2014

The Right to Digital Privacy: Advancing the Jeffersonian Vision of Adaptive Change

Kerry Moller
Claremont McKenna College

CLAREMONT MCKENNA COLLEGE

THE RIGHT TO DIGITAL PRIVACY: ADVANCING THE JEFFERSONIAN VISION OF ADAPTIVE CHANGE

SUBMITTED TO

PROFESSOR GEORGE THOMAS

AND

DEAN NICHOLAS WARNER

BY

KERRY MOLLER

for

SENIOR THESIS

SPRING 2014
APRIL 28, 2014

ACKNOWLEDGMENTS

First and foremost, I would like to thank my reader, Professor George Thomas, for his guidance and praise throughout this process and for inspiring my interest in constitutional law. I would also like to thank my friends and my brother for their encouragement and good humor throughout the semester. Finally, I would like to thank my mom for her patience and encouragement and my dad for his invaluable advice and support throughout this process.

ABSTRACT

The relationship between privacy, technology, and law is complex. Thomas Jefferson's prescient nineteenth century observation that laws and institutions must keep pace with the times offers a vision for change. Statutory law and court precedents help to define our right to privacy, however, the development of new technologies has complicated the application of old precedents and statutes. Third party organizations, such as Google, facilitate new methods of communication, and the government can often collect the information that third parties receive with a subpoena or court order, rather than a Fourth Amendment-mandated warrant. Privacy promotes fundamental democratic freedoms, however, under current law, the digital age has diminished the right to privacy in our electronic communications data.

This work explores the statutory and constitutional law protecting our right to privacy, as well as the inadequacies that have developed with the digital revolution. With commonplace use of third parties to facilitate electronic communication, our courts and lawmakers must amend current laws and doctrines to protect the privacy of communications in the digital age. To provide clarity and appropriate data privacy protections, the following clarifications and amendments should be made to the third party doctrine and the Stored Communications Act (SCA): 1) third party doctrine should only apply to context data, 2) content data should be protected by the Fourth Amendment, 3) the SCA should eliminate the distinction between Remote Computing Services (RCS) and Electronic Communication Services (ECS) communications, and 4) the SCA should require warrants for all content data acquisition.

TABLE OF CONTENTS

INTRODUCTION

In 1816, Thomas Jefferson avowed:

> Laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths disclosed, and manners and opinions change with the change of circumstances, institutions must advance also, and keep pace with the times.[1]

Two centuries later, smartphones have become a commonplace means of internet access, tablets have begun to replace printed books, and the expansion of the internet has allowed us to access nearly any service or good with the touch of a button. Digital technology is fully integrated in our everyday lives as a means of communication, education, and services. The digital revolution, however, has presented several challenges for our laws and institutions to "keep pace with the times" in the balance between the Framers' notions of privacy and technological development.

Today, over 75% of Americans own a personal computer and use the internet.[2] With this development, the interaction between law, privacy, and technology has become more complicated. The Framers created the Fourth Amendment in response to writs of assistance allowing British guards to search through homes and possessions of American colonists.[3] However, the nature of the Fourth Amendment and the statutory protections for individual privacy has significantly changed with technological advancement, and our

---

[1] Susan Clair Imbarrato, *Declarations of Independency in Eighteenth Century*
[2] Thom File, "Computer and Internet Use in the United States," *U.S. Department of Commerce: Economics and Statistics Administration,* May 2013, accessed April 12, 2014, http://www.census.gov/prod/2013pubs/p20-569.pdf.
[3] Stephen J. Schulhofer, *More Essential Than Ever: The Fourth Amendment in the Twenty-First Century*, (New York: Oxford University Press, 2012) 3.

right to privacy has grown increasingly vague. Have our laws and institutions appropriately kept up with "the times" as Jefferson believed they should?

The National Security Agency's use of surveillance in the U.S. is perhaps one of the most pertinent examples of the relationship between the law, privacy, and technology in recent history. Alarmed with the U.S. government's invasion of citizen privacy, many citizens called on the Supreme Court to strike down the NSA's surveillance program under the Fourth Amendment. Others, however, articulated the balance required between individual liberties and national security, arguing in favor of surveillance programs. The rift between privacy and the law in the U.S. has been apparent since the beginning of our government and the Framers' desire to protect against unwarranted home searches. However, the rapid development of technology introduces a new weight to balance in the relationship between privacy and law. Is it reasonable to believe that our email messages or the movies we stream online will remain private information? The issue of privacy, technology, and the law has become quickly complicated in the past decade with the development of the internet. With ever-developing technological advancements, how do we ensure a reasonable degree of privacy in our communications? Furthermore, should the courts or should Congress be given the reigns to determine the future of our privacy?

A study completed by Pew Research Center's Internet Project and Carnegie Mellon University examined the degree of privacy that internet users expect.[4] Several key statistics from the Pew Center study illustrate the issue of privacy online and public perception of the protections guaranteed to citizens to protect privacy:

---

[4] Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden, "Anonymity, Privacy, and Security Online," *Pew Research Internet Project,* September 5, 2013, accessed April 14, 2014, http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

- 68% of internet users think that the U.S. needs better laws to protect online privacy.
- 24% of users think that statutory protections are suitable to current technology and privacy demands.
- 37% of users believe that it is possible to be anonymous online.
- 86% of users have attempted to increase their anonymity online by clearing cookies, using fake email addresses, or another means of decreased visibility.
- 55% of users have attempted to avoid information gathering by specific entities, such as the government or a company.[5]

Privacy in online and electronic communications has become an increasingly salient issue in the past decade, and many Americans are concerned with the amount of legal protection afforded to technological privacy.

Privacy allows an individual to control the information that he or she wants to reveal to others. Whether incriminating evidence to a robbery, medical information, or simply a picture of your mother stored on your cell phone, many individuals seek to protect personal information from public knowledge. Control over what can and cannot be revealed helps to protect against quick judgments, allowing an individual to present the version of his or herself that he or she desires.[6] The right to privacy, however, is complicated. As case law, statutory law, and dozens of journal articles have expressed, there are various considerations in conceptualizing the degree of privacy protection guaranteed to citizens, and with the adoption of technology, personal privacy has become increasingly unclear. Whereas an individual would be prohibited from opening another's letter sent in the mail from a friend, e-mail correspondence is much easier for unwelcome eyes to reach. Cell phones, computers, and other personal devices have become almost

---

[5] Ibid.
[6] Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America*, (New York: Random House, 2000), 11.

second nature to many; however, the degree of privacy in communications is much less robust than before the digital revolution.

The Fourth Amendment protects against unreasonable searches and seizures of homes and of personal information. However, the U.S. Constitution does not expressly guarantee the right to privacy. Although the Bill of Rights lacks an explicit declaration of privacy, many have understood privacy as an inherent guarantee as an American citizen. The definition and application of the right to privacy is unclear, particularly in regard to technology. Explaining the complexity of the right to privacy in the digital age, Professor Jeffery Rosen says:

> [i]n cyberspace the greatest threat to privacy comes not from nosy employers and neighbors but from the electronic footprints that make it possible to monitor and trace nearly everything we read, write, browse, and buy. Most Web browsers are configured to reveal to every Web site you visit the address of the page you visited most recently and your Internet Protocol address, which may—or may not—identify you as an individual user.[7]

A vast amount of information is stored in each web page visited, telephone call received, and text message sent.[8] These "footprints" enable governments, companies, and individuals to access information and data that would otherwise remain private. Very little legal fortification exists to protect our presumed private communications from government subpoena or other unwelcome eyes.

Diminished privacy in light of technological advancement has been at issue since the very beginnings of technology's development. Supreme Court Justice Louis Brandeis and attorney Samuel Warren explored the interaction between emerging technology and

---

[7] Ibid., 163.
[8] Ibid., 164.

privacy during the development of the camera in 1890. The two lawyers issued "The Right to Privacy" after reading a newspaper's discussion of a breakfast party that Warren hosted in celebration of his daughter's wedding.[9] Arguing in favor of a "general right of the individual to be let alone," Warren and Brandeis acknowledged the effect of new technologies on privacy, stating: "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[10] As the Justices recognized, technological advancement began to make it easier for the government, the press, and individuals to gain access to and to exploit information that they otherwise would not have obtained. However, the two men also understood that the right to keep information private "is lost only when the author himself communicates his production to the public, -- in other words, publishes it."[11] Various court cases have since attempted to establish where this line of "publishing" lies. However, with the introduction of technologies such as the internet and smart phones, this line is ambiguous, and personal privacy is left at risk.

The Supreme Court began to outline the right to privacy in regard to emerging technologies in the 1960s. In *Katz v. United States,* Justice John Marshall Harlan issued a concurring opinion illuminating the reaches of the Fourth Amendment. Harlan introduced an individual's "reasonable expectation of privacy," and explained that if someone presumes that an activity will be private and that this expectation is "reasonable," then an

---

[9] Ibid., 7.
[10] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* IV, no. 5, (December 1890).
[11] Ibid.

intrusion should be prohibited.[12] However, if an individual engages in an activity or conversation in the open, there is an understanding that the conversation or activity could be overheard, thus the individual does not have a reasonable expectation to privacy.[13] In addition, *Katz* introduced the distinction between context and content information. While the specific content of communications, such as the text of a message, is private, the context information, such as the numbers called on a phone, does not retain an expectation to privacy.[14] This distinction and what it means in the context of our right to privacy is further explored in Chapter 2, and it is later applied to the NSA's data surveillance program in Chapter 4.

The doctrine introduced by Justice Harlan in *Katz* is not easily applied to twenty-first century technology. In weighing the issue, many courts have split on various ideas of privacy as it relates to technologies, including in two cases that the Supreme Court is set to hear in the 2014 docket addressing law enforcement's ability to search the contents of a cell phone after an arrest, as well as several cases considering the constitutionality and legality of the NSA's surveillance program. As controversy surrounds the topic of privacy and technology, it is a common concern whether we have a reasonable expectation to believe that our digital and electronic communications, such as personal e-mail, text messages, and other information kept on phones and computers should be guaranteed privacy.

---

[12] Katz v. United States, 389 U.S. 347, 88 S. Ct. 507 (1967), in Cornell University Law School Legal Information Institute, http://www.law.cornell.edu/supremecourt/text/389/347 (accessed February 18, 2014).
[13] Ibid.
[14] Ibid.

