom they wish to be friends. boyd notes that teens have crafted two types of strategies to effectuate control, and therefore, arguably a semblance of privacy over their information. The first is structural. Teens limit access by controlling to whom they provide access and by deleting content. They may also seek to

---

[167] boyd and Marwick, “Social Privacy in Networked Publics.”

[168] Ibid., 5.

[169] Ibid., 21. boyd notes that “the complexity of achieving privacy in networked publics has motivated countless teens to act assuming that they are being surveilled.”

[170] danah boyd, “Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life,” in *MacArthur Foundation Series on Digital Learning—Youth, Identity, and Digital Media Volume*, ed. David Buckingham, Berkman Center Research Publication No. 2007–16, The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning (Cambridge, MA: MIT Press, 2007), 31, http://ssrn.com/abstract=1518924.

employ more strategic techniques by limiting access to the message itself, using coded language (a form of social steganography),[171] or hiding in plain sight.[172]

However, teens have a more limited view of from whom they are trying to safeguard their information. They believe that by setting their privacy settings, they are restricting access to strangers and to eavesdroppers. They are often unaware of the extent to which third parties may access their online content.[173] Teens are not always cognizant that their information is constantly accessed by and monetized by social media sites and the firms with whom they conduct business and, depending on the provider's terms of use agreements, may be provided pursuant to a request from law enforcement.

John Palfrey and Urs Gasser in *Born Digital* assert that digital natives who have lived their lives "mediated by digital technologies"[174] face increasingly more difficulty with protecting their privacy as information pertaining to them is compiled in what they call "digital dossiers." In the absence of Congressional action, the level of process necessary for the government to obtain information stored in these third-party digital dossiers has the potential to negate any expectation of privacy young people and their older counterparts have in their digitally stored information, which is becoming more and more problematic as more information is captured and stored in cyberspace.

Finally, the disclosure of personal information that an individual has taken affirmative steps to protect and subjectively believes will remain private can result in harm to an individual's sense of dignity. Michael Zimmer, in "But the Data is Already Public," examined the ethical issues and the impact to the expectation of privacy stemming from the release of personal information data researchers had

---

[171] Steganography is defined as the art and science of hiding information by embedding messages within other, seemingly harmless messages. Webopedia, "Steganography," (n.d.), *Webopedia Computer Dictionary*, http://www.webopedia.com/TERM/S/steganography.html.

[172] Boyd, "Why Youth (Heart) Social Networking Sites."

[173] Ibid.

[174] Palfrey and Gasser, *Born Digital*, 53.

collected from Facebook accounts of the entire student body at Harvard.[175] The researchers had obtained access to this information through the cooperation of the university but without obtaining permission from any of the students. The researchers removed basic personal identifiers, such as name and identification numbers of their subjects, prior to the publication of thief findings in an article entitled "Tastes, Ties, and Time," "a cultural, multiplex, and longitudinal social network dataset."[176] Distribution of the findings was limited to fellow researchers. Within a few days, much of the data had been de-anonymized[177] and the identities of many of the students were ascertained. The researches maintained that they had not committed any ethical violations, betrayed any trust nor diminished any of the students' privacy interests as the information had already been voluntarily posted by the students on a social networking site. Zimmer's account of the researchers' use and release of the data set examined the expectation of privacy held by the students, many of whom had set their privacy settings set to limit the disclosure of their postings. Zimmer dismissed the researchers' argument that their actions were nothing more intrusive than had they sat in a town square observing the comings and goings of people. In a town square, encounters are random, whereas the researchers had accessed a complete targeted demographic group. Further, Zimmer considered the concept of harm and dignity based view of privacy. He noted that even though information had been "de-identified," was provided only to fellow academics that agreed to limit the use of the information, and had not been the subject of a hacker, "merely having one's personal information stripped from the intended sphere of the social

---

[175] Michael Zimmer, "But the Data Is Already Public: On the Ethics of Research in Facebook," *Springer Science Business Media* 12, no. 4 (2010): 321. http://www.springerlink.com/index/q1v7731u26210682.pdf.

[176] Kevin Lewis, Jason Kaufman, Marco Gonzalez, Andreas Wimmer, and Nicholas Christakis, "Taste, Ties and Time," *Berkman Center for Internet & Society*, September 25, 2008, http://cyber.law.harvard.edu/node/4682.

[177] See Latanya Sweeney, "Simple Demographics Often Identify People Uniquely," *Carnegie Mellon University, Data Privacy Working Paper 3*, 2000, for just how easy it is to de-anonymize anonymized data. With just three personal identifiers, gender, birth date and 5 digit zip code, 87% "(216 million of 248 million) of the population in the United States had reported characteristics that likely made them unique."

networking profile, and amassed into a database for external review becomes an affront to the subject's human dignity and their ability to control the flow of their personal information." [178] Zimmer's analysis provides additional support to demonstrate that even though young people utilize the third party services of social media to communicate their thoughts and beliefs, their election of privacy settings demonstrated their expectation of privacy.

4. Techniques That Enable Users to Assert a Semblance of Control Over Online Communications—Anonymity and Pseudonymity

The ability to participate in civil society without fear of governmental reprisal is a fundamental democratic principle. Individuals who feared harm or retribution for the expression of their ideas have long employed anonymous and pseudonymous techniques. Anonymity or pseudonymity can enhance an individual's ability to participate in the democratic process by serving as a "shield from the tyranny of the majority," and as such, is protected by the First Amendment.[179] It can also equalize factors that can diminish an individual's credibility, such as race, religion, or age. A number of prominent Founding Fathers chose to publish what would become the blue print for the fledgling new government in the Federalist papers. They did so under the pseudonym of Publius.

Tracking and monitoring technologies available today enable the government to collect large volumes of information about an individual's activities in social media. In the absence of updated laws and policies to ensure Fourth Amendment like protections for communications occurring in social media,

---

[178] Zimmer, "But the Data Is Already Public," 321.

[179] See *McIntyre v. Ohio*, 514 U.S. 334 (1995) in which the Supreme Court opined anonymity: exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation - and their ideas from suppression - at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse. See *Abrams v. United States*, 250 U.S. 616, 630-31 (1919) (J. Holmes, dissenting).

individuals may feel constrained in exercising their freedom of expression when knowing that their thoughts and ideas could be monitored, scrutinized, and retained long term. Tools enabling anonymous communications in cyberspace, as well as the use of pseudonyms, can empower individuals to express their views more freely.

Today, communicating online anonymously or behind the cloak of a pseudonym, can protect an individual from unwarranted governmental scrutiny.[180] Recently, tools enabling anonymous communication in cyberspace have been used throughout the world to enable political dissidents to communicate with the outside world without fear of discovery or reprisal from their home governments. Repressive regimes, such as China, Iran, Burma, Vietnam and several Middle Eastern countries, are censoring Internet communications and search results, jailing journalists and activists, and imposing laws that restrict online discourse and access to information.[181] Threats to Internet freedom are growing in number and complexity.[182] Repressive regimes, such as China and Iran, have developed their own methods for curtailing their citizens' access to the Internet, requiring dissidents to engage in a dynamic game of cat and mouse, altering their methods of access, and staying one step ahead of government detection. Anonymity provides an individual protection from the threat of peril or physical harm. Similarly, anonymity provides individuals in the United States a method to communicate without fear of reprisal or public ridicule fostering democratic ideals by enabling individuals who otherwise would not feel comfortable engaging in speech that may be controversial or just plain embarrassing.

---

[180] Jisuk Woo, "The Right Not To Be Identified: Privacy and Anonymity in the Interactive Media Environment," *New Media & Society* 8, no. 6 (2006): 949–967, http://www.forum.newmediaandsociety.com.

[181] See Reporters Without Borders, "Enemies of the Internet: Countries Under Surveillance," March 12, 2010, http://en.rsf.org/IMG/pdf/Internet_enemies.pdf.

[182] Department of State, "Internet Freedom, About Internet Freedom at the State Department," Remarks by Secretary of State Hillary Clinton, February 15, 2011, http://www.state.gov/e/eeb/cip/netfreedom/index.htm.

The use of a pseudonym on social media sites is another way individuals can communicate without fear of discovery or reprisal. Pseudonymity is the practice of keeping an identity private and unlinked and may include the use of fictional names or identities. Pseudonyms provide a mask to hide behind and enable individuals to explore their boundaries in cyberspace without fear of being discovered. The use of pseudonyms provides a structural protection for an individual's privacy that may not otherwise be assured.[183] Pseudonyms have been used throughout history by many notable individuals to produce writings or works of art without fear of political, religious, or social reprisal. In the 18th century, James Madison, Alexander Hamilton, and John Jay wrote under the name of Publius and published *The Federalist Papers.*[184] In 19th century England, the Brontë sisters published under pseudonyms to obtain credibility in their work during a time in history when women were not taken seriously.

The use of these techniques is not without shortcomings. In as much as anonymity and pseudonymity provide individuals with the courage to express opinions they may not otherwise feel free to voice, these tools can also be used for disreputable purposes. Hiding behind the cloak of invisibility can provide bad actors a license to plan acts of terrorism or other criminal activities[185] with apparent impunity. The actions of Internet hactivists,[186] such as Anonymous and

---

[183] See Jillian C. York, "The Right to Anonymity Is a Matter of Privacy," *Electronic Freedom Foundation*, January 28, 2012, https://www.eff.org/deeplinks/2012/01/right-anonymity-matter-privacy.

[184] See Chris Whitten, "The Federalist Papers," *FoundingFathers.Info*, 2010, http://www.foundingfathers.info/federalistpapers/. John Jay, Alexander Hamilton and James Madison are reputed to have authored the Federalist papers, a collection of 85 essays outlining a proposed structure for the operation of the nascent U.S. government, under the pseudonym of Publius.

[185] Lyrissa B. Lidsky, "Anonymity in Cyberspace: What Can We Learn from John Doe?" University of Florida Levin College of Law Research Paper No. 2009-37, *Boston College L. Rev.* 50 (2009): 1.

[186] Hactivism is defined by Dorothy E. Denning in "Activism, Hactivism and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy" as the use of hacking techniques against targeted Internet sites with the intent of disrupting normal operations but not causing serious damage. Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy, In *Networks and Net Wars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David F. Ronfeldt (RAND, 2001).

LulzSec, have presented challenges to the law enforcement community. Cyber-bullying and anonymous hate-mail can also be facilitated by the ability to communicate anonymously. Nevertheless, free speech must always be balanced against potential harms to society at large.[187]

However, true anonymity is difficult to achieve. In today's technological environment, an individual's true identity may be difficult to hide. Internet Protocol (IP) addresses in and of themselves can tell a lot about a user. Each computer on the Internet is assigned a unique address somewhat similar to a street address or telephone number. The IP address is captured by every computer or server that a user connects with and can be traced.[188]

Proxy servers, such as TOR (The Onion Router), have been utilized by individuals seeking to communicate their opinions without fear of surveillance or detection.[189] "TOR is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet." [190] TOR works by transmitting an encrypted message through participating nodes on the TOR network so that a message's origins are obscured. However, proxy servers are not fool proof and can be defeated, and thus, enable the identity of the sender to be compromised.[191]

The Internet has always provided individuals with the opportunity to express themselves anonymously or behind the cloak of a pseudonym. At the

---

[187] *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

[188] See Russ Smith, "IP Address: Your Internet Identity," *Consumer.Net*, March 29, 1997, http://www.ntia.doc.gov/legacy/ntiahome/privacy/files/smith.htm.

[189] See Ingmar Zahorsky, "Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum," *University for Peace, Peace and Conflict Monitor*, August 1, 2011, http://www.monitor.upeace.org/innerpg.cfm?id_article=816.

[190] See TOR Project, (n.d.), http://www.torproject.org.

[191] See Kevin Bauer, Dirk Grumwald, Tadayoshi Kohno, Damon McCoy, and Douglas Sicker, "Shining Light in Dark Places: Understanding the TOR Network," August 7. 2007, http://www.cs.washington.edu/homes/yoshi/papers/Tor/PETS2008_37.pdf; Bruce Schneier, "Lessons from the TOR Hack: Anonymity and Privacy Are Not the Same," *Wired News*, September 20, 2007, http://www.wired.com/politics/security/commentary/securitymatters/2007/09/security_matters_0920?currentPage=all.

same time, with more and more terrorist and other criminal actors using the Internet in furtherance of their nefarious aims, anonymity and psuedonymity have made surveillance of the electronic communications more difficult for the law enforcement and intelligence communities. Striking the right balance between techniques that facilitate the ability to participate in the democratic process against the need to keep this nation safe from acts of terrorism or other criminal actions is becoming increasingly more important.

5. Delete Button—The Right to be Forgotten

One of the intriguing debates about privacy currently underway is whether an individual should have the right to have information pertaining to himself deleted from the Internet and other repositories of personal information, and whether a "delete" option is even possible. The ability to delete posted information, or to limit the retention period of pertinent information that others have captured after the initial justification for its capture in no longer valid, is another method for asserting control over personal information and for achieving a semblance of privacy. In particular, many believe that young people who may not always have the wisdom to understand the enduring nature of communications online, should be permitted to redact, or otherwise, limit information pertaining to themselves.[192]

During World War II, the Europeans learned the hard way the harm that can come from the collection of information about its citizens. Due to the population registries maintained by the Dutch and other countries that collected an individual's name, birth date, address, and religion, the Nazis were able adeptly to locate tens of thousands of Jews for transfer to the death camps.[193] Due to the painful lesson of the 20th century, the European Union is currently considering the ability to delete an individual's information online. As such, on

[192] See *Do Not Track Kids Act of 2011*, HR 1895.