In 1986, Congress attempted to advance protection in the digital age with the development of the Stored Communications Act (SCA). The SCA was enacted in response to the emergence of new methods of communication and to govern circumstances in which government and other organizations can access communications information stored with third parties. Congress also passed the Wiretap Act to address the collection of data and to forbid "intercepting" data without a warrant.[15] In enacting new protections, Congress argued:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening … [and] [v]oice communications transmitted via common carrier are protected … But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology.[16]

The SCA recognized the need for new laws to ensure communications privacy. However, the SCA was passed in 1986, and many of its provisions are no longer relevant to new devices. Since 1986, we have seen, for example, the development of the computer as a common household item and smart phones with the same computing ability as home computers. Furthermore, many services have entered the online realm, such as medical records, banking applications, and cloud storage of personal files. The SCA, although offering some protection, does not adequately protect new methods of communicating,

---

[15] Orin S. Kerr, "Use Restrictions and the Future of Surveillance Law," in *Constitution 3.0: Freedom and Technological Change,* ed. Jeffrey Rosen and Benjamin Wittes (Washington D.C.: 2011), 43.

[16] Quoted in Laura Arredondo-Santiteban, "Stealing Glances: Electronic Communications Privacy and the Necessity for New Legislation in the Digital Age," *North Carolina Journal of Law & Technology, Online Edition,* (2013).

and many district courts have interpreted the act very narrowly, excluding protection of new devices with personal data storage.[17]

Further complicating the privacy of electronic communications, both the SCA and the Supreme Court have acknowledged the "third party doctrine" in which individuals who reveal information to a third party cannot reasonably expect that information to remain private.[18] In *Miller v. United States,* the Court determined that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government...even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[19] Applying this doctrine, the Supreme Court has determined that communications conveyed to a third party, such as a phone company, internet service provider, or banking institution, are not guaranteed Fourth Amendment protection.[20] Based on the third party doctrine, the government can collect data from any company that collects or organizes personal data or transactions with a court order or subpoena, rather than probable cause and a warrant.[21] Because much of our communication today takes place by way of a third party, the government can fairly easily obtain our information. With easier access to communications, some may begin to monitor their communications. Journalists, for example, may shy away from contacting controversial political groups out

---

[17] Ibid.
[18] Orin S. Kerr, "The Case for the Third-Party Doctrine," *Michigan Law Review* 107, (2008): 561.
[19] Christopher Slobogin, "Is the Fourth Amendment Relevant in a Technological Age?" in *Constitution 3.0: Freedom and Technological Change,* ed. Jeffrey Rosen and Benjamin Wittes (Washington D.C.: 2011), 17.
[20] Ibid.
[21] Ibid.

of fear that the government will obtain the information and assume that it is being used for an illicit purpose. As demonstrated by the Pew Center's research, many Americans are concerned with the amount of information collected by third parties, and thus increased data collection could endanger freedom of expression through the internet and other means of communication.

Rulings in cases involving access to electronic communications information have been largely inconsistent among the courts, with various courts splitting decisions on similar cases. Technology has become an integral part of our lives in the past decade, however, with this adoption, our privacy has diminished and much of our information has become more public. Courts have limited the scope of the Fourth Amendment in regard to technology with the third party doctrine, and statutory law protects only certain aspects of communications. As the controversy of our data privacy grows, how will the right to privacy and the needs of national security be balanced?

Chapter 1 of this work explains the value of privacy as we have viewed it in society. Warren and Brandeis were among the first scholars to address the issue, and many have assumed that American citizens are guaranteed privacy in personal matters. Courts and Congress have aptly outlined our privacy rights, and Chapter 1 provides an informational primer on Supreme Court cases and statutory law that has defined the guarantee to privacy. Chapter 2 addresses the third party doctrine and the Stored Communications Act (SCA). Each phone call made, website visited, or email sent is recorded and stored by third party companies as it travels to its destination. The Supreme Court established that once information is conveyed to a third party, the expectation to privacy in that information diminishes – and this complicates the right to privacy in our

communications in the digital age. To help guide access to third party communications information, Congress created the SCA, which provides specific protection to stored communications information. Both the third party doctrine and the SCA are controversial and do not strongly protect the right to privacy in electronic communications.

Chapter 3 provides an evaluation of the NSA's data surveillance program under the third party doctrine and illuminates its effects on the SCA. After specifics of the NSA's secret program were revealed in 2013, many American citizens became greatly concerned with privacy in communications information. However, various statutes have complicated the application of the third party doctrine to the NSA's data collection, and the future of the program remains unclear. Chapter 4 assesses the need for updated privacy protections in regard to both surveillance programs and to traditional information collection by law enforcement. The Fourth Amendment should protect the contents of our communications, just as the contents of a mailed letter are protected from unreasonable search and seizure. Current laws and third party jurisprudence allow access to content information with a subpoena or court order, which are much easier to obtain. Privacy in electronic communications has become an important issue for Americans, and both the SCA and the third party doctrine should be amended to more aptly address new methods of communication. Our right to privacy is at risk, and only if the courts and Congress update current protections will our information be protected.

CHAPTER 1: THE RIGHT TO PRIVACY

The Value of Privacy

Privacy as we value it today is not as simple as the right to secrecy in personal matters. Rather, privacy exists as Warren and Brandeis' "right to be let alone" and the "right to control" personal information in the public sphere.[1] The two lawyers assert that individuals have the "right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[2] Although some matters of privacy are simpler, such as the right to privacy when using the restroom, the relationship between privacy and technology is complicated and ever-changing. Warren and Brandeis' conception of privacy is not restricted to past technologies. Instead, Warren and Brandeis recognized the development of technology and illuminated fundamental, unchanging values of privacy to remain constant through technology's development. However, the line between an invasion of privacy and access to information is muddled. Courts have struggled to define and apply privacy to technological advancement. With rapid technological change, it is important to more clearly articulate the right to privacy and its guarantees in relation to technology and data.

Ten years after Warren and Brandies' article was published, courts and legislatures began to outline the right to privacy by introducing invasions of privacy torts.[3] Legislation had not yet truly addressed the issue of privacy, however, many court cases emerged to help define invasions of privacy. In the 1970s, tort law specialist

---

[1] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* IV, no. 5, (December 1890).
[2] Ibid.
[3] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, (New York: New York University Press, 2004), 59.

William Prosser completed a survey of privacy cases to determine the court's conception of privacy law after Warren and Brandeis published "The Right to Privacy."[4] Prosser identified four divisions of privacy in tort law: "intrusion upon seclusion," characterized as intrusion into one's private affairs; "public disclosure of private facts," explained as a tort oriented toward the press to protect against disclosure of a private matter; "false light" torts similar to libel and slander; and "appropriation" to use the name or likeness of another.[5] Although these tort areas help to define the scope of privacy law, it is difficult to discern when, for instance, peering into an individual's online information triggers an invasion of privacy. As explained by data privacy scholar Daniel Solove, it is especially difficult to pin down technological privacy in relation to the "information flows" that characterize much of today's personal data activity.[6] Tech and online matters often include a "multitude of actors, with a vast array of motives and aims, each doing different things at different times," which makes it difficult to define which actions are private and which are not.[7] Courts have not clearly defined how to apply the law to dynamic online activities and applications.

Some believe that the right to privacy can weaken public safety by inhibiting government from obtaining information about criminals.[8] However, privacy is more complex than the criminal information collected by the government and police. Privacy encompasses e-mail accounts, bank statements, medical prescriptions, personal letters,

---

[4] Ibid, 59.
[5] Ibid, 59-60
[6] Ibid, 61-62.
[7] Ibid.
[8] Stephen J. Schulhofer, *More Essential Than Ever: The Fourth Amendment in the Twenty-First Century,* (New York: Oxford University Press, 2012), 15.

conversations with others, and online activity. Although many are not in violation of the law and do not possess incriminating information against themselves or others, there is value in protecting conversations, religious beliefs, political views, and other personal information. It is unlikely that an individual would consent for someone to post all of their private records and information on the internet for others to view, and the right to privacy helps to guarantee control over personal information. Law professor Stephen Schulhofer explains privacy as "indispensable for the capacity to feel at peace, to try out new ideas, to think and grow as an independent individual."[9] The guarantee of privacy allows citizens to define their beliefs and ideas without fear of ridicule or comment from others. Lacking privacy, citizens may feel that they cannot exercise their political or religious beliefs without being ostracized by fellow citizens.

Privacy protections are necessary to uphold essential principles of democracy and American values and freedoms. As Supreme Court Justice Sonia Sotomayor comments in *United States v. Jones,* "[a]wareness that the government may be watching chills associational and expressive freedoms."[10] The guarantee to privacy helps to maintain fundamental values, such as the right to associate and to express one's beliefs without fearing that the government may obtain that information. Solove explains the complications of the digital revolution and democratic freedoms, stating:

> [P]rivacy of associations is becoming more difficult in a world where online postings are archived, where a list of the people a person contacts can easily be generated from telephone and email records, and where

---

[9] Ibid.

[10] Olmstead v. United States, 277 U.S. 438, 48 S. Ct. 564 (1928), in Oyez Legal Information Institute, http://www.oyez.org/cases/1901-1939/1927/1927_493 accessed March 12, 2014).

> records reveal where a person travels, what websites she visits, and so on.[11]

The digital revolution brought ease of communication and access to information, however, online associations, such as religious group activity or communications with others, are much easier for government actors or other individuals to obtain. The web is largely open and accessible, and many online activities are not as private as many assume. However, where can we draw a line to guard freedoms such as the right to associate in cyberspace? We reasonably expect privacy in various areas of the internet and technology, such as personal emails and medical information. However, it is increasingly difficult to maintain privacy in these areas. Despite laws and constitutional provisions to help protect privacy, our personal information is not strongly guarded.

Privacy Protection in Law

For the first century of the U.S. as a nation, government violations of privacy were mainly limited to tangible searches of homes and personal documents. However, technological development created new avenues for privacy violations. Congress enacted various pieces of legislation to protect privacy in several matters; however, privacy legislation has been focused and does not protect the wide range of potential privacy invasions created by information and technology usage. For example, few legislative acts protect state and local records and records from department stores, libraries, charities, and other merchants, which leaves large holes in privacy protection.[12]

Several pieces of legislation have been enacted to protect personal privacy in specific areas. The Family Educational Rights and Privacy Act of 1974 (FERPA)

---

[11] Solove, 63.
[12] Ibid.

provides an example of focused legislation to guard a student's right to privacy. FERPA protects a student's transcripts and educational information from wrongful disclosure.[13] Protecting educational information privacy, FERPA allows students to control the use of their records. Another example of privacy legislation was enacted in response to Robert Bork's controversial Supreme Court nomination battle. Bork's video rental records were disclosed during the nomination process, and many believed that disclosure of such information was a violation of Bork's privacy. Subsequently, the Video Privacy Protection Act (VPPA) of 1988 was enacted to protect an individual's video store records.[14] Although FERPA and the VPPA are only two examples of legislation to protect personal privacy, the two acts demonstrate the focused nature of privacy legislation. Legislation functions well to provide some privacy protection, however, with extreme focus, acts are not often responsive to technological changes. Legislation has helped to define the rights to privacy in particular matters, however, many areas have been left unprotected.

State and United Nations Privacy Protection

Although the U.S. Constitution does not address privacy, several states expressly guarantee privacy protection in their constitutions. Florida's Constitution, for example, states that "[e]very natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."[15] Likewise, California embraces privacy as an inalienable right, stating, "[a]ll

---

[13] Ibid., 69.
[14] Ibid.
[15] "Privacy Protections in State Constitutions," *National Conference of State Legislatures,* last modified December 11, 2013, accessed March 12, 2014,

people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[16] However, there are only a handful of states that acknowledge the right to privacy in their constitutions, and as demonstrated by the NSA controversy discussed later in this work, the right to privacy can be difficult to enforce when considering the capability of new technologies and the importance of preventing threats to national security.

In addition to state acknowledgment of privacy rights, the United Nations has also addressed the right to privacy in light of emerging technologies. In 2013, the United Nations drafted a resolution to preserve individual privacy. Named "The Right to Privacy in the Digital Age," the resolution acknowledges the rapid development of technology and the necessity to respond with appropriate privacy protections. The resolution notes that invasion of digital privacy may trigger UN Human Rights Violations, as well as UN Civil and Political Rights violations.[17] Privacy, the resolution explains, helps to maintain truly democratic societies and freedom of expression.[18] The resolution acknowledges that "concerns about public security may justify the gathering and protection of certain sensitive information, [however,] States must ensure full compliance with their obligations under international human rights law" to ensure democratic, human rights,

---

http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

[16] Ibid.

[17] United Nations, Third Committee, *The Right to Privacy in the Digital Age,* 68th sess., agenda item 69 (b), (November 2013).

[18] Ibid.

and political principles.[19] Discussed more fully later in this work, many allege that the NSA's surveillance program violates constitutional and statutory law. The UN resolution recommends that nations review their "surveillance of communications [and] their interception and collection of personal data" to verify compliance with national and international law.[20] Although the resolution does not have binding power on nations to review their programs and reform their laws to ensure personal information privacy, the resolution helps to call attention to the kinds of invasions of privacy that have become a reality in the past decade and the importance of preserving the right to privacy in light of the digital revolution. The resolution calls for transparency and oversight to ensure privacy protections.

The Fourth Amendment's Privacy Protections

Warren, Brandeis, several Supreme Court opinions, and a few state constitutions have illuminated that privacy should be valued as an inherent right. It is difficult, however, to define privacy in relation to technology. Neither legislative nor constitutional precedent provides sweeping definitions of privacy that can be easily applied to the dimensions of privacy in technology and electronic communications. The U.S. Constitution does not explicitly address the right to privacy. However, several court cases have helped to define the right to privacy and the instances in which we maintain a reasonable expectation to privacy. In a dissenting opinion in *Olmstead v. United States,* Justice Brandeis recognized the difficulty of preserving privacy in the shadow of technological advancement and expressed that, "discovery and invention have made it

[19] Ibid.
[20] Ibid.

possible for the government . . . to obtain disclosure in court of what is whispered in the closet."[21] Advancement in technology has made it easier for the government to obtain incriminating or private information from citizens. However, adequate legal privacy protections have not accompanied the expansion of technology.

The Fourth Amendment offers privacy protection against government actors performing unreasonable searches and seizures. Originally proposed by James Madison, the text of the Fourth Amendment states:

> 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.[22]

When the amendment was proposed, Americans wanted to protect against the British army's "general warrants," in which soldiers could perform searches and seizures with or without evidentiary basis. [23] To guard against general searches, the Amendment explains that the government can search personal information and possessions under the Amendment's provisions, however, searches must be focused, controlled, and justified, and the Amendment does not apply to information and objects in plain view.[24] However, the text is fairly ambiguous and neither its language nor the history of the Amendment helps to clearly define the Amendment's application to technology.[25]

---

[21] Olmstead v. United States.
[22] U.S. Constitution, amend. 4, in Cornell University Law School Legal Information Institute, http://www.law.cornell.edu/constitution/fourth_amendment, accessed March 11, 2014.
[23] Silas J. Wasserstrom, "The Fourth Amendment's Two Clauses," *American Criminal Law Review,* (1988): 1392.
[24] Solove, 188.
[25] Wasserstrom, 1389-1392.

The Fourth Amendment is often referenced as a means for government officials to discover criminal evidence. The Amendment's primary function, however, is as a protection to non-criminals. The Fourth Amendment protects the innocent from unreasonable searches and invasions of privacy, ensuring that government officials cannot search or seize a citizen's personal information or possessions without reasonable suspicion of criminal activity. As Schulhofer explains, the Fourth Amendment guarantees privacy to help "[foster] the sense of personal security that is necessary for individual autonomy and political liberty in a free society."[26] It ensures that government actors will not search citizens arbitrarily. Its use to protect individuals from unlawful searches and seizures helps to ensure a degree of privacy, thus allowing citizens to freely express themselves without fear of unreasonable government seizure of their information. With the development of technology, however, searches that may have been previously been impossible to undertake without violating privacy are much more accessible, and the right to privacy in the context of technology is unclear.

Katz and Olmstead

Several Supreme Court cases have addressed technology and the right to privacy. Two such cases are *Olmstead v. United States* and *Katz v. United States*. Both cases demonstrate law enforcement's direct access to communication content via wiretap. Wiretaps access communications information directly from the source, rather than obtaining information from a third party such as a telephone company. In *Olmstead*, decided in 1928, the petitioner was accused of coordinating a bootlegging operation in violation of the National Prohibition Act. To collect evidence against him, law

[26] Ibid.

enforcement wiretapped Olmstead's office and home and listened to his telephone conversations. The Supreme Court was petitioned to determine whether the wiretap violated the Fourth and Fifth Amendments. The Court ruled that wiretapping did not violate Olmstead's rights and did not qualify as a search and seizure under the Fourth Amendment. Reasoning that the Fourth Amendment applies to tangible evidence, such as papers or possessions, the Supreme Court ruled the Fourth Amendment does not apply to conversations or other intangible information.[27] *Olmstead* set a precedent for application of the Fourth Amendment and defined that it only applies to tangible possessions and information. If the precedent had continued into modern times, the content of communications, such as phone conversations, emails, text message, and video calls would have very little protection from direct access by law enforcement.

The *Olmstead* precedent stood for nearly forty years until the Supreme Court again addressed the issue of communications content privacy in *United States v. Katz* in 1967. In *Katz,* the Supreme Court considered whether it was a violation of the Fourth Amendment to record incriminating conversations from the source of the call. Katz was accused of communicating illegal gambling information over the phone, and police placed eavesdropping equipment on a public phone to gather evidence against him. Overturning *Olmstead,* the Supreme Court determined that intruding on conversations without a warrant violated the Fourth Amendment. Justice Potter Stewart, writing the majority opinion in the 7-1 decision, explained that the "Fourth Amendment protects

[27] Olmstead v. United States.

people, not places."[28] The Court ruled that the Fourth Amendment extends to protect both tangible items, such as personal documents, as well as intangible conversations and data.

The search performed in Katz was focused and based in strong evidence that illegal information was being communicated on the phone. However, the Court explained that the police had not obtained a warrant and the conversation was not in public, thus Katz had a reasonable expectation to privacy in his conversation.[29] The Court stated:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[30]

Katz placed the call in a closed phone booth and assumed that the information conveyed would be private. This principle introduced the distinction between context and content information. Information knowingly conveyed to the public or to a third party does not retain Fourth Amendment rights, while contents of a communication are usually assumed private.[31] The distinction between content and context information is clearly demonstrated by *Ex parte Jackson,* in which the Supreme Court ruled that "[n]o law could empower the government, via its postal inspectors, to violate the protections afforded to the contents of sealed letters and packages by the Fourth Amendment."[32] Context information, such as the address on a letter, is openly conveyed and is not private information. Content information, such as the content of a mailed letter, is not openly

---

[28] Katz v. United States.
[29] Ibid.
[30] Ibid.
[31] Christopher R. Brennan, "Katz Cradle: Holding On to Fourth Amendment Parity in an Age of Evolving Electronic Communication," *William and Mary Law Review* 53, (2012): 1803.
[32] Ibid.

communicated, and thus one can assume that the information will remain private. With the amount of information transmitted on the internet and cell phones through third parties, this distinction becomes important in the digital age.

Aside from the distinction between context and content information, Justice John Marshall Harlan introduced a test to determine the expectation of privacy. In a concurring opinion, Justice Harlan argued that Katz held a reasonable expectation of privacy in his conversation.[33] Katz placed his call in a phone booth with the door shut and presumed that his conversation would be private. Harlan agrees that this expectation of privacy is reasonable and should be constitutionally protected.[34] Although it may be difficult to discern a defendant's expectation to privacy in each particular situation before the Court, Harlan argues that without a warrant and where an individual has a reasonable expectation of privacy, the individual's right to privacy should prevail.

In *Katz* and *Olmstead,* communications were accessed directly from the source and thus retain Fourth Amendment protection based on current precedent. Today, many of our communications take place via third parties, and the Supreme Court has established that information communicated to third parties often forfeits the right to Fourth Amendment protection in that information. The distinction between content and context introduced in *Katz* and *Ex parte Jackson* becomes an important consideration in the right to privacy in electronic communications received by third parties. Some courts and scholars have argued that the content of communications should retain Fourth Amendment protections, while the context information communicated to third parties

[33] Katz v. United States.
[34] Ibid.

gives up the right to privacy in that information. Others, however, contend that both context and content communication information conveyed to third parties have become so commonplace that they should retain Fourth Amendment protections despite being conveyed to multiple parties.

CHAPTER 2: CURRENT COURT AND LEGISLATIVE PROTECTIONS TO ELECTRONIC COMMUNICATIONS INFORMATION

Limited protection exists to preserve privacy in communications. In the past decade, courts and legislative measures have established that much of our communication information does not require a warrant to obtain. Nearly all of our communications today take place via third parties, and many court cases have established that citizens do not have a reasonable expectation to privacy in third-party communications information. Aside from the courts, legislation has also expressed that upon third party receipt of communication information, privacy in that information is extinguished. With increasing use of email and phone communications, are we giving up our right to privacy as we adopt new and convenient methods of communication?