[193] See Viktor Mayer-Shonberger, *Delete the Virtue of Forgetting in the Digital Age* (Princeton: University Press, 2009).

January 25, 2012, the European Commission proposed an amendment to the 1995 Data Protection Directive 95/46/EC[194] which, if adopted, would provide an individual the "Right to Erasure."[195] Article 16 of the proposed Amendment provides as follows:

> Right to erasure
>
> 1. Member States shall provide for the right of the data subject to obtain from the controller the erasure of personal data relating to them where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (e), 7 and 8 of this Directive.
> 2. The controller shall carry out the erasure without delay.[196]

The impact of the proposal will undoubtedly greatly influence information flows as more and more information is being stored in the cloud outside of the territorial boundaries of both service providers and the individual to whom the information pertains.

While the delete option presents an appealing prospect for limiting the retention of digital communications, the technological feasibility of the concept is doubtful. By its nature, communications occurring in social media can be stored in a multitude of locations, some intentionally and others unintentional. At a minimum, it is stored on the third party service provider, in the author's accounts and in those of confidents or friends. Account user's information may also be sold to data aggregators and merchants to market products to the users. Even if it were possible to delete a user's, projects like "The Way Back Machine," available

---

[194] European Commission, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Official Journal L 281, 23/11/1995 P. 0031–0050, October 24, 1995.

[195] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).* SEC(2012) 72/73 Final, January 25, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[196] European Commission, *Draft Directive of the European Parliament and of the Council, on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data Brussels*, 2012/0010 (COD), January 25, 2012.

at www.archive.org, catalogues widespread segments of the Internet for posterity, which can make the deletion of information in any streamlined manner very difficult. The Way Back Machine project is "building a digital library of Internet sites and other cultural artifacts in digital form."[197] Arguably, such projects may not have access to information hidden behind passwords. However, with storage becoming cheaper, social networking and cloud computing services are retaining information indefinitely.

Further, the deletion of information implicates competing values. Although the deletion of information can afford an individual control over personal information, and therefore, a semblance of privacy, it may trample another's First Amendment protected speech.[198] The very nature of communications online is that it involves interacting with others. It may not be possible to extricate communications that have been interwoven into discussions with others without trampling on their First Amendment rights. Caroline Kennedy and Ellen Alderman in *The Right to Privacy* noted that often in cases in which invasion of privacy is asserted, competing values might be at stake that could override privacy interests. "Privacy may seem paramount to the person who has lost it but that right often clashes with other rights and responsibilities that we as a society deem important."[199]

6. Reconstituting Privacy

Traditionally, privacy has been viewed as an individual centric value, i.e., freedom from unwarranted search and seizure (trespass), the right to be left

[197] "The Way Back Machine," *Welcome to the Archive*, (n.d.), http://www.archive.org/index.php.

[198] See Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You," *Stan. L. Rev.* 52, no. 1049 (1999), which explores tensions that exist between the right to privacy over an individual's information and another's First Amendment free speech rights, and concludes that typically, privacy is subservient to First Amendment rights.

[199] Ellen Alderman and Caroline Kennedy, *The Right to Privacy* (New York: Vintage, 1997).

alone (solitude and intimacy, and reserve and anonymity),[200] an individual's "reasonable expectation of privacy," ala *Katz. v. U.S*.[201] and, more recently, the right to control pertinent personal information.[202] In 1967, Prof. Alan Westin in *Privacy and Freedom* posited a ground breaking theory that privacy is the control over personal information. He defined privacy as:

> the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person form the general society through physical or psychological means either in a state of solitude or small group intimacy, or when among larger groups in condition of anonymity or resolve.[203]

Westin qualified this definition by noting "an individual's desire for privacy is never absolute, since participating in society is an equally powerful desire."[204] Social media has greatly enhanced the ability to participate in society by facilitating the formation of and participation in online communities. At the same time, the storage and aggregation of vast amounts of personal data in third party services has significantly altered an individual's ability to maintain control over data pertaining to oneself, and has adversely impacted the legally recognizable expectation of privacy. Nevertheless, the principles embedded in the Fourth Amendment, the protection of the individual from the strong arm of the sovereign, remain as pertinent today as in the days of the Founding Fathers.

In today's networked world, these traditional notions are no longer adequate. With information flowing freely from the individual to the commercial sector and to governmental entities, as well as to an individual's friends in e-mail

---

[200] Brandeis and Warren, "The Right to Privacy." See also Donald R. Zoufal, ""Someone to Watch Over Me?" Privacy and Governance Strategies for CCTB and Emerging Surveillance Technologies (master's thesis, Naval Postgraduate School, 2008).

[201] *Katz v. U.S*.

[202] Helen Nissenbaum, "Privacy As Contextual Integrity," *Wash. L. Rev.* 79, no. 119 (2004), http://ssrn.com/abstract=139144.

[203] Westin, *Privacy and Freedom*, 7.

[204] Ibid.

and social media, control over personal information becomes much more difficult to achieve. Valerie Steeves, in *Reclaiming the Social Value of Privacy,* opines that privacy is a dynamic socially constructed process in which an individual negotiates "personal boundaries in intersubjective relations."[205] This dynamic process is being conducted in a myriad of different ways in cyberspace. As was noted by danah boyd, today's social media users employ a host of structural and strategic practices to limit and control who may access information they communicate in social media.[206]

These discussions of privacy, however, miss the mark. They miss the mark because, as with *Katz*, they remain focused in one way or another on the individual, and whether the individual has a legitimate expectation of privacy. While focusing on the individual when it comes to an individual's privacy may seem obviously intuitive, it is also why current dialogue is trapped in a regressive logical loop. A Fourth Amendment analysis of privacy that focuses solely on a *Katz* expectation of privacy test cannot resolve the Fourth Amendment jurisprudential conundrum confronted by modern interactive communications because it has neglected that the Fourth Amendment is about a restraint on government power. The Fourth Amendment asks the question, not just does a personal expectation of privacy exist, but also why does the government need to know? The Fourth Amendment recognizes, as the colonists recognized with the King, as Brandeis recognized with the telephone, and as Europe recognized with the Nazis, information is power. Likewise a government, which has unbridled access to personal information, is a government bound for totalitarianism. Information in the hands of the sovereign is a powerful, but dangerous thing. The

---

[205] Valerie Steeves, *Reclaiming the Social Value of Privacy, Lessons from the Identity Trail*, ch. 1 (Oxford University Press, 2009), http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_11.pdf.

[206] A recent survey revealed that 58% of social media users report limiting with whom they share information with women being "more likely to choose private settings." See Mary Madden, "Privacy Management on Social Media Sites," *Pew Internet and American Life Project*, February 24, 2012, http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx; Woodrow N. Hartzog and Frederic D. Stutzman, "Boundary Regulation in Social Media," *The University of North Carolina At Chapel Hill*, October 8, 2009, http://ssrn.com/abstract=1566904.

Fourth Amendment recognized the necessity of the sovereign to access information with probable cause. Where a government has not demonstrated probable cause with which to answer why it needs to know, access to private information is denied as a check on power. Privacy analysis must move past *Katz*, past a mere analysis of a personal expectation of privacy, and return to a concern for limitations of governmental power.

B. PROBABLE CAUSE 2.0

The Fourth Amendment was written by the Founding Fathers who were suspect of unrestrained government surveillance. The Fourth Amendment is a Constitutional analysis that balances the privacy interests of the individual against the need of government to serve the public good. The restraint of the Fourth Amendment is that to transgress the privacy of the individual, the government must establish *probable cause*. Probable cause is defined as follows:

> The amount and quality of information police must have before they can search or arrest without a warrant. Most of the time, police must present their probable cause to a judge or magistrate, whom they ask for a search or arrest warrant. Information is reliable if it shows that it's more likely than not that a crime has occurred and the evidence sought exists at the place named in the search warrant, or that the suspect named in the arrest warrant has committed a crime.[207]

How implementation of this Constitutional policy has historically evolved to match the privacy expectations of individuals and how social media has turned those expectations of privacy upside down has been explored. This section turns to *probable cause* itself and the use of social media for surveillance.

1. The Dark Web

The Internet has provided unprecedented access to ideas and information. However, for all the advantages the Internet provides, the Internet and social

[207] Legal Information Institute, “Probable Cause,” *Cornell University Law School*, 2010, http://www.law.cornell.edu/wex/probable_cause.

networking sites are increasingly being utilized by terrorist entities for recruiting, planning, financing, and execution of terrorist acts,[208] as well as to gather military and political intelligence on intended targets.[209] In "Terrorist Financing and the Internet," Michael Jacobson asserts that terrorist organizations, such as Al Qaeda, are increasingly relying on the Internet "to spread its toxic message and drum up support throughout the world."[210]

Prof. Gabriel Weimann from the University of Haifa has engaged in a decade-long study[211] of the encoded and public Internet sites of international terrorism organizations and groups that support them, as well as social media sites on Facebook, Twitter, chat rooms, YouTube, and MySpace. Prof. Weimann maintains, "today, about 90 percent of organized terrorism on the Internet is being carried out through social media." By using these tools, the organizations are able to be active in recruiting new "friends" without geographical limitations."[212] Prof. Weimann explains that:

> when it comes to terrorism online, [terrorist organizations] used to apply a pull strategy; waiting in chat rooms for supporters, interested people, and members of the group to join in. Today, using the social networks, they can actually come to you. That is, using the social nature of Facebook, a page opens to another page, and so on. Friends and friends of friends, like widening circles, all become a huge social web. They can use all that by getting only the first to post the messages they want.[213]

---

[208] EUROPOL, *TE-SAT 2010: EU Terrorism Situation and Trend Report*.

[209] CBS News, "Terrorist Groups Recruiting Through Social Media," *CBC News Technology and Science*, January 10, 2012. http://www.cbc.ca/news/technology/story/ 2012/01/10/tech-terrorist-social-media.html.

[210] Jacobson, "Terrorist Financing and the Internet," 353–63.

[211] Weimann, "Terror on the Internet: The New Arena, the New Challenge." See also CBS News, 2012.

[212] University of Haifa, "Friend Request from Al-Qaeda," *School of Communications and Media Relations*, January 7, 2012, http://newmedia-eng.haifa.ac.il/?p=5680.

[213] Doug Bernard, "Does Social Media Help or Hurt Terrorism," *The Voice of America, Digital Frontiers*, January 21, 2012, http://blogs.voanews.com/digital-frontiers/2012/01/21/does-social-media-help-or-hurt-terrorism/.

Ironically, “the most advanced of Western communication technology is, paradoxically, what the terror organizations are now using to fight the West,” Prof. Weimann said.[214]

In an attempt to identify and track terrorist activities on the web, the University of Arizona’s Artificial Intelligence lab in coordination with the National Science Foundation, instituted the “Dark Web” Project.[215] The Dark Web utilizes a number of tools to identify and track online communications of terrorist organizations. These include the use of a tool called Writeprint, as well as the use of web spiders. Writeprint automatically extracts thousands of multilingual, structural, and semantic features to determine who is creating 'anonymous' content online. Writeprint can look at a posting on an online bulletin board, for example, and compare it with writings found elsewhere on the Internet. By analyzing these certain features, it can determine with more than 95% accuracy if the author has produced other content in the past. The system can then alert analysts when the same author produces new content, as well as where on the Internet the content is being copied, linked to or discussed. Dark Web also uses complex tracking software called Web spiders to search discussion threads and other content to find the corners of the Internet in which terrorist activities are occurring.

In 2007, the Project Lab estimated that between 7,000 and 8,000 websites “created and maintained by known international terrorist groups, including Al-Qaeda, the Iraqi insurgencies, and many homegrown terrorist cells in Europe.”[216] By 2010, the number had grown to 100,000 sites that contained extremist or terrorist content with the largest growth in Web 2.0 enabled “forums, videos,

[214] University of Haifa, “Friend Request from Al-Qaeda.”

[215] National Science Foundation, “University of Arizona, Dark Web Project: Scientists Use the “Dark Web” to Snag Extremists and Terrorists Online,” *Press Release 07-118*, September 10, 2007, http://www.nsf.gov/news/news_summ.jsp?cntn_id=110040. See also Artificial Intelligence Laboratory, “Intelligence and Security Informatics,” (n.d.), http://ai.arizonia.edu/research/isi.

[216] National Science Foundation, 2007. See also Gabriel Weimann, ““al-Qai’ida’s Extensive Use of the Internet,” *Combating Terrorism Center at West Point, CTC Centennial* 1, no. 2 (January 2008): 607, http://www.ctc.usma.edu/posts/al-qaida%E2%80%99s-extensive-use-of-the-internet reporting that al-Qai’da has had a presence on the web dating back to the 1990.

blogs, virtual worlds etc."[217] Dorothy E. Denning, in "Terror's Web: How the Internet is Transforming Terrorism," asserts that the Internet is "fundamentally transforming terrorism."[218] Terrorist groups are using a variety of Internet functionalities from static websites and social networking sites to chat rooms, message boards and blogs to accomplish their aims. Making similar findings, Jane's Strategic Advisory Service in 2009, also reported increased Jihadist activities on Facebook and other social media sites.[219]

In addition to the use of the Internet and Web 2.0 technologies to plan and promote acts of terrorism, it being used by individuals engaged in other malicious ventures, such as the series of attacks perpetrated on government and private sector websites by "hacktivists" like LulzSec[220] and Anonymous. International criminal syndicates are also using the Internet to engage in cybercrimes including identity theft. As terrorist groups have moved online, social media has become a treasure trove of reconnaissance and information for the law enforcement and intelligence communities.[221] According to published reports, U.S. government agencies have been able to monitor[222] and confirm terrorist threats online, and thus, give protective services advanced warning and the ability to shore up vulnerabilities. Government agencies are exploring how they can expand and

---

[217] Hsinchun Chen, *Dark Web: Exploring and Data Mining the Dark Side of the Web* (Tucson, AZ: Springer, 2010).

[218] Dorothy E. Denning, "Terror's Web: How the Internet is Transforming Terrorism," in *Handbook on Internet Crime*, ed. Yvonne Jewkes and Majid Yar (Willian Publishing, 2010).

[219] Tim Pippard, "Jane's Strategic Advisory Services: Al-Qaeda—Jihadists Use of the Internet," *IHS Jane's*, April 16, 2009, http://mspublicsafetysymposium.com/media/pdf/PDF_Presentations/PDF_Files/Al-Qaeda_Jihadist_Use_of_the_Internet_Keynote.pdf.

[220] BBC News, "LulzSec Hackers Claim CIA Website Shutdown," June 16, 2011, http://www.bbc.co.uk/news/technology-13787229. An anonymous hacking group that claimed to have taken down CIA's public facing website and was reputed to have launched denial of service attacks against SONY and Ninetendo.

[221] See Marcus Wohlson, "FBI Seeks Digital Tool to Mine Entire Use of Social Media," *Chicago Times,* February 12, 2012, http://www.suntimes.com/news/nation/10605702-418/fbi-seeks-digital-tool-to-mine-entire-universe-of-social-media.html.

[222] See Edna Reid, "FBI Analysis Jihadi Extremists Videos," *FBI Forensic Science Communications* 11, no. 3 (July 2009), http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2009/research_tech/2009_07_research01.htm.

improve their use of social media. Recently, a FBI initiative to develop an "app" that could help to detect suspicious activity garnered considerable attention from the privacy and civil liberties communities.[223]

2. Crimes and Misdemeanors

Online communications create new opportunities for entrepreneurs, fraudsters, and criminals. The Internet Crime Complaint Center (a partnership of the Federal Bureau of Investigation, the National White Collar Crime Center, and the Department of Justice's Bureau of Justice Assistance) is an organization that tracks online criminal activity. In the past decade, the Internet Crime Complaint Center has seen a substantial increase in both the number of complaints received, as well as the dollars lost in these incidents. While over the past decade the number one complaint has been about auction fraud, the types of crimes complained about have diversified with significant numbers of complaints about identity theft, credit card fraud, and computer crimes.[224]

In terms of surveillance, however, it is not relevant whether the crime transpired online or off. Information available online has become a vital forensics tool[225] regardless of the location of the crime. Social media has become an important law enforcement investigation tool.[226] The 2011 survey of the International Association of Chiefs of Police Center for Social Media shows how adept law enforcement has become in utilizing social media as a tool. According to the report,

---

[223] See Catherine Herridge, "FBI Seeks Developers for App to Track Suspicious Social Media Posts, Sparking Privacy Concerns," *Fox News,* February 16, 2012, http://www.foxnews.com/politics/2012/02/16/fbi-seeks-developers-for-app-to-track-suspicious-social-media-posts-sparking/; NPR All Things Considered, "What the FBI Wants in a Social Media Monitoring App," January 30, 2012, http://www.npr.org/blogs/alltechconsidered/2012/01/31/146090425/what-the-fbi-wants-in-a-social-media-monitoring-app.

[224] Internet Crime Complaint Center, "2010 Internet Crime Report," 2010, http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf

[225] See "Forensics," *Cybertelecom*, 2012, http://www.cybertelecom.org/security/forensic.htm.

[226] See Council of Europe, Convention on Cybercrime, November 12, 2001, http://conventions.coe.int/treaty/en/treaties/html/185.htm.

- "88.1% of agencies surveyed use social media;"
- 71.1% use it for criminal investigations;
- 40.1% use it for soliciting tips on crime; and
- 32% use it for listening or monitoring.[227]

Law enforcement has used social media to track suspects.[228] The use of social media by government officials extends beyond criminal investigations. It may be used by government officials in administrative matters to review applications submitted by individuals for government services.

C. DIGITAL DOSSIERS

Social networking technologies have provided the government with a new ability to amass huge profiles on individuals, without it having to engage directly in surveillance. With the tremendous amount of information available through new commercial databases, online government records (real estate, driver's license), and personal information individuals may post online about themselves, governments can create these profiles with ease. These profiles can give law enforcement and the intelligence communities a powerful tool.

With the ready availability of personal information held in the hands of commercial entities, the government, and the public at large, dossiers on an individual are amassed long before an individual is even born, and may be

[227] IACP Center for Social Media, "IACP Social Media Survey," 2011, http://www.iacpsocialmedia.org/Resources/Publications/2011SurveyResults.aspx.

[228] See Joann Pan, "FBI Uses Social Media to Catch Murder Suspect Who Stole $2.3 Million." *Mashable*, March 9, 2012, http://mashable.com/2012/03/09/kenneth-konias-wanted-fugitive/; Annette Peagler, "Florence Police Use Facebook to Catch Criminals," *KyPost*, March 13, 2012, http://www.kypost.com/dpps/news/region_northern_kentucky/florence/florence-police-use-facebook-to-catch-criminals_7298753. Joe Sinopoli, "Social Media Now a Tool for Crimefighters, Including Downers Grove Police." *mysururbanlife.com*, March 7, 2012, http://www.mysuburbanlife.com/lisle/topstories/x1785613234/Social-media-now-a-tool-for-crimefighters-including-Downers-Grove-police. ("'Mainly in a case we had over a stabbing in town in August 2010," Roundtree said. "We utilized (the alleged criminal's) Facebook page to look into who his friends were.'"); Roger Yu, "Social Media Role in Police Cases Growing," *USAToday*, March 18, 2012, http://www.usatoday.com/tech/news/story/2012-03-18/social-media-law-enforcement/53614910/1. "Police departments and federal agencies utilizing social-media to obtain information in ongoing investigations and are beefing up their budgets to find online clues left by criminals."

amassed after an individual has died.[229] Technology greatly contributes to the compilation of information, by connecting the streams of data held in the hands of a multitude of custodians. While not all the information compiled may be correct, these digital dossiers can become a major part of an individual's identity in the digital world. Today, the government may obtain more information about its citizens by accessing digital data than ever before, and thereby, straining the Constitutional protections against unbridled governmental access to an individual's person and papers.

In the heart of the Cold War, when McCarthyism was gripping the country, the government amassed large quantities of information about Americans in the name of combating the threat of communism on American soil. Dossiers were compiled on individuals in many cases chronicling First Amendment protected activities. One of the most famous targets of this action was Dr. Martin Luther King Jr.[230] When the breadth of this massive surveillance campaign on American citizens, as well as the abuses that occurred during the Watergate era became known, two Congressional Committees, the Pike (House of Representatives) and the Church (Senate) were formed. Their findings resulted in a major overhaul of the intelligence community and the issuance of Executive Order 11905, United States Intelligence Activities, [231] which mandated an intelligence oversight paradigm for the Executive Branch.

The concerns expressed in the Pike and Church Commissions regarding the creation of dossiers on citizens is further heightened in the new information

---

[229] See Berkman Center for Internet and Society, "Digital Natives: Lifecycle of a Digital Dossier," August 13, 2008, http://cyber.law.harvard.edu/node/4535.

[230] From December 1963 until his death in 1968, Dr. Martin Luther King, Jr. was the target of extensive surveillance by the FBI. Initially authorized by Attorney General Robert Kennedy, the FBI utilized "nearly every intelligence-gathering technique at the Bureau's disposal." FBI efforts were in part to obtain information to "discredit King as 'an effective negro leader.'" See Senate Select Committee to Study Governmental Operations, "Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Book III," *The Church Commission*, April 14, 1976.

[231] Executive Order 11905 was subsequently replaced by Executive Order 12333 Intelligence Activities, (1981) as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008).

technology era in which the ability to aggregate information is greatly enhanced. In today's digital world, with information pertaining to an individual so readily available, "Digital Dossiers" are easier to compile than ever and the information compiled is on a quantitatively different scale. What previously took teams of agents hours of work, stakeouts, and other resource intensive intelligence gathering efforts,[232] can now be acquired by surfing social media sites or purchasing reports on individuals from third parties.

In *Born Digital*, John Palfrey and Urs Gasser explain that a digital dossier may be created on individuals from information they provided about themselves, from information derived about them from their participation on social networks, such as Facebook, from information compiled from other public sources, as well as from non-public sources, such as medical and financial records, and even from an individual's reading lists compiled from public libraries and book sellers. Everything that an individual posts online, anything that someone else posts about them, anything they ever link to, anyone they ever friend, any purchase they ever make, any link they ever click on, any comment they ever "like," any image they ever view or upload, can all become part of their digital dossier—easily creating a comprehensive picture of the individual. Information contained within a digital dossier includes information supplied or available to the individual, as well as information that may not be available to include records created from non-public government records. These pieces of information can be compiled to form a comprehensive picture of an individual's personality, tastes, interests, political and religious positions, or any other aspect of said individual's life. Once information is digitized, it is virtually impossible to delete or correct.

[232] The Church Report chronicles the efforts undertaken by the FBI during its surveillance program that employed nearly every intelligence-gathering technique at the Bureau's disposal. They noted 16 occasions in which the FBI placed microphones in hotel rooms stayed in by King. His home and office, as well as those of his associates, were wiretapped, and which necessitated the expenditure of huge resources. Senate Select Committee to Study Governmental Operations.

Governments can readily obtain more information about its citizens by accessing digital data than ever before. The ability to do so led Prof. David Solove to muse that it might ultimately result in a

> Kafkaesque world of bureaucracy, where we are increasingly powerless and vulnerable, where personal information is not only outside our control but also subjected to a bureaucratic process that is itself not adequately controlled. This generalized harm already exists; we need not wait for specific abuses to occur.[233]

Further, Evgeny Morozov in the *Net Delusion* quips that today, intelligence entities such as the KGB can easily obtain information that in the past they could only have obtained through the use of torture.[234]

Today, digital dossiers are readily available about individuals. For just $2.95 per month on Spokeo.com, anyone can purchase information about a person's gender, relationship, real estate holdings, salary, ethnicity, political affiliation, religious affiliation, educational level, and occupation.[235] Contrast this against the labor-intensive efforts to gather intelligence about Dr. Martin Luther King Jr. and it is possible to realize how easy it is for today's government to compile dossiers on an individual.

D. INTERNET FREEDOM

The Internet promotes American ideals of participatory government, the corner stone to a sound democracy, while at the same time, it enhances national security by providing situational awareness about country conditions so as to not be blindsided when political upheavals occur.[236] It has enabled the spread of democratic ideals both within this country and around the world. The recent events in the Middle East known as the "Arab Spring" were facilitated by social media technologies. Individuals in repressive regimes utilized social media to

---

[233] Daniel J. Solove, *Digital Person, Technology and Privacy in the Information Age* (New York: University Press, 2004), 96.

[234] Evgeny Morozov, *The Net Delusion: How Not to Liberate the World* (Allen Lane, 2011).

[235] Spokeo, "Join," (n.d.), http://spokeo.com.

[236] *ACLU v. Reno*, 929 F.Supp. 825 (E.D.Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

communicate with like-minded people in ways previously only possible at great peril to their well-being. It also enabled dissidents to focus international attention on these repressive regimes by transmitting news of atrocities committed by government forces.[237]

The Federal Court in *ACLU v. Reno* noted the important role the Internet has played in U.S. democracy:

> It is no exaggeration to conclude that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country – and indeed the world has yet seen. The plaintiffs in these actions correctly describe the "democratizing" effects of Internet communication: individual citizens of limited means can speak to a worldwide audience on issues of concern to them. Federalists and Anti-Federalists may debate the structure of their government nightly, but these debates occur in newsgroups or chat rooms rather than in pamphlets. Modern-day Luthers still post their theses, but to electronic bulletin boards rather than the door of the Wittenberg Schlosskirche. More mundane (but from a constitutional perspective, equally important) dialogue occurs between aspiring artists, or French cooks, or dog lovers, or fly fishermen . . . . [T] he Internet may fairly be regarded as a never-ending worldwide conversation.[238]

Given the significant role the Internet plays in fostering democratic ideals, on February 15, 2011, Secretary of State Hillary Clinton gave a speech entitled "Internet Rights and Wrongs: Choice & Challenges in a Networked World." Secretary Clinton called for a "global commitment to Internet freedom" in which human rights are protected online as they are off line.[239] These freedoms include the freedom to assemble and associate in cyberspace. Secretary Clinton noted, "connection technologies" provide "on the one hand an accelerant of political, social and economic change and on the hand as a means to stifle or extinguish

---

[237] See Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Philadelphia: Basic Books, 2012).