Both the Supreme Court and Congress have endeavored to define the limits of data protection; the Supreme Court established the third party doctrine and Congress enacted the SCA. The Supreme Court's third party doctrine allows the government to seize information revealed to a third party without a warrant. Even if information is conveyed for a specific purpose, information is not protected from government search and seizure via court order or subpoena. Judges or partial prosecutors can issue subpoenas, and court orders only require "relevance" to an investigation.[1] Warrants, on the other hand, are evaluated by neutral judges and are based on "probable cause," a standard much higher than that of a subpoena or court order.[2] Third party communications companies, such as internet service providers (ISP), store customer

---

[1] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, (New York: New York University Press, 2004), 203.
[2] Ibid.

information in service databases accessible by subpoenas, court orders, or warrants. The Supreme Court has adopted the third party doctrine as a main tenant to decide the admissibility of third party searches.

Congress has also attempted to regulate data privacy. The Stored Communications Act (SCA) was enacted in 1986 as a part of the Electronic Communications Privacy Act, and it has remained the primary third party data privacy law since enacted. The SCA governs the ability for government and other parties to obtain information from electronic communications companies and defines the ability of third party communications companies to disclose the information that they receive. However, as technology continues to develop and as third parties become more entrenched as our main means of communication, should the law guarantee a higher degree of privacy in our third party communications information? The SCA and the third party doctrine provide basic substantive, explanatory means to define our current privacy rights, however, both leave something to be desired in regard to privacy guaranteed in our communications information. This section will explore the third party doctrine, legislative data protection, and when we can expect privacy in our electronic communications.

The Supreme Court and the Third Party Doctrine

The Supreme Court has established the third party doctrine to govern the privacy of communications that take place through third parties, including electronic communications information. Several cases demonstrate the Court's use of the third party doctrine and its role in society. Although originally applied to non-electronic communications, the doctrine has been adapted to electronic communications, such as

email and phone calls. Application to emerging technologies presents complications, particularly as we have begun to rely on third parties to facilitate communications. The doctrine, however, has long existed as a part of the judicial system and provides a bright-line rule to determine privacy in communications.

The Fourth Amendment's relationship with electronic communications and internet communications is complex. Kerr, explaining the ambiguity in applying the Fourth Amendment to the internet, says:

> A user does not have a physical "home," nor really any private space at all. Instead, a user typically is owned by a network service provider, such as America Online or Comcast. Although a user may think of that storage space as a "virtual home," in fact that "home is really just a block of ones and zeros stored somewhere on somebody else's computer. This means that when we use the Internet, we communicate with and through that remote computer to contact other computers. Our most private information ends up being sent to private third parties and held far away on remote network servers.[3]

Electronic communications are much easier to obtain than papers kept in an individual's home. To obtain electronic communication information, the government can issue a warrant, subpoena, or court order for information stored with third parties.[4] Furthermore, if a company required a customer to sign a consent-to-disclosure contract before providing a service, the consumer may forfeit the right to privacy in the information conveyed to the third party. To limit abuses to third party information, both the courts and Congress have enacted protections. However, electronic information stored with third parties has much weaker privacy protections than other communications, and many

---

[3] Orin S. Kerr, "A User's Guide to the Stored Communications Act – And a Legislator's Guide to Amending It," *George Washington Law Review* 72, (2004): 3.
[4] Ibid., 13.

consumers are unaware of the rights affected by use of third parties for electronic communications.

The Supreme Court has demonstrated the third party doctrine in several cases. In *United States v. Miller* in 1976*,* the Court established that bank accounts could be searched as long as law enforcement obtained a subpoena.[5] After issuing subpoenas for Miller's bank information, the bank released his records to the police to examine for evidence of unpaid liquor taxes.[6] Miller challenged the search under his Fourth Amendment rights. Writing the majority opinion, Justice Potter Stewart explained that,

> [t]here is no legitimate "expectation of privacy" in the contents of the original checks and deposit slips, since the checks are not confidential communications, but negotiable instruments to be used in commercial transactions, and all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.[7]

Although we may wish the utmost privacy in financial matters, keeping records with banks and financial institutions forfeits the right to keep monetary information wholly private. Once an individual communicates financial or other information to a third party, one can no longer expect complete privacy regarding that information. A few years after the *Miller* decision, the Court issued a similar decision in *United States v. Payner*, in which Justice Stewart reinforced the third party doctrine.[8] In *Payner,* police agents stole a briefcase containing incriminating bank account information during an investigation. The

---

[5] United States v. Miller, 307 U.S. 174 (1939), in Cornell University Law School Legal Information Institute, http://www.law.cornell.edu/supremecourt/text/307/174, accessed March 17, 2014.
[6] Ibid.
[7] Ibid.
[8] United States v. Payner, 447 U.S. 727 (1980), in The Oyez Project at IIT Chicago-Kent College of Law, http://www.oyez.org/cases/1970-1979/1979/1979_78_1729, accessed March 17, 2014.

Supreme Court held that the case was indistinguishable from *Miller,* ruling in favor of the third party doctrine to judge the right to privacy in the banking information. In *Miller, Payner,* and several other cases, the Supreme Court firmly established the third party doctrine as it relates to tangible paper copies of information conveyed to third parties.

The third party doctrine also applies to verbal communications between individuals. The courts saw a wave of cases in the latter half of the twentieth century addressing information revealed to secret agents, and *Lee v. United States* demonstrates use of the third party doctrine in this context. After revealing incriminating details to an undercover agent, Lee argued that the use of a secret agent qualified as an unlawful search inside of his store.[9] The Supreme Court, however, reasoned that someone could not reasonably expect information conveyed to another individual to remain secret, even if Lee had trusted that the man would keep the information private. Once information is communicated to another party, the expectation of privacy diminishes because the information is voluntarily disclosed and one cannot predict how the recipient will use the information communicated. This doctrine was applied in a similar context in several cases throughout the twentieth century and helped to firmly establish the third party doctrine as it pertains to verbal communications between individuals.

The Third Party Doctrine and Electronic Communications

In the latter half of the twentieth century, the Supreme Court began to address third party doctrine cases involving new technologies. In 1979, the Supreme Court applied the third party doctrine to telephones in *Smith v. Maryland*. After identifying Smith as an accused robber, the police installed a pen register to monitor Smith's phone

[9] Ibid., 567-568.

calls. The Court reasoned that context phone call information, such as phone numbers, the duration of a call, and the time the call was placed do not fall under the Fourth Amendment. Justice Harry Blackmun delivered the majority opinion and explained the Court's reasoning:

> [I]t is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial, since they typically know that they must convey phone numbers to the telephone company and that the company has its facilities for recording this information and does in fact record it for various legitimate business purposes.[10]

By communicating through a third party telephone operator, the Supreme Court ruled that citizens should not expect that their call information is private. By voluntarily disclosing context information to telephone companies, one can assume that the information conveyed may be recorded for billing or other business purposes. Blackmun continued, stating that when Smith "conveyed numerical information to the phone company and . . . its equipment in the normal course of business, he assumed the risk that the company would reveal the information to the police."[11] Once someone discloses information to a communications company, she or he forfeits the right to keep the numbers dialed private. In an important distinction, *Smith* differentiates between context and content information as highlighted in *Katz* and *Ex parte Jackson*. The pen register monitored only the phone numbers Smith dialed, rather than Smith's phone conversations. The Court in *Smith* did not grant government the ability to obtain the conversations relayed during Smith's phone calls.

---

[10] Michael Lee Smith, Petitioner, V. State of Maryland, 442 U.S. 735 99 S.Ct. 2577, (1979), in Cornell University Law School Legal Information Institute, http://www.law.cornell.edu/supremecourt/text/442/735, accessed March 17, 2014.
[11] Ibid.

Throughout the twentieth century, the Supreme Court firmly established the third party doctrine in relation to third party communications of various kinds. If an individual reveals information to another person, business, or other entity, one can no longer assume that the information revealed will remain private. With the development and frequency of communications on cell phones, tablets, and computers, the third party doctrine assumes that any communication through an outside entity, such as Verizon or Comcast, is readily discoverable. With the prevalence of communications through third parties and very few alternatives, should the courts continue to apply the third party doctrine as they have in the past or should the doctrine be tailored to reconcile with technological developments and their predominance in society?

A Necessary Distinction: An Argument for the Third Party Doctrine

The third party doctrine is controversial. It seeks to balance information privacy and the ability for law enforcement to obtain evidence against alleged criminals. Should our right to privacy accommodate the ability of government to obtain data to prevent crime or identify criminals? Is it reasonable to expect that some of our information, such as the content of our phone calls and text messages, will remain private unless essential to thwart an impending national security threat? Various scholars have debated the merits of the third party doctrine and how to apply the doctrine in light of the digital revolution.

Those in support of the third party doctrine contend that it provides a general standard under which the government can judge the ability to retrieve personal data and information conveyed to a third party.[12] When we convey information to another party, it

[12] Orin S. Kerr, "The Case for the Third Party Doctrine," *Michigan Law Review* 107, (2008): 569-570.

may not be reasonable to assume that some of the information, such as the context information, will not be used for other purposes. Even in verbal communications, we cannot presume that the other individual will keep the information communicated private. We often give up information in order to obtain a service, and third parties must store that information for purposes such as billing. In a sense, as privacy law scholar Orin Kerr suggests, we consent to the use of our information when we voluntarily disclose it to a third party to use that information.[13]

Some scholars argue that the third party doctrine "ensures technological neutrality in the Fourth Amendment rules" and thus eliminates the ability of criminals to keep otherwise public aspects of crime private.[14] Without the third party doctrine, criminals could use technology to hide what would otherwise be a public aspect of a crime.[15] The third party doctrine ensures that criminals cannot hide their information from government search and seizure by invoking Fourth Amendment rights long after the information has been communicated to others.[16] For example, whereas someone would previously have had to purchase an illegal item in person, many transactions can be completed over the internet or other electronic communications, thus guarding the information from law enforcement under Fourth Amendment protections. The third-party doctrine guarantees

---

[13] Kerr, "The Case for the Third Party Doctrine," 572.
[14] Ibid, 573; Ric Simmons, "Why 2007 is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence," *Journal of Criminal Law and Criminology* 97 (2007): 15-16, accessed April 14, 2014, http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7262&context=jclc.
[15] Ibid.
[16] Kerr, "The Case for the Third Party Doctrine," 575.

that communications that were previously discoverable are still discoverable with the development of new technologies.