[238] *ACLU*, 929 F.Supp. 825.

[239] Department of State, "Internet Freedom, About Internet Freedom at the State Department."

that change."[240] Accordingly, Ms. Clinton declared that Internet freedom is "a foreign policy priority . . . one that will only increase in importance in the years to come."[241]

The recent events in the Middle East and North Africa illustrate the benefit of providing individuals in repressive countries access to the digital tools. The revolutionary fervor present throughout the Middle East had been growing for some time and would most likely have come to a head even in the absence of social networking sites and other connection technologies. Individuals in the Middle East took to the street in protest to seek basic freedoms after suffering under brutal and totalitarian rule for years. Social media sites provided a forum for voices that in the past might have been expressed through the distribution of leaflets or by people standing on soap boxes in the town square. Electronic communications served as catalysis for the growing opposition to the status quo and enabled the unprecedented wave of protest throughout the Middle East.[242]

As more and more individuals embrace social media to express their thoughts and views, it is imperative to update privacy laws and adopt appropriate safeguards to ensure that governmental surveillance and access does not have a chilling impact on the "democratizing effects of Internet communications" both at

[240] Department of State, "Internet Freedom, About Internet Freedom at the State Department."

[241] Ibid.

[242] See Michelle Norris, "Interview with Alec Ross Advisor to Hilary Clinton, re Internet Freedom and the U.S. State Department," *National Public Radio, All Things Considered*, February 17, 2011, http://www.npr.org/2011/02/17/133847146/Internet-Freedom-And-U-S-State-Department (rejecting notion that social media caused the revolutions by stating "These were people-based revolutions. You know, I think we need to recognize that technology is just a tool. Now, it was a tool used to very powerful effect in Tunisia and in Egypt. But the technology, the social media, isn't the end unto itself.").

home and abroad. The guarantees of liberty provided by the United States for its own citizens are held up as an international model (for good or for bad).[243]

[243] See Zhang Xiang, "Britain's U-Turn Over Web-Monitoring," *Xinhuanet*, August 12, 2011, http://news.xinhuanet.com/english2010/indepth/2011-08/12/c_131046237.htm. ("We may wonder why western leaders, on the one hand, tend to indiscriminately accuse other nations of monitoring, but on the other take for granted their steps to monitor and control the Internet. They are not interested in learning what content those nations are monitoring, let alone their varied national conditions or their different development stages. Laying undue emphasis on Internet freedom, the western leaders become prejudiced against those "other than us," stand ready to put them in the dock and attempt to stir up their internal conflicts."); The China Post, "Cut to Cell Phone Service Sparks Controversy in SF," August 15, 2011, http://www.chinapost.com.tw/international/americas/2011/08/15/313394/Cut-to.htm ("An illegal, Orwellian violation of free-speech rights? Or just a smart tactic to protect train passengers from rowdy would-be demonstrators during a busy evening commute?"); Eva Galperin, "BART Pulls a Mubarack in San Francisco," *Electronic Freedom Foundation*, August 12, 2011, https://www.eff.org/deeplinks/2011/08/bart-pulls-mubarak-san-francisco.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES IN AN ERA OF SOCIAL MEDIA

Social media by its nature is collaborative. It enables individuals to form communities and to be interactive in a digital manner. Today, individuals are taking their conversations from their living rooms to cyberspace. Young people are living their lives in cyberspace. The fact that their communications are occurring in a space owned and operated by a third party does not mean an expectation of privacy is any less as articulated by the Supreme Court in *Katz*. Just as the Founding Fathers almost 240 years ago wanted to be secure from intrusive governmental acts, so do individuals today. Just as the colonists recognized the need for government to engage in actions to protect themselves from threats from abroad, so too today do Americans recognize that law enforcement and intelligence communities' need to engage in surveillance to detect, thwart and respond to threats from terrorists and other criminal actors.

Fifty years passed between the invention of the telephone and *Olmstead*; Justice Brandeis discerningly grasped the peril presented by evolving communications and surveillance technology as a potential erosion of Fourth Amendment protections. Four decades passed between *Olmstead* and *Katz*; the Supreme Court acknowledged that surveillance laws at that time were incongruous with advances in communications. Twenty years passed between *Katz* and ECPA; surveillance laws were again out of alignment with advances in communications. [244] Twenty five years have passed since ECPA; communications have advanced tremendously so as to confound not only *Katz* but ECPA as well. ECPA's analysis flounders on a 1986 comprehension of computer networks that has little relation to today's communications environment.

[244] Congress of the United States, Office of Technology Assessment, "Electronic Surveillance and Civil Liberties."

Katz's analysis crashes in the regressive logical loop that is Third Party Doctrine. Combined, neither affords privacy protections and restraint on government surveillance guaranteed by the Fourth Amendment.

A. THE DARK WEB REVISITED

Grave concern exists that the tracking of terrorist activity may result in a degradation in privacy and civil rights. In "Terror on the Internet,"[245] Gabriel Weimann provides an in-depth analysis of terrorists' use and presence in cyberspace, but argued that although terrorist organizations take advantage of the largely "unregulated, anonymous and accessible nature of the Internet," surveillance of the Internet by law enforcement and intelligence community entities may result in an infringement of an individual's privacy. He echoes the views of other privacy advocates that it is not the use or monitoring of the Internet but rather the lack of judicial oversight that is of concern.[246] Understanding the potential harm that can be perpetrated upon U.S. society by terrorists using Internet technologies to assist in their nefarious aims, Mark Rotenberg, Executive Director of the Electronic Privacy Information Center, an online civil-liberties group, also cautioned that the tools utilized by projects like the Dark Web and other more recent efforts of the federal government "to track terrorists can also be used to track political opponents."[247] Rotenberg posits that such tools should comply with existing privacy laws. As valuable as the Dark Web and similar tools may be to detect and thwart terrorist aims, safeguards must be implemented to ensure that they do not infringe upon the rights provided by the First and Fourth Amendments.

The American Civil Liberties Union warns that with the increase in governmental surveillance efforts on the Internet, America is at risk of becoming

---

[245] Gabriel, "Terror on the Internet: The New Arena, the New Challenge."

[246] Ibid., 218.

[247] Steven Kotler, "'Dark Web' Project Takes on Cyber-Terrorism," October 12, 2010, http://www.stevenkotler.com/node/87.

a "surveillance society."[248] In the days following the tragic events of September 11, 2001, a greater emphasis was placed on the collection of information pertaining to individuals hastened by the weakening of existing regulations on its collection and the passage of sweeping legislation like the USA Patriot Act. The "commodification" of data by the private sector, which has been collecting all means and methods of an individual's activities online, has only added to the move towards a surveillance society.[249]

In "Bigger Monster, Weaker Chains," Jay Stanley and Barry Steinhardt, writing on behalf of the ACLU, argue for the passage of new and comprehensive privacy laws to provide privacy and civil liberties protections for new and emerging technologies:

> In the past, new technologies that threatened our privacy, such as telephone wiretapping, were assimilated over time into our society. The legal system had time to adapt and reinterpret existing laws, the political system had to consider and enact new laws or regulations, and the culture had time to absorb the implications of the new technology for daily life.[250]

However, today, new technologies, such as social networking and cloud computing, are being developed at such breakneck speed; laws have failed to keep pace. Post-September 11 efforts to protect this country from future acts of terrorism and other crimes have resulted in an erosion of privacy and civil liberties. Therefore, Stanley and Steinhardt argue that "the reasonable expectation of privacy cannot be defined by the power that technology affords the government" to perform surveillance and should be reevaluated to take into account contemporary circumstances.[251]

---

[248] ACLU, "Is the U.S. Turning into a Surveillance Society? Big Brother is No Longer a Fiction," *ACLU Technology and Liberty Program 2003*, 2003, http://www.aclu.org/technology-and-liberty/big-brother-no-longer-fiction-aclu-warns-new-report.

[249] Jay Stanley and Barry Steinhardt, "Bigger Monster, Weaker Chains," ACLU 2003, 2003, http://www.aclu.org/files/pdfs/privacy/bigger_weaker.pdf.

[250] Ibid., 16.

[251] Ibid., 17.

B. *KATZ* REVISITED: THIRD PARTY DOCTRINE: A REGRESSIVE LOGICAL LOOP

Katz's Third Party Doctrine is particularly troubling because today most data residing in the digital world is transmitted or stored on third party intermediary sites. The application of the Third Party Doctrine to data transmitted and communicated in social media or stored in the cloud would arguably provide the government with such unfettered access it would negate the protections envisioned by the Fourth Amendment. Today, comments made on Facebook can be likened to parlor talk in which friends can betray confidence, and thus, less privacy is afforded. However, just because they can, does this mean that the government gets to enjoy fruits of third parties? The limits of what is constitutionally permissible should not be defined by what is technically feasible. The Third Party Doctrine, taken to its logical conclusion, has the potential to deprive all electronic communications occurring in social media and stored in the cloud of any Fourth Amendment protection,[252] and therefore, it must be modified. John Palfrey in "The Public and the Private at the United States Border with Cyberspace" has argued it is time to "rethink legal protections for citizens from state surveillance in a digital age as a result of this third-party data problem."[253]

As Supreme Court Justice Sotomayor also posited in *U.S. v. Jones*, given the rapid advancements in technology, it is time to reevaluate the Third Party Doctrine and the legal interpretation that an individual has no reasonable expectation in information voluntarily disclosed to third parties:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[254]

---

[252] Strandburg, "Home, Home on the Web, and Other Fourth Amendment Implications of Technosocial Change."

[253] Palfrey, "The Public and the Private at the United States Border with Cyberspace."

[254] *Jones*, 565 U.S. slip at 5-6 (2012).

Recently, the propriety of the Department of Homeland Security's monitoring of social media and the impact it has on constitutionally guaranteed free speech was the subject of a hearing before the House Homeland Security Committee's Subcommittee on Counterterrorism and Intelligence.[255] Chairman Patrick Meehan, while acknowledging the importance of following leads "wherever they may take investigators" in keeping this country safe from terrorists and other criminal actors, nevertheless questioned whether "collecting, analyzing, and disseminating private citizens' comments could have a chilling effect on individual privacy rights and people's freedom of speech and dissent against their government."[256] Today, with the availability of information and the ease of access, it is more important then ever to take legislative, administrative and judicial steps to ensure that an appropriate balance is struck between the government's intelligence needs against an individual's privacy and civil liberties.

C. ECPA REVISITED

Twenty five years after the passage of ECPA, calls have been made for its reform.[257] The evolution of electronic communications has occurred with breakneck speed, with the Internet being widely adapted by modern society. Web 2.0 and the social media enable functionality, interactivity, and exposure that did not exist at the time of ECPA's passage in 1986. Although ECPA was a forward-looking statute at the time of its passage, its technology centric approach resulted in the statute being limited to technology as it existed twenty five years

---

[255] *DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy*: *Hearing before Committee on Homeland Security, Subcommittee Counterterrorism and Intelligence*, February 16, 2012, http://homeland.house.gov/hearing/subcommittee-hearing-dhs-monitoring-social-networking-and-media-enhancing-intelligence.

[256] Ibid.

[257] See, e.g., The *Electronic Communications Act: Government Perspectives on Protecting Privacy in the Digital Age. Hearing of the United States Senate Committee on the Judiciary*, April 6, 2011; *ECPA Reform and the Revolution in Location Based Technologies and Services, Hearing of the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties*, June 24, 2010; *Electronic Communications Privacy Act Reform. Hearing of the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties*, Serial No. 111–98, 111th Cong., May 5, 2010.

ago. Applying ECPA to today's social networking technologies is like using a sledgehammer to hang a digital picture frame. The result has been awkward and inconsistent judicial interpretations that have left the public with little to no expectation of privacy.[258] As such, many believe that EPCA no longer provides sufficient clarity to govern today's technological abilities and are calling for a statutory fix to afford Fourth Amendment like protections to an individual's "papers and effects" now stored in the cloud.[259]

Since 1986, e-mail has become a dominant means for communicating in the country. Web 2.0 enabled an individual to communicate in a collaborative manner with larger communities. With the price of storage becoming negligible, it is not uncommon to retain many if not all e-mails and other communications indefinitely on third party provider servers. Applying ECPA's 25-year-old standards to today's digital communications deprives users of the Fourth Amendment like protections Congress had intended.

With the growth in popularity of Web 2.0 technologies, and with more and more computing activities moving to the cloud, the issue of to what extent an individual possesses a reasonable expectation of privacy when using a social media tool is not well settled. The courts are now addressing how Fourth Amendment privacy protections apply in the new evolving social media environment. A district court in California confronted this issue for the first time in 2010 and held that private messages sent using Facebook or MySpace do in fact

---

[258] *See City of Ontario, Cal. v. Quon*, 130 S.Ct. 2619 (2010). Demonstrating the Supreme Court's reluctance to infer Fourth Amendment protections to nascent electronic communications. "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *See also Crispin v. Christian Audigier, Inc*., 717 F.Supp.2d 965 (C.D.Ca. 2010) (holding Stored Communication Act applies to Facebook messaging and may apply to Facebook wall posts given certain privacy settings).

[259] The Digital Due Process Coalition, whose members include members of the technology and commerce sectors, such as Amazon, AOL, Microsoft, Center for Democracy and Technology, AT&T and Google, are seeking the amendment of ECPA so as "To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public." ACLU, "Modernizing the Electronic Communications Privacy Act," (n.d.). http://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa.

fall under the protections of the Stored Communications Act that limits the government's ability to force Internet Service Provider to "disclose information in their possession about their customers and subscribers."[260] Similarly, items posted on an individual's wall may also enjoy the protections of the Stored Communications Act, but only to the extent that an individual invoked the sites' privacy protections.

Many believe that EPCA fails to provide sufficient clarity to govern today's transformed social media environment and are calling for a statutory revision. In 2010, Congress held hearings in which it explored the possibility of reforming ECPA.[261] Testimony not only focused on the need to fix the legendary "lack of clarity" provided by ECPA but also on the need to bring the law into alignment with the development in technology and societal expectations of privacy. At the September 22, 2010, Senate Judiciary Committee hearing, Committee Chairman Patrick Leahy stated that '[b]ringing this privacy law into the Digital Age will be one of Congress's greatest challenges . . . the 'ECPA is a law that is often hampered by conflicting privacy standards that create uncertainty and confusion for law enforcement, the business community and American consumers."[262] On May 19, 2011, Senator Leahy introduced the ECPA Amendments Act of 2011.

The ECPA amendment eliminates the distinctions between communications in transit, communications in storage, as well as the between e-mails and other forms of electronic communications. It decreases the time before law enforcement (LE) is required to provide notification to the subject that a search has occurred and requires LE to obtain a warrant to access mobile phone locational data. In particular, the Act would make the following modifications:

---

[260] *Crispin v. Audigier, Inc.,* 717 F.Supp.2d 965. Court opined that because Facebook and MySpace provide private messaging or e-mail services, as well as electronic storage, they qualify as both ECS and RCS providers, and as such, warrant the protections of the SCA. This decision is binding only in the Central District of California but may be persuasive in other courts that begin to confront similar issues.

[261] *ECPA Reform and the Revolution in Cloud Computing*.

[262] *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age. Hearing of the Senate Committee on the Judiciary*.

- Voluntary disclosure by service providers—with limited exception, service providers would be prohibited from voluntarily disclosing the contents of customers' electronic communications to the government.
- Compelled disclosure of the contents of communications—eliminates the 180-day rule; would require a warrant for the disclosure of the contents of any electronic communications regardless of how long the communications had been stored.
- Disclosure of transactional data—an administrative or grand jury subpoena would be required for government access to transactional data that includes customer name, address, session time records, length of service information, subscriber number and temporarily assigned network address, and means and source of payment information.
- Notice—the government would be required to provide notice (a copy of the warrant and any other pertinent information) to the affected customer within three days. Delivery of the required notice could be delayed for up to 90 days upon a showing that notice would endanger national security.
- New protections for geolocation information—governmental access to contemporaneous geolocation information defined as "any information concerning the location of an electronic communications device that is in whole or in part generated by or derived from the operation or use of the electronic communications device," is permitted only pursuant to a warrant or express consent of the owner of the mobile device or application, except in certain emergency circumstances. Access to historical communications is permissible pursuant to a warrant, consent or court order upon a showing of "specific and articulable facts that. . . there are reasonable grounds to believe that the information [communications] . . . is relevant and material to an ongoing criminal investigation.

The ECPA amendment eliminates the distinctions between communications in transit, communications in storage, as well as the between e-mails and other forms of electronic communications. It decreases the time before LE is required to provide notification to the subject that a search has occurred. Further, it requires LE to obtain a warrant to access mobile phone locational data.

Until such time as Congress affords some statutory relief, the lack of clear standards for governmental access to information, communicated in social media

and stored on third party servers, places service providers on the front lines of the debate. Many major service providers, such as Microsoft, state in their privacy policies that they will provide content to law enforcement or intelligence entities in response to lawful requests. However, the determination of whether a request is valid and permissible, and that the government has procured the proper level of process, is left up to the companies and their legal counsel to determine.[263] In addition, in many circumstances, the individual may never know that a request was made for information and the extent to which it has been honored.[264] The quandary third party service providers find themselves in further highlights the ever increasing need to strike the correct balance between Fourth Amendment expectations of privacy with the law enforcement and intelligence communities' need to obtain pertinent information to detect, prevent and thwart potential terrorist and other criminal acts.[265] Striking the correct balance is now more critical then ever as Supreme Court Justice William J. Brennan reminded, "the needs of law enforcement stand in constant tension with the Constitution's protections of the individual. . . It is precisely the predictability of these pressures that counsels a resolute loyalty to Constitutional safeguards.[266]

---

[263] An example occurred in 2005 when the Department of Justice attempted to use a subpoena to compel the disclosure of one week and one million randomly selected web addresses occurring over a one-week period, from Google, to help DOJ defend its position on the Child Online Protection Act. *Gonzales v. Google, Inc.,* No. 5:06-mc-80006-JW (N.D. Cal. motion to compel filed January 18, 2006). Google held the position that the request was improper, overly broad and refused to honor the request in the absence of a warrant as required by the Stored Communication Act of ECPA. Google was then forced to defend its position in court. *Google's Opposition to the Government's Motion to Compel in Gonzales v., Inc.,* No. 5:06-mc-80006-JW (N.D. Cal. Filed 2006) googleblog.blogspot.com/pdf/Google_Oppo_to_Motion.pdf.

[264] Currently, only Google provides the public with high-level information about the numbers of access requests it received and to which it responded. In its most recent *Google Transparency Report,* in the period between January 2011 and June 2011, Google received 5,950 government requests for disclosure of user data from Google accounts or services. They partially or fully responded 93% of the time. See Google, "Transparency Report," 2011. http://www.google.com/transparencyreport/.

[265] See Associated Press, "Google Rebuffs Feds on Search Requests," *MSNBC.com Tech and Gadgets*, January 19, 1996, http://www.msnbc.msn.com/id/10925344/ns/technology_and_science-tech_and_gadgets/t/google-rebuffs-feds-over-access-search-data/.

[266] *Michigan Dept. of State Police v. Slitz*, 110 S.Ct. 2481, 2490 (1990) (quoting Alameida-Sanchez v. United States 413 U.S. 266, 273 (1973)).

Privacy and civil liberties are at a crossroad in cyberspace. This moment in Fourth Amendment history is very reminiscent of the period leading up to the enactment of ECPA during which U.S. Circuit Court Judge Richard Posner chided Congress to take action to bring the Wiretap Act into alignment with the current state of technology. Posner quipped, "we would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope . . . judges are not authorized to amend statutes even to bring them up to date."[267] ECPA is obsolete. Patches downloaded from Congress are unlikely to restore functionality. ECPA is out of alignment with social media communications and societal expectations related to it. The statute no longer achieves Fourth Amendment objectives of establishing appropriate restraints on government surveillance and protection of privacy.

D. BRANDEIS REVISITED

More than a century has passed since Louis Brandeis and his law partner Samuel Warren advocated for the recognition of the right to privacy in common law. Brandeis and Warren observed first hand the impact new and emerging technology can have on an individual's privacy. Responding to newly emerging practices of journalists, in particular photojournalists "invading the sacred precincts of private and domestic life and [whose] numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops,'"[268] they authored the seminal law review article, "The Right to Privacy." The "Right to Privacy" set forth a framework for establishing legal protections to remedy intrusions on an individual's privacy that is still pertinent today. They argued that the ever-evolving instrument of common law should be evoked to respond to "recent inventions and business practices" that enabled the intrusion of one's "thoughts, emotions and sensations," and

[267] *U.S. v. Torres*, 751 F.2d 875 (7th Cir. 1984) held that the making of a bomb was not oral or wire communications under the 1968 Federal Wiretap. Therefore, the act did not require the government to obtain a warrant to videotape the defendant's in the act of bomb making.

[268] Brandeis and Warren, "The Right to Privacy."

bestow upon the individual, legal recognition of "the right to be left alone."[269] The concerns they raised and their call for judicial intervention in the face of intrusive new technologies struck a chord that continues to reverberate today in the era of social media.

Several years after Brandeis wrote "The Right to Privacy," he became a Supreme Court Justice and once again was confronted with the intrusions to privacy caused by emerging technologies, this time brought about by the government. In the dissenting opinion *in Olmstead v. U.S*., he asserted that an individual has a Constitutional right to be left alone as against the government. Brandeis argued the Court must recognize the Constitution as a living document. The framers of the Constitution could not have anticipated the advancements that had occurred in technology since the colonial era nor did they intend for the protections afforded by the Bill of Rights to be limited to those threats that existed in the early days of this nation. Brandeis cautioned that "discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[270]

With the advancements in technology that became available in Brandeis's lifetime and those that he intuitively knew were yet to come, he warned of the need to ensure that the protections of the Fourth Amendment transcended time, as was the intention of the drafters of the Constitution. In 2012, Brandeis' words ring as true as ever. In an era in which personal effects that used to be secured in a desk behind the walls of an individual's home, are now communicated and stored in cyberspace, an individual has no less protection against unfettered access by the government. As Brandeis admonished, the law must continue to evolve and keep pace with new and emerging technologies.

---

[269] Brandeis and Warren, "The Right to Privacy."

[270] *Olmstead v. United States*, 277 U.S. 438 (1928), 473 (J. Brandeis, Dissenting Opinion).

E. CONCLUSION

Privacy is one of the most cherished values of a society. It is essential to a strong democracy. The Founding Fathers responding to abuses of the Crown provided protections to the individual as against the government in the Bill of Rights. The Fourth Amendment recognized the need of the government to take appropriate action to protect its citizens even if it meant engaging in surveillance. However, consistent with the Constitutional framework embedded in this country's system of government, a judicial warrant premised upon probable cause must be obtained to place a check against governmental excesses.

Throughout this country's history, a constant cycle of technological developments have challenged an individual's privacy and civil liberties, legislative attempts to rectify gaps in the protections of those civil liberties, and judicial efforts to align societal expectations of Constitutional rights with new and emerging technologies, even when the state of the law fails to keep pace.

Sadly, on the morning of September 11, 2001, "a day of unprecedented shock and suffering in the history of the United States,"[271] when nearly three 3,000 people died, "the largest single loss of life from an enemy attack on American soil,"[272] the bounds of the protections of the Fourth Amendment were challenged. Greater demands were placed on the law enforcement and intelligence communities to detect, prevent, thwart and respond to attacks against Americans and their interest. They, like a growing number of Americans, turned to the Internet.

Since September 11, society has begun to adopt social networking technologies to communicate with loves ones, form communities with individuals with similar interests, and to store their personal effects in the cloud. Similarly, terrorists and other criminal actors have also embraced social networking

---

[271] *The National Commission on Terrorist Attacks Upon the United States, The 9-11 Commission Report* (New York; W.W. Norton & Company, 2003), xv.

[272] Ibid.

technologies, and as such, they have provided a treasure trove of information for the government. The Artificial Intelligence Dark Web project and Professor Gabriel Weinmann documented the use of social media technologies by terrorist organizations to recruit new adherents, raise funds, plan and execute acts of terror, and to spread propaganda about their endeavors and their ideologies.

As effective as surveillance of the Internet may be, it must not be undertaken at the expense of individual privacy and civil liberties. Existing privacy and civil rights law have failed to keep pace with advancements in technology. With the advent of social media and cloud computing, laws have once again failed to keep pace with the rapid advancements in technologies. Currently, this period of time is reminiscent of the days leading up to the passage of ECPA when as observed by the Congressional Office of Technology Assessment:

> In the last 20 years, there has been a virtual revolution in the technology relevant to electronic surveillance. Advances in electronics, semiconductors, computers, imaging, databases, and related technologies have greatly increased the technical options for surveillance activities . . . The existing statutory framework and judicial interpretations thereof do not adequately cover new electronic surveillance applications. The Fourth amendment–which protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures' '—was written at a time when people conducted their affairs in a simple, direct, and personalized fashion. . . public policy on the use of information technology to electronically monitor individual movements, actions, and communications has been based on a careful balancing of the civil liberty versus law enforcement or investigative interests. New technologies . . . have outstripped the existing statutory framework for balancing these interests.[273]

Private papers are now stored in the cloud and not behind the four walls of an individual's home as they were in the days of the Founding Fathers. However, as suggested by Justice Brandeis in "The Right to Privacy," and later in the

[273] Congress of the United States, Office of Technology Assessment, "Electronic Surveillance and Civil Liberties," NTIS Order #PB86-123239, 39, 1985, http://www.fas.org/ota/reports/8509.pdf.

Olmstead dissent, the principles enshrined in the Fourth Amendment protecting against unrestrained governmental access to personal papers were not meant to lay dormant in the 1700s but must continue to progress with advancements in technology. Once again it is necessary to heed the cry to action of Justice Possner and seek statutory guidance that strikes an appropriate balance between an individual's privacy and civil liberties and the government's need for information to keep this country safe.