Kerr also points out a valuable characteristic of the third party doctrine: it provides "ex ante clarity."[17] Kerr's conception of the third party doctrine eliminates Fourth Amendment rights when the third party receives the information communicated; he states, "the present location of information defines the Fourth Amendment rules for collecting it, and the Fourth Amendment rules are constant within each location."[18] This principle maintains Fourth Amendment protections at the origin of the communication, such as an individual's personal computer or information in transit to the third party. Once the information reaches the third party, the third party doctrine is applied and the Fourth Amendment no longer protects that information. Providing this distinction helps to discern when Fourth Amendment protections are triggered. Otherwise, it may be difficult to determine in which situations an individual believed they had an expectation to information privacy.

Although it may be harder to rationalize in some cases, the third party doctrine allows for more consistent application of the Fourth Amendment and draws a line to determine privacy protections in an area that may otherwise be ambiguous and difficult to discern in application. Kerr aptly demonstrates the doctrine's bright-line rule, stating,

> [u]nder the third-party doctrine, if *A* tells a secret to *B*, *A* has no rights in *B*'s possession of the information. If the third-party doctrine is rejected, however, *A*'s rights in that information should continue even though *B* has the information now in addition to *A*.[19]

---

[17] Ibid., 582.
[18] Ibid., 581.
[19] Ibid., 583.

In the absence of a third party doctrine, where do we draw the line regarding privacy rights of information? Is there ever a point in which information is not protected by a reasonable expectation of privacy if the third party doctrine is eliminated? The third party doctrine may provide necessary clarity and neutrality in the application of the Fourth Amendment and privacy rights.

Critique of the Third Party Doctrine

Although Kerr and other scholars contend that the third party doctrine is necessary to discern privacy protections, many also illuminate the doctrine's weakness in preserving privacy in communications, especially when considered in light of the frequency of use of third parties for communication. The third party doctrine provides an easier-to-apply bright-line rule, however, it assumes that we give up the right to information and data privacy as soon as another party receives information. Many believe that the right to information privacy should be further extended, particularly as most of our communications today take place through third parties.

Dissenting in *Smith v. Maryland,* Justice Marshall expressed the majority's failure to uphold the expectation of reasonable information privacy. Justice Marshall illuminated the weakness of the doctrine's privacy protections, stating "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[20] Justice Marshall recognized that there are few substitute methods of communication that Smith could have used to keep his information private, and it is unreasonable to expect Smith not to use telephone communications if he wished to keep his telephone communication information private. Marshall believed that the Supreme

[20] Michael Lee Smith, Petitioner, V. State of Maryland.

Court's decision would be "disturbing" even to those who did not have anything to hide in their information and communications. He explained that many individuals, such as journalists and "unpopular political organizations" may wish to keep their communications and contacts private, and that "[p]ermitting government access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society."[21] Marshall's dissent demonstrates one of the major criticisms of the third party doctrine. A "realistic alternative" is not always available for communications, particularly with the prevalence of online and phone communications in the modern world. Communications via third parties are extremely common, and under the third party doctrine, many people sacrifice the right to privacy in everyday communication and information sharing. Marshall highlights the potential dangers to democratic freedoms that can arise when information privacy is not strictly maintained.

Another criticism of the third party doctrine is that it grants the government easier access to communications.[22] Justice Harlan articulated this critique in *United States v. White*. In *White,* the petitioner argued that placement of an informant to collect incriminating information violated Fourth Amendment rights. Justice Harlan challenged the Court's use of the third party doctrine, stating that it granted the government too much power to monitor conversations. Like Marshall, Harlan reasoned that the doctrine

---

[21] Ibid.
[22] United States v. White, 401 U.S. 745, 91 S. Ct. 1122, (1971), in The Oyez Project at IIT Chicago-Kent College of Law, http://www.oyez.org/cases/1960-1969/1969/1969_13, accessed April 10, 2014.

could threaten public discourse, thus endangering democratic principles by forcing citizens to be wary of what they communicate to others.[23] Based on current third party doctrine application, the government can obtain information such as emails and text messages without probable cause and a warrant, which may endanger freedom of expression. Court orders and subpoenas are much easier to obtain, thus allowing easier access to otherwise private communications. Some argue that the third party doctrine should be reformed to fairly consider the prevalence of third parties in new methods of communication. [24]

Highlighting another critique of the doctrine, law professor Erin Murphy argues that many aspects of crimes are not committed in public as Kerr argues. Murphy argues that "[w]e do not obliterate privacy protections for the home, for instance, just because the vast majority of child sexual abuse occurs there."[25] Not all crimes are committed in public, and it may be improper to assume that there is a public aspect to every crime that could be hidden with new technologies. Without the third party doctrine, technological development could allow criminals to hide their transactions on the internet and or other means protected by the Fourth Amendment, whereas these actions used to be conducted in public.[26] Murphy, however, argues that most criminals will not take the time to ensure their criminal acts are hidden in technological and constitutional protections and that the third party doctrine is superfluous in this respect.[27]

---

[23] Ibid.
[24] Kerr, "The Case for the Third Party Doctrine," 572.
[25] Erin Murphy, "The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr," *Berkeley Technology Law Journal* 24, (2009):1244.
[26] Kerr, "The Case for the Third Party Doctrine," 572.
[27] Murphy, 1242.

In addition, opponents of the doctrine believe that the Supreme Court has thus far improperly judged that private matters disclosed to one other party equates to disclosure to all. Privacy scholar Daniel Solove, an opponent to the third party doctrine, argues that the doctrine understands privacy as complete secrecy or as complete disclosure, rather than as varying degrees of privacy.[28] Solove believes that even if an individual conveys information to a third party company for a service and loses privacy rights in regard to that company, the individual should still have control over disclosure of that information to other parties. Large amounts of data and personal information are conveyed in everyday use of technology, and individuals should have the ability to control the privacy of their information.

The third party doctrine is controversial, and various scholars and judges have evaluated the merits of the doctrine. The next section details the proportionality principle; an alternative to the third party doctrine that several scholars believe better preserves individual privacy in communications information. Just like the third party doctrine, however, the proportionality principle is not without fault, and some scholars, such as Kerr, argue that the doctrine is too ambiguous in application, whereas the third party doctrine provides more clarity.

An Idealistic Alternative: The Proportionality Principle

Privacy scholar Christopher Slobogin contends that we cannot rely on the third party doctrine to properly protect our privacy. Instead, to preserve an individual's reasonable expectation to privacy, cases should be evaluated under the "proportionality

[28] Ibid.

principle."[29] This doctrine argues that law enforcement must "[calibrate] the justification for an action by reference to its impact on the affected party."[30] This allows for consideration of whether the search inhibits an individual's fundamental right when determining the constitutionality of a search.[31] The proportionality principle is demonstrated in *Terry v. Ohio,* in which the Supreme Court said, "[t]here can be 'no ready test for determining the reasonableness [of a search] other than by balancing the need to search against the invasion which the search entails."[32] The proportionality principle allows consideration of a broader set of factors to determine Fourth Amendment protection, rather than the third party doctrine's bright-line rule. It allows judges and law enforcement to consider the individual's reasonable expectation to privacy in the information. Slobogin, however, explains that the courts have not consistently applied the proportionality principle in search and seizure jurisprudence.

Despite inconsistent application, the proportionality principle could offer an alternative to the third party doctrine to better preserve personal privacy. Applying the proportionality principle, government officers would have to determine the invasiveness of the search in relation to an individual's right to privacy. Less-invasive searches would require a lesser degree of cause for search, such as relevancy to an ongoing investigation, while more invasive searches would require a higher standard, such as probable cause. It would allow discretion in deciding the reasonableness of a search and whether it invades

---

[29] Christopher Slobogin, "Is the Fourth Amendment Relevancy in a Technological Age?" in *Constitution 3.0: Freedom and Technological Change,* ed. Jeffrey Rosen and Benjamin Wittes (Washington D.C.: 2011), 24.
[30] Ibid.
[31] Ibid.
[32] Ibid.

the fundamental right to privacy; however, this discretion could either help maintain the right to privacy, or it could lead to bias or to inconsistent rulings in similar cases, which is contrary to the ideals of the American justice system.

With the vast amount of transactions, data, and information that passes through the web and via smart phones, this doctrine may be difficult to apply. It necessitates that law enforcement discern which searches are invasive enough to trigger an invasion of privacy and would require the courts to evaluate each case and identify whether or not Fourth Amendment rights apply. Although strict application guidelines and the appeals process can help to protect against wrongful searches under the proportionality principle, the third party doctrine's bright-line rule provides clarity and efficiency that judicial and police discretion cannot. Furthermore, it is hard to discern if an individual's right to privacy has been violated and whether an individual expected privacy in his or her communication information. Kerr explains that electronic communication "history is often complex and impossible to reconstruct. Just as a glass of water from a kitchen sink tap might have been rainwater in the Amazon thousands of years ago, information today often has a long past of interpersonal transmission."[33] It is difficult to determine the expectation of privacy an individual held regarding information passed through channels of communication. A new definition would need to be developed to help define the limits of the expectation to privacy under the proportionality principle.

The proportionality principle may offer an alternative route of privacy protection, however, the third party doctrine provides more clarity in application. Although the third party doctrine is not without faults, it provides an effective rule to determine information

[33] Kerr, "The Case for the Third Party Doctrine," 583.

privacy. Aside from court-constructed doctrines to determine our right to third party communications privacy, Congress has also addressed the issue and created legislation to help define the expectation to privacy in the digital age.

Legislative Protections

The Stored Communications Act

In the 1980s, Congress's Office of Technology Assessment assessed legal protections to emerging technologies and the privacy rights of individuals. Finding inadequate privacy protections for electronic communications, Congress began brainstorming legislation to outline the right to privacy in electronic communications.[34] Congress previously enacted the Wiretap Act of 1968 to prevent unlawful wiretaps, however, emerging technologies began changing the way Americans communicated and introduced a new set of technologies to consider.

Recognizing the need for stronger privacy protection in electronic communications, Congress developed the Electronic Communications Privacy Act (ECPA). After their initial investigation into privacy protections, the House and Senate Committees concluded that "[a]lthough the principle of the [F]ourth [A]mendment is timeless, its application has not kept abreast of current technologies."[35] Congress further concluded that "given the high threat to civil liberties posed by interception of electronic mail … the governmental interest in interception [is] quite compelling."[36] Emerging technologies required new legislative protections to ensure the right to privacy. In an

---

[34] U.S. Congress, House, Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary, Hearing on H.R. 3378, *Electronic Communications Privacy Act*, 99th Cong., 11th sess., 1986.
[35] Ibid.
[36] Ibid.

initial report, Congress discussed that e-mail messages stored on the author's computer or e-mail account would likely fall under Fourth Amendment protections, however, messages "in-transit" or stored on a remote server were not protected by the Fourth Amendment or by legislation.[37] Congress ruled that messages in-transit and in third party storage needed statutory protections.

The first section of the ECPA amends the Wiretap Act of 1968 to include electronic communications, rather than just wire communications. The Wiretap Act governs the ability to intercept communications in transit to another party and defines intercepting as use of any device to seize communication content while being transmitted electronically.[38] Information protected by the Wiretap Act, however, can be accessed with a court order specifying the particular time, place, and type of communication, as well as clear evidence that criminal activity is being relayed in the communication.[39] The Wiretap Act provides important limits on the ability of the government to obtain information in-transit. However, the Act only requires a court order to gain access rights to interception of a communication. Prior jurisprudence has held that content information requires a warrant to obtain, as demonstrated by *Katz v. United States.* Although the Act helps to protect against wrongful interception of communications, it should offer stronger legal standards to protect information privacy.

The second section of the ECPA created the Stored Communications Act (SCA) to protect material in electronic storage, such as third party records of an email account.

---

[37] *Electronic Communications Privacy Act*, 18 U.S.C. (1986), § 2510-2522.
[38] Daniel J. Solove and Paul M. Schwartz, "Privacy, Information, and Technology, (New York: Aspen Publishers 2009): 142.
[39] Ibid.

The SCA helped to define the limits of unlawful access to third party electronic communication information. Kerr explains the basic protections of the SCA, stating that it:

> creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information. It does this in two ways. First, the statute creates limits on the government's ability to compel providers to disclose information in their possession about their customers and subscribers. … Second, the statute places limits on the ability of ISPs to voluntarily disclose information about their customers and subscribers to the government.[40]

The statute protects both content and context information of users of third party communications services, and it acknowledges both third party use of data and government requests for data. The Act states that third parties must provide the name, address, phone connection records, services utilized, phone number or network address, and how the individual paid for the service if a warrant, subpoena, or court order is issued for the information.[41] The SCA prohibits ISPs and phone companies from sharing content information without a warrant in most cases.[42] However, the SCA makes several other distinctions that allow law enforcement to obtain content information without a warrant.

Although the Act protects content data in most situations, the SCA's distinction between Electronic Communication Services (ECS), which are services that offer users the ability to communicate via wire or electronic signal, and Remote Computing Services (RCS), which are defined as "any temporary, intermediate storage of a wire or electronic

---

[40]Kerr, "A User's Guide to the Stored Communications Act," 11.
[41] *Electronic Communications Privacy Act,* § 2703(c)(1).
[42] Ibid., § 2703(a).

communication incidental to the electronic transmission thereof" allow the government to obtain content data without a warrant.[43] An ECS communication, for example, is an unopened email in a recipient's personal e-mail account. However, if an email is viewed and not deleted by the recipient, it becomes an RCS communication stored on the ISP's server. Furthermore, the SCA only covers public ISPs, such as Gmail or Yahoo! Accounts. The SCA does not govern private ISPs, such as government or university servers, which are instead evaluated under the Fourth Amendment.[44]

The Act prohibits both RCS and ECS services from automatically disclosing data to government sources, however, the SCA's distinction between RCS and ECS allows government access to content information without a warrant. The Act states that with a warrant, government authorities can access information stored in an ECS within 180 days of its receipt. However, if ECS data is more than 180 days old or stored within a RCS, it can be obtained with a warrant, subpoena, or court order. Subpoenas and court orders only require that law enforcement show that the material is relevant to an ongoing investigation.[45] In addition, law enforcement has 90 days to inform the individual being searched, rather than requiring immediate notice of a search.[46] This standard for protection is much less robust than the protection guaranteed to content information by the Fourth Amendment and the precedent set in *Katz*.[47] Whereas warrants require probable cause, court orders rely on an easier burden of proof, allowing government officials to more easily access RCS data and ECS data more than 180 days old.

---

[43] Ibid., § 2711(2).
[44] Kerr, "A User's Guide to the Stored Communications Act," 11.
[45] *Electronic Communications Privacy Act*, § 2703 (c)(10)(D).
[46] Ibid.
[47] Ibid.

When the ECPA was established, email servers did not automatically store individual communications; a user would have to manually place the email into a saved folder to keep emails past 180 days. Today, however, many store their communications for long periods of time, and email providers allow storage of large quantities email data. In addition, many phone companies store text message data, and third-party data storage services, such as Dropbox, provide users with storage space for data and documents. The SCA's RCS and ECS qualifications have become obsolete in light of technological development, and new legislation to address electronic information privacy protections should be considered to augment the SCA's current protections.

In special cases, other means can replace the SCA's requirements for a warrant, court order, or subpoena. As demonstrated by the 2013 NSA surveillance controversy, government officials can request a "national security letter" to request communications in the interest of immediate national security needs.[48] National security letter requests do not require regular judicial approval, but the information obtained must be demonstrated as "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities" to a special judge.[49] As discussed later in this paper, national security letters greatly expanded the government's ability to obtain communications information, and many have debated the legality and constitutionality of national security letters and the NSA's data collection program.

---

[48] American Civil Liberties Union, et al. v. James R. Clapper, et al., 13 Civ. 3994 (U.S. Dist. Court Southern Dist. Of New York, 2013), in ACLU, https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf, accessed March 12, 2014.

[49] *Electronic Communications Privacy Act*, § 2709(b)(1).

The Courts and The SCA

The SCA, like the third-party doctrine, is controversial. Many believe that the Act does not provide adequate protection to content information or properly address new technologies, while others believe its framework provides the necessary basis to determine the ability of law enforcement to obtain electronic communications information. Despite the SCA's distinction between RCS and ECS communications, many courts now apply that a message retains its ECS protections until "the underlying message has expired in the normal course," regardless of whether the message has been opened by the recipient.[50] This application may better serve our current use of stored communications, however, it should be consistently applied in order to fully protect the privacy of communications information.

In *Warshak v. United States,* a case argued in the U.S. Appeals Court for the Sixth Circuit in 2010, a court order was issued to obtain Warshak's emails over 180 days old.[51] Warshak argued that the government's access to his emails violated the Fourth Amendment, while the government claimed that the SCA authorized access to Warshak's email content. The court ruled that the content of emails should require a warrant to obtain and that there is a reasonable expectation to privacy in email content.[52] The court argued that the SCA's warrantless access to content information was unconstitutional and that Warshak's Fourth Amendment rights were violated by the search, however, the court allowed the provisions of the SCA to prevail and did not exclude the emails from

---

[50] Quoted in Kerr, "A User's Guide to the Stored Communications Act," 11.
[51] United States of America v. Steven Warshak et al., 631 F.3d 266, 6th Cir. (2010), in USCourts.gov, http://www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf, accessed March 20, 2014.
[52] Ibid.

Warshak's trial. In the court's reasoning, the SCA allowed the government to effectively circumvent Warshak's Fourth Amendment rights to obtain content material.

The SCA was again addressed in *City of Ontario v. Quon.* City police department employee Jeff Quon used a city-issued pager to send sexually explicit text messages to a colleague. The police department had a general technology policy that stated that employees "should have no expectation of privacy or confidentiality when using [city-issued] resources."[53] Quon and other department employees claimed that the department's search of the pager message content violated both the Fourth Amendment and the SCA, because the information was acquired without a court order, subpoena, or warrant.[54] Judging the case in 2008, the Ninth Circuit Court drew upon *Katz* to rule that a reasonable expectation of privacy exists in the content of text messages and that the police department's search of the pager content violated Quon's Fourth Amendment rights.[55] The decision was petitioned to the Supreme Court, and in a 9-0 decision in 2010, the Court held that the text message search was constitutional.[56] Writing the majority opinion, Justice Kennedy stated that the "[p]etitioners' warrantless review of Quon's pager transcript was reasonable … because it was motivated by a legitimate work-related purpose, and because it was not excessive in scope."[57] The Court did not fully address

---

[53] City of Ontario, California, et al., v. Quon et al., Sup. Ct. No. 08-1332 (2009), in SupremeCourt.gov, http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf, accessed March 17, 2014.
[54] Ibid.
[55] Quon v. Arch Wireless Operating Company, Inc. et al., 9th Cir. 406 F.3d 1110 (2008), in USCourts.gov, http://cdn.ca9.uscourts.gov/datastore/opinions/2009/02/06/0755282o.pdf, accessed March 17, 2014.
[56] Ibid.
[57] Ibid.

Fourth Amendment content issues or the SCA and instead relied on the reasonableness of the search to justify the search's constitutionality. The Court relied on precedent set in *Treasury Employees v. Von Raab,* which established that "where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation "for noninvestigatory, work-related purpose, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances.""[58] The Court in *Quon,* although petitioned on violations of the Fourth Amendment and the SCA, decided the case based on *Von Raab*, which helped to define information privacy rights in the workplace.

For better or for worse, new technologies and methods of communication are discoverable by the government without a warrant in certain situations. Although the SCA and the Supreme Court's third party doctrine seek to clarify the situations in which we can expect information privacy, application of each is complex and many courts and scholars have argued against both. As cell phones and internet communications have become our main means of communication, how should the issue of privacy and government access to communications be resolved in the future? Should we rely on the Supreme Court to outline our privacy rights, or should Congress enact legislation to enhance our communications privacy rights? Furthermore, how should traditional context and content jurisprudence apply to the issue of national security and the NSA's data?

[58] Ibid.

CHAPTER 3: AN EVALUATION OF THE NATIONAL SECURITY AGENCY'S COLLECTION OF THIRD PARTY RECORDS

The NSA's surveillance program provides a pertinent example to examine in light of the third party doctrine and the SCA. In 2013, former NSA contractor Edward Snowden leaked information and secret documents of the NSA's warrantless surveillance program, and in response, many Americans became greatly concerned with communications privacy. Several citizens filed court cases against the government's data collection. Snowden's leaks were first published in the British news source *The Guardian*, in which he revealed that on "an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications" are monitored by the NSA.[1] After the first leaks were exposed, more details about the NSA's surveillance of phone and internet communications were released, and many questions were raised regarding the legality and constitutionality of the NSA's program. The government has argued that the NSA surveillance program serves a compelling government interest to identify possible national security threats, however, the Snowden leaks have left many Americans wondering whether the government is obstructing their right to privacy.