LIST OF REFERENCES

18 U.S.C § 2510 et seq.

Abrams v. United States, 250 U.S. 616, 630-31 (1919) (J. Holmes, Dissenting).

ACLU v. Reno, 929 F.Supp. 825 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

ACLU. "Modernizing the Electronic Communications Privacy Act." (n.d.). http://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa.

———. "Is the U.S. Turning Into a Surveillance Society? Big Brother is No Longer a Fiction." *ACLU Technology and Liberty Program 2003.* 2003. http://www.aclu.org/technology-and-liberty/big-brother-no-longer-fiction-aclu-warns-new-report.

Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. New York: Vintage, 1997.

In re Application of the United States of America for Historical Cell Phone Data Site Data, 747 F. Supp.2d 827 (S.D. Tex. 2010).

Artificial Intelligence Laboratory. "Intelligence and Security Informatics." (n.d.). http://ai.arizonia.edu/research/isi.

Associated Press. "Google Rebuffs Feds on Search Requests." *MSNBC.com Tech and Gadgets*. January 19, 1996. http://www.msnbc.msn.com/id/10925344/ns/technology_and_science-tech_and_gadgets/t/google-rebuffs-feds-over-access-search-data/.

Bauer, Kevin, Dirk Grumwald, Tadayoshi Kohno, Damon McCoy, and Douglas Sicker, "Shining Light in Dark Places: Understanding the TOR Network." August 7, 2007. http://www.cs.washington.edu/homes/yoshi/papers/Tor/PETS2008_37.pdf.

BBC News. "LulzSec Hackers Claim CIA Website Shutdown." June 16, 2011. http://www.bbc.co.uk/news/technology-13787229.

Berger v. New York, 388 U.S. 41 (1967).

Berkman Center for Internet and Society. "Digital Natives: Lifecycle of a Digital Dossier." August 13, 2008. http://cyber.law.harvard.edu/node/4535.

Bernard, Doug. “Does Social Media Help or Hurt Terrorism.” *The Voice of America, Digital Frontiers*, January 21, 2012. http://blogs.voanews.com/digital-frontiers/2012/01/21/does-social-media-help-or-hurt-terrorism/.

Bishop, Joel P. *Bishop Commentaries on Criminal Law*. 670, 1882.

Blackstone, William. “Commentaries on the Law of England.” 1769. http://www.lonang.com/exlibris/blackstone.

Bloustein, Edward J. “Privacy As an Aspect of Human Dignity: An Answer to Dean Prosser.” *39 N.Y.U. L. Rev* 962 (1964).

The Boston Society. “History of the Old State House Building.” 2012. http://www.bostonhistory.org/?s=osh&p=history.

boyd, danah. “Facebook’s Privacy Trainwreck.” *Convergence: The International Journal of Research into New Media Technologies* 14, no. 1 (2008): 13. http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf

———. “Taken Out of Context: American Teen Sociality in Networked Publics.” *Dissertation*, *University of California, Berkeley*. 2008. http://www.danah.org/papers/TakenOutOfContext.pdf.

———. “Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life.” In *MacArthur Foundation Series on Digital Learning—Youth, Identity, and Digital Media Volume*, edited by David Buckingham. Berkman Center Research Publication No. 2007–16. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. 31. Cambridge, MA: MIT Press, 2007. http://ssrn.com/abstract=1518924.

boyd, danah, and Alice E. Marwick. “Social Privacy in Networked Publics: Teens’ Attitudes, Practices, and Strategies: A Decade in Internet Time.” *Symposium on the Dynamics of the Internet and Society*. September 2011. http://ssrn.com/abstract=1925128.

———. “The Drama! Teen Conflict, Gossip, and Bullying in Networked Publics: A Decade in Internet Time.” *Symposium on the Dynamics of the Internet and Society*. September 2011. http://ssrn.com/abstract=1926349.

boyd, danah, and Nicole Ellison. “Social Network Sites: Definition, History and Scholarship.” *Journal of Computer-Mediated Communication* 13, no. 1 (2007): article 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

Boyd v. U.S., 116 U.S. 616 (1886).

Brandeis, Louis D., and Samuel Warren. “The Right to Privacy.” *Harv. L. Rev. 4,* 193 (1890).

Bratman, Ben E. “Brandeis and Warren’s the Right to Privacy and the Birth of the Right to Privacy.” *Tennessee L. Rev.*, 69, *U. of Pittsburgh Legal Studies Research Paper*. 2002. SSRN: http://ssrn.com/abstract=1334296.

Briggs v. Am. Air Filter Co., 630 F.2d 414 (5th Cir. 1980).

Cannon, Robert. “ECPA Title I: The Wiretap Act: Exceptions.” *Cybertelecom* http://www.cybertelecom.org/security/ecpaexception.htm

———. “The Patriot Act.” *Cybertelecom*. 2012. http://www.cybertelecom.org/security/patriot.htm

CBS News. “Terrorist Groups Recruiting Through Social Media.” *CBC News Technology and Science*, January 10, 2012. http://www.cbc.ca/news/technology/story/ 2012/01/10/tech-terrorist-social-media.html

Chen, Hsinchun. *Dark Web: Exploring and Data Mining the Dark Side of the Web*. Tucson, AZ: Springer, 2011.

The China Post. “Cut to Cell Phone Service Sparks Controversy in SF.” August 15, 2011. http://www.chinapost.com.tw/international/americas/2011/08/15/313394/Cut-to.htm

City of Ontario, California, et al. v. Quon et al, 130 S.Ct. 2619 (2010).

Congress of the United States. Office of Technology Assessment. “Electronic Surveillance and Civil Liberties.” NTIS Order #PB86-123239, 39. 1985. http://www.fas.org/ota/reports/8509.pdf.

Couillard, David A. “Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing.” *Minnesota L. Rev., 93, 2205*. June 2009. SSRN: http://ssrn.com/abstract=1832982.

Council of Europe. Convention on Cybercrime. November 12, 2001. http://conventions.coe.int/treaty/en/treaties/html/185.htm.

Cranor, Lorrie F., Patrick Gage Kelley, Aleecia M. McDonald, and Robert W. Reeder. “A Comparative Study of Online Privacy Policies and Formats.” *Lecture Notes in Computer Science*, 5672/2009, 37-55, DOI: 10.1007/978-3-642-03168-7_3. 2009. http://www.springerlink.com/content/e2640gw68436054k/

Crispin v. Audigier, Inc., 717 F.Supp.2d 965 (2010).

Denning, Dorothy E. “Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy.” In *Networks and Net Wars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David F. Ronfeldt, RAND, 2001.

———. “Terror’s Web: How the Internet is Transforming Terrorism.” In *Handbook on Internet Crime*, edited by Yvonne Jewkes and Majid Yar. Willian Publishing, 2010.

Department of State. “Internet Freedom, About Internet Freedom at the State Department.” Remarks by Secretary of State Hillary Clinton. February 15, 2011. http://www.state.gov/e/eeb/cip/netfreedom/index.htm.

Digital Due Process Coalition. (n.d.). http://www.digitaldueprocess.org.

———. “Who We Are.” 2010. http://www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163.

DLP Coalition. Letter to the Honorable Patrick J. Leahy Chairman United States Senate Committee on the Judiciary. April 6, 2011. http://www.scribd.com/doc/52390394/DLP-Coalition-Letter-on-ECPA.

Doyle, Charles, and Gina Stevens. “Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping.” *Congressional Research Service*. Order Code 98-326, 2008.

ECPA Reform and the Revolution in Cloud Computing. Hearing of the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights and Civil Liberties. 111th Cong., September 23, 2010.

———. *Hearing of the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights and Civil Liberties*. 111th Cong., September 23, 2010 (testimony of Cameron F. Kerry, General Counsel, United States Department of Commerce). http://www.judiciary.senate.gov/pdf/11-4-6%20Kerry%20Testimony.pdf.

———. *Hearing of the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights and Civil Liberties*. 111th Cong., September 23, 2010 (Testimony of Kevin Werbach). http://judiciary.house.gov/hearings/hear_100923.html.

ECPA Reform and the Revolution in Location Based Technologies and Services, Hearing of the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties. 111th Cong., June 24, 2010.

The Electronic Communications Act: Government Perspectives on Protecting Privacy in the Digital Age. *Hearing of the United States Senate Committee on the Judiciary*, 111th Cong., April 6, 2011.

The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age. Hearing of the Senate Committee on the Judiciary (Statement of Senator Patrick Leahy (D-Vt.), Chairman, Senate Committee on the Judiciary). September 22, 2010. http://judiciary.senate.gov/hearings/testimony.cfm?id=4776&wit_id=2629.

Electronic Communications Privacy Act Reform. *Hearing of the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties*. Serial No. 111–98, 111th Cong., May 5, 2010.

Electronic Communications Privacy Act and Legislative History. Public Law 99-508, *U.S. Statutes at Large* 100 (1986): 1848.

Electronic Privacy Information Center. “Wiretapping.” (n.d.). http://epic.org/privacy/wiretap/.

Entick v. Carrington, 19 Howell's State Trials 1030 (1765).

EPIC. “Electronic Communications Privacy Act-Reform.” (n.d.). http://epic.org/privacy/ecpa/default.html.

European Commission. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.* Official Journal L 281, 23/11/1995 P. 0031–0050*.* October 24, 1995.

———. *Draft Directive of the European Parliament and of the Council, on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data Brussels*. 2012/0010 (COD). January 25, 2012.

———. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation.* SEC(2012) 72/73 Final. January 25, 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

EUROPOL. “TE-SAT 2010: EU Terrorism Situation and Trend Report.” 2010. http://www.consilium.europa.eu/uedocs/cmsUpload/TE-SAT%202010.pdf.

Ex parte Jackson, 96 U.S. 727 (1877).

Facebook. “Facebook’s Privacy Policy.” December 22, 2010. http://www.facebook.com/policy.php.

———. “Information for Law Enforcement Authorities.” 2012. https://www.facebook.com/safety/groups/law/guidelines/.

———. “Statistics.” (n.d.). http://www.facebook.com/press/info.php?statistics.

Federal Bureau of Investigation. “Intelligence collection disciplines (INTs) in which the collection of publicly available information by the intelligence community has been deemed ‘open source intelligence.’” (n.d.). http://www.fbi.gov/about-us/intelligence/disciplines.

Federal Law Enforcement Training Center. “Legal Division Handbook.” 2010. http://www.fletc.gov/legal.

Flagg, v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008).

Flaherty, David H. *Privacy in Colonial New England*. University of Virginia Press, 1967.

Flemming, Robert. *Political Discourses, viz. Patriachal, or the Natural Power of Kings: the Free-Holders Grand-Inquest*. Google Books, 1680.

“Forensics.” *Cybertelecom*. 2012. http://www.cybertelecom.org/security/forensic.htm.

Franklin, Benjamin. Wikiquote. (n.d.). http://en.wikiquote.org/wiki/Benjamin_Franklin.

Galperin, Eva. “BART Pulls a Mubarack in San Francisco.” *Electronic Freedom Foundation*. August 12, 2011. https://www.eff.org/deeplinks/2011/08/bart-pulls-mubarak-san-francisco

Gonzales v. Google, Inc., No. 5:06-mc-80006-JW (N.D. Cal. motion to compel filed January 18, 2006).

Google. “Privacy Policy.” 2012. https://www.google.com/intl/en/policies/privacy/.

———. “Transparency Report.” 2011. http://www.google.com/transparencyreport/.

Google’s Opposition to the Government’s Motion to Compel in Gonzales v., Inc. No. 5:06-mc-80006-JW (N.D. Cal. Filed 2006). http://googleblog.blogspot.com/pdf/Google_Oppo_to_Motion.pdf

Grance, Tim, and Peter Mell. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology, Special Publication 800-145*, September 2011.

Grance, Tim, and Wayne Jancen. “Guidelines on Security and Privacy in Public Cloud Computing.” *National Institute of Standards and Technology, National Institute of Standards and Technology, Special Publication 800-144.* December 2011.

Hartzog, Woodrow N., and Frederic D. Stutzman. “Boundary Regulation in Social Media.” *The University of North Carolina At Chapel Hill.* October 8, 2009. http://ssrn.com/abstract=1566904.

Herridge, Catherine. “FBI Seeks Developers for App to Track Suspicious Social Media Posts, Sparking Privacy Concerns.” *Fox News.* February 16, 2012. http://www.foxnews.com/politics/2012/02/16/fbi-seeks-developers-for-app-to-track-suspicious-social-media-posts-sparking/.

Hintze, Mike. “Restoring Balance to American Surveillance Laws.” March 30, 2010. http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/03/30/restoring-balance-to-american-surveillance-laws.aspx.

IACP Center for Social Media. “IACP Social Media Survey.” 2011. http://www.iacpsocialmedia.org/Resources/Publications/2011SurveyResults.aspx.

Internet Crime Complaint Center. “2010 Internet Crime Report.” 2010. http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

Ivester, Matt. *lol....OMG: What Every Student Should Know About Online Reputation Management, Digital Citizenship and Cyberbullying*. Nevada Sierra Knight Publishing, 2011.