Following 9/11, President George W. Bush signed the Patriot Act to enhance the government's ability to obtain phone and internet records. The Patriot Act allows the FBI and other government officials to obtain records without a warrant, court order, or subpoena in the interest of national security, granted a national security letter is issued to authorize access to the information. To protect the legality of the government's actions,

---

[1] "The NSA Files," *The Guardian,* accessed April 16, 2014, http://www.theguardian.com/world/the-nsa-files.

the Patriot Act amended the SCA's applicability to government, only maintaining that citizens can "sue the United States for money for claims arising out of the Wiretap Act, the Stored Communications Act, and the Foreign Intelligence Surveillance Act."[2] By amending the SCA's provisions as they apply to the government, traditional SCA protections governing content and context data are replaced by national security letters, which can be easier to obtain than a warrant, court order, or subpoena.

In order to further enhance surveillance, Congress passed the FISA Amendments Act in 2008, which allows the NSA to monitor foreign targets without obtaining a warrant.[3] By obtaining foreign communication information without a warrant, law enforcement can more quickly analyze data to identify possible terror threats. The current NSA program allows the government to access a wide range of communications without a warrant and without the limitations of the SCA. The program collects telephone information, email, text messages, web communications, and internet activity both in the U.S. and between the U.S. and foreign sources.[4] PRISM, the NSA's major data collection program allows government to monitor communications by collecting information from third party communication companies, such as Apple, Google, Facebook, Microsoft, Yahoo, Skype, YouTube, PalTalk, and AOL, as well as telephone companies, such as

---

[2] American Civil Liberties Union, et al. v. James R. Clapper, et al., 13 Civ. 3994 (U.S. Dist. Court Southern Dist. Of New York, 2013), in ACLU, https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf, accessed March 12, 2014.

[3] FISA Amendments Reauthorization Act of 2012 (FISA Amendments Act), H.R. 5949, 112th Congress (2008), In www.GovTrack.us, from http://www.govtrack.us/congress/bills/112/hr5949, accessed April 3, 2014.

[4] Carolyn Jewel et al. v. National Security Agency et al., no. 10-15616, 9th Cir. (2011), in USCourts.gov, http://cdn.ca9.uscourts.gov/datastore/opinions/2011/12/29/10-15616.pdf, accessed April 5, 2014.

AT&T, Verizon, and Sprint.[5] The NSA collects both content and context information and can retain information for an extended period of time.

Contrasting reports have been presented by government officials and by leaked documents about the type and extent of content information collected by PRISM. Content information, aside from wiretapped phone calls, is collected via third party communications companies.[6] Most content data is removed from NSA storage within three days. However, if the data matches an identified foreign "target," it is stored and evaluated.[7] John Inglis, the former Deputy Director of the NSA, confirmed that the NSA does "not target the content of U.S. person's communications without a specific warrant anywhere on the Earth."[8] However, leaked documents posted by *The Guardian* have suggested that the U.S. monitors much more content information than initially believed. Documents revealed that the Foreign Intelligence Surveillance Court (FISC), which is assumed to abide by the Constitution, authorized the collection of content information from communications between individuals in the U.S. and non-citizens without a warrant.[9] Information collected includes "IP addresses, statements made by the potential target, and other information in NSA databases, which can include public information

---

[5] "The NSA Files."
[6] Scott Cawley, et al., "The NSA and surveillance … made simple," *The Guardian,* November 26, 2013, http://www.theguardian.com/world/video/2013/nov/26/nsa-gchq-surveillance-made-simple-video-animation.
[7] Ibid.
[8] "Inglis on domestic spying," *C-SPAN,* last modified August 6, 2013, accessed April 17, 2014, http://www.c-span.org/video/?c4461523/inglis-domestic-spying.
[9] Ibid.

and data collected by other agencies."[10] Because the content data is collected from both U.S. citizens and foreigners, the content data obtained from citizens may violate the Fourth Amendment. Surveillance is halted if the foreign target is later identified as within the U.S., however, data is still initially collected from at least one subject within the U.S., which could be ruled in violation of the Fourth Amendment.[11] However, insufficient evidence proves that the U.S. collects content information from citizens, thus the FISC's authorization of the surveillance program should be trusted.

The extent of the context data collected by the NSA is much more clear. There are few legal restrictions to limit collection of third party context information, particularly after the enactment of the Patriot Act and the FISA Amendments Act. Context information is stored for a longer period of up to five years in order to identify relationships and communication patterns.[12] If a target is identified and approval is received of an identified "reasonable, articulable suspicion" from a designated official, the target's number is queried in the PRISM database to collect all information associated with the number.[13] This allows the NSA to track communications over a period of time and to identify patterns that may provide information regarding terror threats.[14] Although the authorization requirement helps to ensure that data is not collected and analyzed

---

[10] Glenn Greenwald and James Ball, "The top secret rules that allow NSA to use US data without a warrant," *The Guardian,* last modified June 20, 2013, accessed April 17, 2014, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.
[11] Ibid.
[12] Cawley.
[13] Klayman et al. v. Obama et al., No. 13-0851, U.S. Dist. Court, Dist. of Columbia November (2013), in Google Scholar, http://scholar.google.com/scholar_case?case=5338740867216353 93&hl=en&as_sdt=6&as_vis=1&oi=scholarr, accessed April 17, 2014.
[14] Cawley.

without authorization, there have been several instances in which data has been examined without authorization and the FISC has sanctioned the NSA.[15] In one of the most recent compliance issues, an FISC judge found that "the Government had misrepresented the scope of its targeting of certain internet communications."[16] Much of the information about the NSA's data collection program remains classified and it is difficult to judge the severity of the NSA's compliance issues, however, many Americans believe the NSA's surveillance invades the right to privacy, and many have questioned the legality and constitutionality of the program.

Court Rulings on the NSA's Program

Several court cases have been filed against the NSA's surveillance program. Prior to the Snowden leaks, the ACLU filed a case in response to the FISA Amendments Act because of its expansion of the NSA's ability to obtain information. In *ACLU v. Clapper*, Judge Pauley for the Southern District of New York held that if the precedent in *Smith v. Maryland* stands, then the NSA's program should be ruled constitutional. In *Smith*, as previously mentioned, law enforcement installed a pen-register to collect context information about Smith's calls. Because the information was voluntarily conveyed to the phone company, the Supreme Court ruled that the NSA's metadata collection was constitutional. In *Clapper,* the petitioners alleged that NSA's bulk data collection without probable cause was in violation of the Fourth Amendment, the First Amendment, and several statutory provisions. The ACLU argued that the context information collected could "reveal a person's religion, political associations, use of a telephone-sex hotline,

[15] Ibid., 22.
[16] Ibid.

contemplation of suicide, addiction to gambling or drugs, experience with rape, grappling with sexuality, or support for particular political causes."[17] The NSA's program could endanger essential democratic values. However, the plaintiffs did not have any direct evidence of surveillance and the court ruled that the ACLU did not have proper standing.[18] Nonetheless, the case raised important considerations about the NSA's data collection and the perceptions of data collection by American citizens.

Although he did not issue a ruling in the case, Judge Pauley discussed the legality and constitutionality of the NSA's surveillance.[19] Pauley found that because the NSA collects data from telephone and electronic communications companies, rather than retrieving communications from personal computers, the information received triggers the third party doctrine. As established by *Smith* and several other third party doctrine cases, the government can obtain information from third parties using various legal means. Siding with the NSA's use of the system, Judge Pauley highlights that the NSA only receives context information and can only access that information if it meets a designated target. The information does not immediately identify any particular individual, and only a small fraction of the data collected is analyzed.[20] Judge Pauley contends that the NSA's program should be ruled in concurrence with third party doctrine cases, because the context information is obtained from third parties with a national security letter, which functions as a court order for the information.[21] However, *ACLU v.*

---

[17] American Civil Liberties Union, et al. v. James R. Clapper, et al.
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.

Clapper was decided before the Snowden leaks, and more specific details about the program may have affected Pauley's opinion.

Other judges have interpreted the NSA's surveillance program in a different Fourth Amendment light. In *Klayman v. Obama,*[22] Klayman, like the ACLU, filed a case against the NSA for violating the Fourth Amendment. The court decided to address the NSA's metadata collection, rather than collection of content information, because reports have not confirmed that the NSA is collecting bulk content information from citizens.[23] Unlike *ACLU v. Clapper, Klayman* was filed after Snowden's leaks, thus allowing the petitioner to substantively claim the NSA's metadata collection. A final ruling has not been issued in the case and Klayman has petitioned the Supreme Court to address the issue, however, Judge Leon issued his opinion of the constitutionality of the NSA's surveillance.

Unlike Judge Pauley, Judge Leon writes that metadata collection is different from the principles presented in *Smith,* thus *Smith* should not serve as precedent. Judge Leon emphasized that the *Smith* precedent limited the pen-register search to "short-term, forward-looking (as opposed to historical), and highly-limited data collection," whereas the NSA's surveillance is historical and broad.[24] Explaining his ruling, Leon states:

> When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become to thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* does not apply? The answer, unfortunately for the Government, is now. . . It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is

[22] Klayman v. Obama.
[23] Ibid.
[24] Ibid.

> quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government.[25]

The sweeping and historical nature of the NSA's program is greatly different than any case previously considered by the Court, and Leon called on the Supreme Court to consider the historical characteristics of the NSA's program.[26] Rather than focused, reasonable searches based on probable cause, the NSA's program seizes nearly every electronic communication in the United States. Leon argues that the search and seizure plainly violates the Fourth Amendment.

Is it Constitutional? The Third Party Doctrine and the SCA Applied

Although the NSA's surveillance has several distinguishing characteristics in comparison to other third party doctrine cases, the underlying principle of each case is similar. PRISM collects data from communications companies, such as AT&T and Google. It does not collect information directly from citizens' email boxes or telephones. By using communications companies to search and seize information, the government does not violate Fourth Amendment precedent. Once information is transmitted to a third party for a service, the expectation of privacy in that information is extinguished and government agencies or officials can legally request context data without a warrant under the Patriot Act. Although it is controversial whether it is reasonable for the government to seize bulk context information in the interest of efficiently identifying security threats, application of the third party doctrine to the NSA's surveillance program's metadata collection verifies its constitutionality. As consumers, we surrender complete privacy

---

[25] Ibid.
[26] Ibid.

rights to pieces of information upon communicating them to someone else, and internet and phone companies operate as third parties to our communications, thus the Fourth Amendment does not protect the information they receive.