Jacobson, Michael. “Terrorist Financing and the Internet.” *Studies in Conflict & Terrorism* 33, no. 4 (2010): 353–63.

Katz v. U.S., 389 U.S. 347 (1967).

Kerr, Orin S. “A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It.” *Geo Wash L. Rev. 72* (2004): 1208.

———. “Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn’t.” *NW. U. L. Rev.* 97, no. 2 (2003): 607.

———. “Lifting the “Fog” of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law.” *Hastings L. J.* 54 (2003): 805.

———. “The Case for the Third-Party Doctrine.” GWU Legal Studies Research Paper No. 421. GWU Law School Pub. L. Research Paper No. 421. *Michigan L. Rev.* 107 (2009).

———. “Applying the Fourth Amendment to the Internet: A General Approach.” *Stanford L. Rev.* 62, no. 4 (2010).

———. “Searches and Seizures in a Digital World.” *George Washington Law School Pub. L. Research Paper No. 13, Harvard L. Rev.* 119 (2005): 531.

King v. U.S., 55 F.3rd 1193 (6th Cir. 1995).

Kotler, Steven. “'Dark Web' Project Takes on Cyber-Terrorism.” October 12, 2010. http://www.stevenkotler.com/Node/87.

Laslett, Peter. *John Locke, Two Treatises of Government*. New York: Mentor Books, 1963.

Legal Information Institute. “Probable Cause.” *Cornell University Law School*. 2010. http://www.law.cornell.edu/wex/probable_cause.

Lenhart, Amanda, and Mary Madden. “Teens, Privacy & Online Social Networks.” *Pew Internet and American Life Project.* April 18, 2007. http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx.

Lewis, Kevin, Jason Kaufman, Marco Gonzalez, Andreas Wimmer, and Nicholas Christakis. “Taste, Ties and Time.” *Berkman Center for Internet & Society*. September 25, 2008. http://cyber.law.harvard.edu/node/4682.

Lidsky, Lyrissa B. “Anonymity in Cyberspace: What Can We Learn from John Doe?” University of Florida Levin College of Law Research Paper No. 2009-37. *Boston College L. Rev.* 50 (2009): 1.

Locke, John. *Two Treatises of Government*. Google Books, 1821.

Lupu, Yonatan. “The Wiretap Act and Web Monitoring: A Breakthrough for Privacy Rights?” *VA. J. L. & Tech.* 9, no. 3 (2004).

MacKinnon, Rebecca. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. Philadelphia: Basic Books, 2012.

Madden, Mary. “Privacy Management on Social Media Sites.” *Pew Internet and American Life Project*. February 24, 2012. http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx.

Madden, Mary, and Aaron Smith. “Reputation Management and Social Media.” *Pew Internet and American Life Project*. May 2010. http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx.

Mayer-Shonberger, Viktor. *Delete the Virtue of Forgetting in the Digital Age*. Princeton: University Press, 2009.

McDonald, Aleecia, and Lorrie F. Cranor. “The Cost of Reading Privacy Policies.” *ACM Transactions on Computer-Human Interaction* 389, no. 3 (2008): 1. http://www.mendeley.com/research/the-cost-of-reading-privacy-policies/.

McIntyre v. Ohio, 514 U.S. 334 (1995).

Michigan Dept. of State Police v. Slitz, 110 S.Ct. 2481 (1990).

Morozov, Evgeny. *The Net Delusion: How Not to Liberate the World*. Allen Lane, 2011.

The National Commission on Terrorist Attacks Upon the United States, The 9-11 Commission Report. New York; W.W. Norton & Company, 2003.

National Science Foundation. “University of Arizona, Dark Web Project: Scientists Use the “Dark Web” to Snag Extremists and Terrorists Online.” *Press Release 07-118*. September 10, 2007. http://www.nsf.gov/news/news_summ.jsp?cntn_id=110040.

Nelson, Kristopher. “Applying the United States Fourth Amendment to Data in the Cloud.” *Social Media Today.* January 20, 2010. http://socialmediatoday.com/index.php?q=all/14232.

Net Industries. “Search and Seizure-The Fourth Amendment: Origins, Text, and History.” 2012. http://law.jrank.org/pages/2014/Search-Seizure-Fourth Amendment.

Nissenbaum, Helen. “Privacy As Contextual Integrity.” *Wash. L. Rev.* 79, no. 119 (2004). http://ssrn.com/abstract=139144.

Norris, Michelle. “Interview with Alec Ross Advisor to Hilary Clinton, re Internet Freedom and the U.S. State Department.” *National Public Radio, All Things Considered.* February 17, 2011. http://www.npr.org/2011/02/17/133847146/Internet-Freedom-And-U-S-State-Department.

NPR All Things Considered. “What the FBI Wants in a Social Media Monitoring App.” January 30, 2012. http://www.npr.org/blogs/alltechconsidered/2012/01/31/ 146090425/what-the-fbi-wants-in-a-social-media-monitoring-app.

O’Neill Communication. “All the Different Types of Social Media.” (n.d.). http://www.oneillcommunications.com/2010/04/all-the-different-types-of-social-media/.

O’Reilly, Tim. “What is Web 2.0.” *O’Reilly Media*. September 30, 2005. http://oreilly.com/web2/archive/what-is-web-20.html.

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

Organization of Economic Cooperation and Development. “Participative Web: User-generated content. OECD Committee for Information, Computer and Communications Policy report, DSTI/ICCP/IE(2006)7/FINAL.” April 2007. http://www.oecd.org/dataoecd/57/14/38393115.pdf.

Otis, James. “Against Writs of Assistance.” *National Humanities Institute*. February 1761. http://www.nhinet.org/ccs/docs/writs.htm.

Palfrey, John. “The Public and the Private at the United States Border with Cyberspace.” *Miss. L. J.* 78, no. 2 (2008): 241–292.

Palfrey, John, and Urs Gasser. *Born Digital*. New York: Basic Books, 2008.

Pan, Joann. “FBI Uses Social Media to Catch Murder Suspect Who Stole $2.3 Million.” *mashable*. March 9, 2012. http://mashable.com/2012/03/09/kenneth-konias-wanted-fugitive/.

Peagler, Annette. “Florence Police Use Facebook to Catch Criminals.” *KyPost*. March 13, 2012. http://www.kypost.com/dpps/news/region_northern_kentucky/florence/florence-police-use-facebook-to-catch-criminals_7298753.

Pippard, Tim. “Jane’s Strategic Advisory Services: Al-Qaeda—Jihadists Use of the Internet.” *IHS Jane’s.* April 16, 2009. http://mspublicsafetysymposium.com/media/pdf/PDF_Presentations/PDF_Files/Al-Qaeda_Jihadist_Use_of_the_Internet_Keynote.pdf.

Prensky, Marc. “Digital Natives, Digital Immigrants.” *On the Horizon* 9, no. 5 (October 2010). http://www.marcprensky.com/writing/Prensky%20%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf.

Quon v. Arch Wireless Operating Co., 529 F.3d 892 (2008).

Reid, Edna. “FBI Analysis Jihadi Extremists Videos.” *FBI Forensic Science Communications* 11, no. 3 (July 2009). http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2009/research_tech/2009_07_research01.htm.

Reporters Without Borders. “Enemies of the Internet: Countries Under Surveillance.” March 12, 2010. http://en.rsf.org/IMG/pdf/Internet_enemies.pdf.

Restatement of the Law, Second, Torts, Sec. 652. *The American Law Institute*, 1997.

Roberts, Lawrence G., and Barry D. Wessler. “Computer Network Development to Achieve Resource Sharing.” *Proceedings of AFIPS.* 1970. http://www.packet.cc/files/comp-net-dev.html.

Schneier, Bruce. “Lessons from the TOR Hack: Anonymity and Privacy Are Not the Same.” *Wired News*. September 20, 2007. http://www.wired.com/politics/security/commentary/securitymatters/2007/09/security_matters_0920?currentPage=all.

Semayne’s Case 5 Co. Rep. 91a, 91b, 77 Eng. Rep. 194 (K. B. 1603). 1604. http://www.law cornell.edu/ancon/html/amd4frag1_user.html.

Senate Select Committee to Study Governmental Operations. “Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Book III.” *The Church Commission*. April 14, 1976.

Sinopoli, Joe. “Social Media Now a Tool for Crimefighters, Including Downers Grove Police.” *mysururbanlife.com*. March 7, 2012. http://www.mysuburbanlife.com/lisle/topstories/x1785613234/Social-media-now-a-tool-for-crimefighters-including-Downers-Grove-police.

Sitimore, Curtis. “To Benno Schmidt Jr., There Can Be No Free Society Without Privacy.” *Christian Science Monitor*. December 5, 1986. http://www.csmonitor.com/1986/1205/zfree3b.html#.ThRqspPmwIs.e-mail.

Smith, Aaron. “Web 2.0.” *The Pew Internet and American Life Project.* November 15, 2011. http://www.pewinternet.org/topics/Web-20.aspx.

Smith, Robert E. “Ben Franklin’s Web Site: Privacy and Curiosity from Colonial America to the Internet.” *Privacy Journal*. 2000. http://www.worldcat.org/title/ben-franklins-web-site-privacy-and-curiosity-from-plymouth-rock-to-the-internet/oclc/43615216.

Smith, Russ. “IP Address: Your Internet Identity.” *Consumer.Net*. March 29, 1997. http://www.ntia.doc.gov/legacy/ntiahome/privacy/files/smith.htm.

Solove, Daniel J. “A Brief History of Information Privacy Law.” *Proskauer on Privacy, PLI, GWU Law School Pub. L. Research Paper No. 215*. (2006): 1–11. SSRN: http://ssrn.com/abstract=914271.

———. “A Taxonomy of Privacy.” *University of Pennsylvania L. Rev.* 154, no. 3 (2006): 477–479. *GWU Law School Pub. L. Research Paper No. 129.* SSRN: http://ssrn.com/abstract=667622.

———. “Conceptualizing Privacy.” *Cal. L. Rev.* 90, no. 1087 (2002).

———. “I’ve Got Nothing to Hide, and Other Misunderstandings of Privacy. *San Diego L. Rev., 44*. 2007, https://www.cs.drexel.edu/~greenie/privacy/solove.pdf

———. “Surveillance Law Reshaping the Framework. *Geo. Wash. L. Rev.* 72, no. 1264 (2004).

———. *Digital Person, Technology and Privacy in the Information Age*. New York: University Press, 2004.

———. *The Future of Reputation, Gossip, Rumor and Privacy on the Internet*. Yale University Press, 2007.

S. Rep. No. 99-541. Reprinted in 1986 U.S.C.C.A.N. 3555, 3564-65, 1986.

Spokeo. “Join.” (n.d.). http://spokeo.com.

Sprenger, Polly. “Sun on Privacy: ‘Get Over It’.” *Wired*. January 26, 1999. http://www.wired.com/politics/law/news/1999/01/17538.

Stanley, Jay, and Barry Steinhardt. “Bigger Monster, Weaker Chains.” *American Civil Liberties Union*. 2003. http://www.aclu.org/files/pdfs/privacy/bigger_weaker.pdf.

Steeves, Valerie. *Reclaiming the Social Value of Privacy, Lessons from the Identity Trail*. ch. 1. Oxford University Press, 2009. http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_11.pdf.

Steve Jackson Games, Inc. 816 F. Supp. at 442-43.

Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994).

Strandburg, Katherine J. “Home, Home on the Web, and Other Fourth Amendment Implications of Technosocial Change.” *Maryland L. Rev*. 70, no. 101 (2011). http://ssrn.com/abstract=1808071.

Sweeney, Latanya. “Simple Demographics Often Identify People Uniquely.” *Carnegie Mellon University, Data Privacy Working Paper 3*, 2000.

TechFreedom. “Letter to the Honorable Patrick J. Leahy Chairman United States Senate Committee on the Judiciary.” April 6, 2011. http://www.scribd.com/doc/52390394/DLP-Coalition-Letter-on-ECPA.

Theofel v. Farley-Jones, 341 F.3d 978 (9th Cir. 2003).

TOR Project. (n.d.). http://www.torproject.org.

U.S. Congress. House. Committee on the Budget. *Long-Term Sustainability of Current Defense Plans: Hearing before the Committee on the Budget.* 111th Cong. 1st sess., February 4, 2009.

U.S. Congress. House. *DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy*: *Hearing before Committee on Homeland Security, Subcommittee Counterterrorism and Intelligence*. 112th Cong., February 16, 2012. http://homeland.house.gov/hearing/ subcommittee-hearing-dhs-monitoring-social-networking-and-media-enhancing-intelligence.

U.S. Congress. House. *Electronic Communications Privacy Act Reform. Hearing of the House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Serial No. 111–98*. 111th Cong., May 5, 2010.

U.S. Congress. Senate. *The Electronic Communications Act: Government Perspectives on Protecting Privacy in the Digital Age*. *Hearing of the United States Senate Committee on the Judiciary*. 111th Cong., April 6, 2011.

U.S. House. *Do Not Track Kids Act of 2011*. 112th Cong. 1st sess., 2011. H. Doc 1895.

U.S. President. Executive Order no. 12,333. *United States Intelligence Activities*. 2008.

U.S. v. Jones, 565 U.S. __ (2012, January 23).

U.S. v. Miller, 425 U. S. 435 (1976).

U.S. v. Smith, 155 F.3d 1051 (9th Cir. 1998).

U.S. v. Torres, 751 F.2d 875 (7th Cir. 1984).

U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010).

United States Department of Justice. Computer Crime and Intellectual Property Section, Criminal Division. “Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.” 2009.

———. DOJ-The Online Investigations Working Group. “Online Investigative Principles for Federal Law Enforcement Agents.” November 1999. http://publicintelligence.net/department-of-justice-online-investigative-principles-for-federal-law-enforcement-agents/.

United States Postal Service. “Publication 100—The United States Postal Service—An American History 1775–2006: Colonial Times.” May 2007. http://about.usps.com/publications/pub100/pub100_002.htm.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Public Law 107–56, *U.S. Statutes at Large* 210 (2001): 2010.

University of Haifa. “Friend Request from Al-Qaeda.” *School of Communications and Media Relations*. January 7, 2012. http://newmedia-eng.haifa.ac.il/?p=5680.

Volokh, Eugene. “Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You.” *Stan. L. Rev.* 52, no. 1049 (1999).

W3C. “W3C Semantic Web Activity.” 2011. http://www.w3.org/2001/sw/.

“The Way Back Machine.” *Welcome to the Archive*. (n.d.). http://www.archive.org/index.php.

Webopedia. “Steganography.” *Webopedia Computer Dictionary*. (n.d.). http://www.webopedia.com/TERM/S/steganography.html.

Weimann, Gabriel. “al-Qai’ida’s Extensive Use of the Internet. *Combating Terrorism Center at West Point, CTC Centennial* 1, no. 2 (January 2008): 607. http://www.ctc.usma.edu/posts/al-qaida%E2%80%99s-extensive-use-of-the-internet.

———. “Terror on the Internet: The New Arena, the New Challenge.” *The United States Institute of Peace*, 2006.

Westin, Alan F. *Privacy and Freedom.* New York: Atheneum, 1967.

The White House. “Consumer Data Protection in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Digital World Economy.” February 23, 2012. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Whitten, Chris. “The Federalist Papers.” *FoundingFathers.Info*. 2010. http://www.foundingfathers.info/federalistpapers/.

Wohlson, Marcus. “FBI Seeks Digital Tool to Mine Entire Use of Social Media.” *Chicago Times.* February 12, 2012. http://www.suntimes.com/news/nation/10605702-418/fbi-seeks-digital-tool-to-mine-entire-universe-of-social-media.html.

Woo, Jisuk. “The Right Not To Be Identified: Privacy and Anonymity in the Interactive Media Environment.” *New Media & Society* 8, no. 6 (2006): 949–967. http://www.forum.newmediaandsociety.com.

Xiang, Zhang. “Britain’s U-Turn Over Web-Monitoring.” *Xinhuanet*. August 12, 2011. http://news.xinhuanet.com/english2010/indepth/2011-08/12/c_131046237.htm.

York, Jillian C. “The Right to Anonymity Is a Matter of Privacy.” *Electronic Freedom Foundation*. January 28, 2012. https://www.eff.org/deeplinks/2012/01/right-anonymity-matter-privacy.

Yu, Roger. “Social Media Role in Police Cases Growing.” *USAToday*. March 18, 2012. http://www.usatoday.com/tech/news/story/2012-03-18/social-media-law-enforcement/53614910/1.

Zahorsky, Ingmar. “Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum.” *University for Peace, Peace and Conflict Monitor*. August 1, 2011. http://www.monitor.upeace.org/innerpg.cfm?id_article=816.

Zimmer, Michael. “But the Data Is Already Public: On the Ethics of Research in Facebook.” *Springer Science Business Media* 12, no. 4 (2010): 321. http://www.springerlink.com/index/q1v7731u26210682.pdf.

Zoufal, Donald R. ““Someone to Watch Over Me?” Privacy and Governance Strategies for CCTB and Emerging Surveillance Technologies.” Master’s thesis, Naval Postgraduate School, 2008.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

40 Stat. 1017-18 (1918).

Balebako, Rebecca, Lorrie Cranor, Pedro Leon, Richard, Shay, Blase Ur, and Yang Wang. “Why Johnny Can’t Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising.” *Carnegie Mellon CyLab, CMU-CyLab-11-017.* (October 31, 2011). http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html.

Belia, Patricia L., and Susan Freiwald. *Fourth Amendment Protection for Stored E-Mail*. University of Chicago, 2008.

boyd, danah, and Eszter Hargittai. “Facebook Privacy Settings: Who Cares.” August 2010. http://www.danah.org/papers/2010/FM-FacebookPrivacySettings.pdf.

Brandon, Arnold, Will DeVries, Charles H. Kennedy, Wilkinson Barker Knauer, and Julian Sanchez. “An ECPA for the 21st Century: The Present Reform Effort and Beyond.” *Cato Capitol Hill Briefing*, October 11, 2011.

Burr, Beckwith. “The Electronic Communications Privacy Act of 1986: Principles for Reform.” *Digital Due Process Coalition*. March, 2010. http://www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-.

Cohen, Julie E. “Privacy, Visibility, Transparency, and Exposure.” *University of Chicago L. Rev.* 2008. http://ssrn.com/abstract=1012068.

———. “Right to Read Anonymously: A Closer Look at “Copyright Management.” In cyberspace. *Conn. L. Rev 28, 981.* 1996. http://ssrn.com/abstract=17990.

Deibert, Ronald J., John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press, 2010.

Doyle, Charles. The USA PATRIOT Act: A Legal Analysis. April 15, 2002. *Congressional Research Service,* Order Code RL3137.

Electronic Communication Privacy Act, 18 U.S.C.A. (1986), sec. 2510.

Electronic Communication Privacy Act Amendments Act of 2011, S. 1011, Section II Prohibition on Voluntary Disclosure of Content (2011).

Hafner, Katie, and Matt Richtel. “Google Resists U.S. Subpoena of Search Data.” *N.Y. Times*, January 20, 2006.

Henderson. Nathan C. “The Patriot Act’s Impact on the Government’s Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications.” *Duke L. J. 52, 179*, 2002.

Herman, Susan. N. *Taking Liberties: The War on Terror and the American Democracy*. Oxford University Press, 2011.

Hodge, Matthew J. “The Fourth Amendment and Privacy Issues on the “New” Internet: Facebook.com and Myspace.com.” *Illinois University L. J., 31, 95*, Fall 2006.

Intelligence Community Directive Number 301. “National Open Source Enterprise, (ICD) 301.” July 11, 2006. http://www.fas.org/irp/dni/icd/icd-301.pdf.

Jefferson, Thomas. “On the Omission of a Bill of Rights from the Constitution.” *Encyclopedia Britannica’s Guide to American Presidents*. 1787, December 20, 1787. http://www.britannica.com/presidents/article-9116913.

Kattan, Ilana. “Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud.” *13 Vanderbilt Journal of Entertainment and Technology Law* 617 (2011).

Kyllo v. U.S., 533 U.S. 27 (2001).

Levis, Christian. “Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy.” *Fordham Law Legal Studies Research Paper Fordham Intellectual Property, Media & Entertainment L. J.* 22, no. 1 (2011): 191.

Lynch, Jennifer. “Government Finds Uses for Social Networking Sites Beyond Investigations.” *Electronic Freedom Foundation.* August 10, 2010. http://www.eff.org/deeplinks/2010/08/government-finds-uses-social-networking-sites.

Martel, Frances. “Government Proposes Expansion of Intelligence Gathering to Social Media.” September 27, 2010. http://www.mediaite.com/online/federal-government-proposing-expansion-of-intelligence-gathering-to-skype-other-social-media/.

Marwick, Alice E., Diego Murgia-Diaz, and John Palfrey. “Privacy and Reputation (Literature Review).” Youth and Media Policy Working Group Initiative. *Berkman Center Research Publication No. 2010-5; Harvard Pub. L. Working Paper No. 10-29.* (2010).

Mello, John P. Jr. “Social Network Users' Main Focus Is Staying in Touch.” *The Pew Internet and American Life Project*. November 15, 2011. http://pewinternet.org/Media-Mentions/2011/Social-Network-Users-Main-Focus-is-Staying-in-Touch.aspx.

Mulligan, Deirdre. “Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act.” *George Washington L. Rev.* 72, no. 1557 (2004).

National Academy of Sciences. “Who Goes There: Authentication Through the Lens of Privacy.” *National Research Council Committee on Authentication Technologies and Their Privacy Implications.* 2003. http://www.nap.edu/openbook.php?record_id=10656&page=R1.

Ohm, Paul. “Parallel-Effect Statutes and E-Mail Warrants: Reframing the Internet Surveillance Debate.” *George Washington L. Rev.* 72, no. 1559 (2004).

Palfrey, John. “Testimony on Internet Filtering and Surveillance.” *Open Internet Initiative*. May 20, 2008. http://blogs.law.harvard.edu/palfrey/2008/05/20/testimony-on-internet-filtering-and-surveillance/.

Petrashek, Nathan. “The Fourth Amendment and the Brave New World of Online Social Networking.” *Marq. L. Rev.* 93, no. 1495 (2010).

Plourde-Cole, Haley. “Back to Katz: Reasonable Expectation of Privacy in the Facebook Age.” *Fordham Urban L. J.* 38 (2010).

Privacy Rights Clearinghouse. “A Review of the Fair Information Principles: The Foundation of Privacy Public Policy.” July 2010. https://www.privacyrights.org/ar/fairinfo.htm.

Reclaim Privacy.Org. (n.d.). http://www.reclaimprivacy.org.

Reding, Viviane. Vice President, Eur. Comm’n. “The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5.” January 22, 2012. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF.

Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000.

Rosenbach, Marcel, and Hilmar Schmudt. “The War on Web Anonymity.” *Spiegel Online.* August 5, 2011. http://www.spiegel.de/international/spiegel/0,1518,778138,00.html.

Scribner, C. “Subpoena to Google Inc. in ACLU v. Gonzales: Big Brother is Watching Your Internet Searches through Government Subpoenas.” *Comment and Casenote, U. Cin. L. Rev*. 75, no. 1273 (Spring 2007).

Serwen, Andrew B. ECPA Reform-Inconsistent Holdings on Social Media. *Foley & Lardner LLP, Privacy & Security Source*. December 16, 2011. http://www.privacysecuritysource.com/2010/10/02/ecpa-reform-inconsistent-holdings-on-social-media/.

Simmons, Joshua. “Buying You, the Government’s Use of Fourth-Parties to Launder Data About the People.” *Colum. Bus. L. Rev.* 950 (2009).

Slobogin, C. “Is the Fourth Amendment Relevant in a Technological Age?” *Vanderbilt Pub. L. Research Paper No. 10-64; Vanderbilt Law and Economics Research Paper No. 10-56*. January 4. 2011. http://ssrn.com/abstract=1734755.

Smith v. Maryland, 442 U.S. 735 (1979).

Stored Wire and Electronic Communications and Transactional Records (Stored Communications Act). 18 U.S.C.A. § 2701 (1986).

Suzlon v. Microsoft. Case No. 10-35793 (C.A. 9, Oct. 3, 2011).

Taslitz, Andrew. “Enduring and Empowering: The Bill of Rights in the Third Millennium: The Fourth Amendment in the Twenty-First Century.” *Technology, Privacy and Human Emotions*, *Law and Contemporary Problems* 65, no. 2 (2002): 125.

———. *Reconstructing the Fourth Amendment, a History of Search and Seizure. 1789–1868*. NYU Press, 2006.

Tene, Omer. “What Google Knows: Privacy and Internet Search Engines.” *Utah L. Rev.* (October 1, 2007). http://ssrn.com/abstract=1021490.

Tessler, Joelle. “Privacy Erosion: A Net Loss.” *Congressional Quarterly Weekly*, 2006.

U.S. Const. amend. IV.

U.S. Library of Congress. Congressional Research Service. *Terrorist Use of the Internet: Information Operations in Cyberspace*, by John Rollins, and Catherine Theohary. CRS Report R41674. Washington, DC: Office of Congressional Information and Publishing, March 8, 2011.

United States Department of Homeland Security. “The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security.” *Memorandum Number: 2008*. December 29, 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

———. Office of Operations Coordination and Planning. “Privacy Impact Assessment Publicly Available Social Media Monitoring and Situational Awareness Initiative.” June 22, 2010. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia.pdf.

United States Department of Justice. “Attorney General Guidelines for Domestic FBI Operations.” September 29, 2008. http://www.justice.gov/ag/readingroom/guidelines.pdf.

United States Federal Trade Commission. “Fair Information Practice Principles.” 2007. http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

Weimann, Gabriel. “How Modern Terrorism Uses the Internet. *The United States Institute of Peace*, March 2004.

Werner, Matthew. “Google and Ye Shall Be Found: Privacy, Search Queries and the Recognition of a Qualified Privilege.” *AllBusinees.com*. (n.d.). http://www.allbusiness.com/technology/software-services-applications-search-engines/10547212-1.html.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Post Graduate School
   Monterey, California