In the normal course of Fourth Amendment jurisprudence, the sweeping and historical nature of the NSA's program may be problematic. However, national security needs and specific legislative acts, such as the Patriot Act, have changed the characteristics of context data acquisition. Traditional application of the third party doctrine requires that government officials obtain a court order to access data. However, the Patriot Act changed this component for the NSA's surveillance program. The Patriot Act authorized government to access data in the interest of national security with national security letters. These letters act as a court order to access communications information from third party companies, thus validating the constitutionality of the bulk data collection under the third party doctrine. Constitutional law scholars debate whether the third party doctrine and the precedent set in *Smith* should be applied to the NSA's surveillance program, however, the information is obtained from third parties with a specialized court order, thus the context data acquired under the NSA's program is constitutional. As cases against the NSA advance through the court system, however, courts will have to decide whether the third party doctrine should apply to the NSA's data collection. If ruled that it does not apply, the courts will need strong explanation to support why the NSA's third party context data collection is beyond the scope of the third party doctrine.

It is likely that the NSA's metadata collection is not in violation of the third party doctrine or the Fourth Amendment. However, the NSA's collection of content

information may pose Fourth Amendment problems. The third party doctrine has sometimes been limited to collecting context information, such as the data collected by the pen-register in *Smith.* If the Supreme Court precedents in *Smith* and *Katz* are applied to the NSA's collection of electronic communications, content data collection should be ruled unconstitutional. However, the third party doctrine has sometimes allowed collection of content data, as demonstrated by *Miller*, in which the content information of Miller's bank account was subpoenaed and ruled constitutional. As private communications, however, the NSA's content collection should follow the precedents in *Smith* and *Katz.* Although it is unclear how much content data is collected – the NSA has denied that it collects content data from citizens and news reports have alleged otherwise – any content information collected from citizens without a warrant should be ruled a violation of the Fourth Amendment. The FISA Amendments Act authorized the government to collect data from targeted non-citizens, however, content communicated within the U.S. should not be obtained.

Katz v. United States, a previously mentioned case that struck down warrantless wiretapping, and *Warshak v. United States,* a third party doctrine case, can be applied to establish protection of content information acquired by the NSA. Although the information obtained in *Katz* was not collected from a third party organization, *Katz* has been applied as a main tenant to restrict law enforcement from obtaining content information without a warrant and can be aptly applied to the NSA's data collection. In *Katz,* Justice Harlan ruled that individuals properly assume the right to privacy in personal conversations, such as phone calls and emails, and the Court ruled that it was

unlawful to monitor Katz's phone calls without a warrant.[27] Although provisions of the Patriot Act and FISA Amendments Act grant the government more leeway in accessing content, citizens still maintain a reasonable expectation of privacy in content information, and the Fourth Amendment should protect this information.

In *Warshak v. United States,* the Sixth U.S. Circuit Court of Appeals at Cincinnati applied the third party doctrine and the SCA to evaluate government access to electronic communications. The court determined that the Fourth Amendment should protect email content and that there is a reasonable expectation of privacy in content information.[28] Although the information may be retrieved from a third party, content information can reveal intimate details, and it is reasonably assumed that the information will remain private and will not be used by third parties. Although the judges in *Warshak* deferred to the "good faith" of the provisions of the SCA that validated warrantless government search of email, judges should apply the court's evaluation of content data collection in *Warshak* to determine the constitutionality of access to content information.[29]

Allowing the seizure of content information without a warrant or reasonable suspicion could endanger democratic principles and violate the fundamental "right to be let alone." If the government upheld the ability to monitor the content of communications, citizens may shy away from expressing beliefs and ideas over the internet, especially if those beliefs were controversial. As 86% of Americans have tried to

---

[27] Katz v. United States, 389 U.S. 347, 88 S. Ct. 507 (1967), in Cornell University Law School Legal Information Institute, http://www.law.cornell.edu/supremecourt/text/389/347, accessed February 18, 2014.
[28] United States of America v. Steven Warshak et al., 631 F.3d 266, 6th Cir. (2010), in USCourts.gov, http://www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf, accessed March 20, 2014.
[29] Ibid.

increase their anonymity online, the amount of information readily accessible to the government is a salient issue that could increasingly affect the use of electronic communications if the government were able to collect bulk content information.[30] The judges in both *Katz* and *Warshak* provide an evaluation of content data collection, and both cases should be followed to determine the constitutionality of NSA surveillance.

Although parts of the NSA's surveillance program are likely constitutional, the program plainly violates the SCA's original provisions. The Patriot Act amended the SCA as it applies to the government and authorized more extensive government surveillance, only guaranteeing monetary redress if a government actor violates the Act's terms. If the SCA did apply to the NSA's data collection, it would place limits on the ability of the government to obtain information from third party sources and would restrict the information that communications companies could voluntarily disclose. The Patriot Act and FISA Amendments Act's provisions are less stringent than those of the SCA and allow the government to more easily obtain communications information from citizens by using national security letters.

Other considerations complicate the surveillance program's constitutionality and legality, such as national security and the efficiency of identifying potential terror threats. Although the NSA's data program can be evaluated under the third party doctrine and the SCA, as an issue of national security, the controversy is not resolved with simple application of these principles. Parts of the NSA's program may violate traditional

---

[30] Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden, "Anonymity, Privacy, and Security Online," *Pew Research Internet Project,* September 5, 2013, accessed April 14, 2014, http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

conceptions of third party jurisprudence, however, special considerations beyond the scope of this work complicate the program's legality and constitutionality. However, many Americans have voiced concern over the NSA's sweeping searches and the danger to maintaining the right to privacy in the digital age, and this controversy may trigger the need for new standards of privacy and reform of our national security programs in order to balance privacy and security needs.

In January 2014, President Obama gave a speech about plans to reform the NSA's surveillance program and to remove the NSA's ability to collect bulk data without a warrant or court order.[31] Obama, however, acknowledged the difficulty in balancing privacy rights and security needs. In March 2014, Obama announced legislation to reform the NSA's data program. Obama's March proposal limits the NSA's ability to collect bulk telecommunication information, and if passed, information could only be obtained by issuance of a specialized court order more stringent than a national security letter.[32] Obama requested another 90-day renewal of the current surveillance program while the new program reforms are developed.[33] Congress has also addressed the issue and has begun to develop its own bill for NSA program reform. Regardless of the NSA surveillance program's constitutionality and legality, the public outcry in response to the Snowden leaks and the increased concern over the right to privacy in the digital

---

[31] President Barack Obama, "Remarks by the President on Review of Signals Intelligence," *The White House Office of the Press Secretary,* January 17, 2014, accessed April 12, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[32] Charlie Savage, "Obama to Call for End to N.S.A.'s Bulk Data Collection," *The New York Times,* March 24, 2014, accessed April 14, 2014, http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html.

[33] Ibid.

revolution should trigger reform to the surveillance program in order to enhance privacy rights and protect the democratic freedoms that the right to privacy helps to guarantee.

CHAPTER 4: ADDRESSING PRIVACY CONCERNS GOING FORWARD

In *Quon,* the court stated that email had become "so pervasive that some persons may consider [it] to be [an] essential means or necessary [instrument] for self-expression, even self-identification."[1] New forms of communication have become commonplace, and many of these methods of communication are not strongly protected by the Fourth Amendment. The third party doctrine and the SCA are helpful in outlining the right to privacy; however, current protections are not adequate to preserve privacy in the digital age. As demonstrated by the Pew Center's research discussed earlier in this work, many Americans believe that information privacy is valuable, and a large majority of Americans have tried to increase their anonymity online.[2] Despite personal efforts to increase privacy, much of our information transmitted through the internet and through phones can be acquired by the government, and often with relatively easy legal means. Most Americans are not satisfied with current privacy protections and believe that the government should enact new laws to more strongly guard our information.[3] It will be difficult to appease both extreme-privacy supporters and those who favor enhanced law enforcement, nevertheless, the current system warrants reform to more equally balance these two areas.

---

[1] Quon v. Arch Wireless Operating Company, Inc. et al., 9th Cir. 406 F.3d 1110 (2008), in USCourts.gov, http://cdn.ca9.uscourts.gov/datastore/opinions/2009/02/06/0755282o.pdf, accessed March 17, 2014.

[2] Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden, "Anonymity, Privacy, and Security Online," *PewResearch Internet Project,* September 5, 2013, accessed April 14, 2014, http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

[3] Ibid.

With the amount of information transmitted to third parties, it may be unreasonable to expect that our data will remain truly secret; however, we can expect more privacy than is currently guaranteed. Third parties must process much of the information we convey, such as phone numbers and email addresses. However, increased concern over privacy in the digital age demands that our laws and doctrines are amended to accommodate privacy concerns. The large proportion of Americans who have tried to increase their anonymity online illustrates the fear of the ease at which personal information is collected in the digital age. Weak privacy protections may pressure Americans to censor their communications and online activity. Fear of expressing oneself is contrary to fundamental American principles, and our laws should accommodate the right to privacy in order to preserve these principles. However, there is also value in the ability of law enforcement to efficiently and effectively collect information to identify crime. Allowing law enforcement to obtain communication information conveyed over phones and on the internet helps to efficiently collect evidence, and in the case of national security, to identify potential terror threats. Both the right to privacy and the needs of law enforcement are important issues, and the SCA and the third party doctrine are necessary to help strike a balance between these needs. Current conceptions of the third party doctrine and the SCA, however, do not provide enough information protection.

Both the SCA and the third party doctrine provide bright-line rules to determine the privacy of our communications. This helps to promote efficiency in law enforcement and clarity in applying the rules. However, both the SCA and the third party doctrine should be altered to provide further clarity in application, as well as to define the specific instances in which we can expect our information to retain Fourth Amendment

protections. Alternatives to the third party doctrine, such as the proportionality principle discussed in Chapter 2, would be difficult to apply and would rely heavily on discretion of law enforcement and judges. Amended versions of the third party doctrine and the SCA would provide a sound balance between law enforcement's ability to obtain information and to guarantee the right to privacy. To provide clarity and appropriate data privacy protections, the following clarifications and amendments should be made to the third party doctrine and the SCA: 1) third party doctrine should only apply to context data, 2) content data should be protected by the Fourth Amendment, 3) the SCA should eliminate the distinction between RCS and ECS communications, and 4) the SCA should require warrants for all content data acquisition.

The Third Party Doctrine's Application to Electronic Communications

The third party doctrine has been established in our court system to determine the ability of law enforcement to access information revealed to a third party. The doctrine's application to electronic communications is controversial; however, it provides a bright-line rule to promote efficient law enforcement, while also offering necessary protections to personal information. To provide further clarity and protection going forward, the third party doctrine should be tailored to fit privacy needs that have developed with the digital revolution. To do so, context information should be governed under the third party doctrine, and content information should retain Fourth Amendment protection. Although the third party doctrine has previously covered some content information, such as verbal conversations to an undercover agent, electronic content information should not fall under the third party doctrine. This principle will help to strike a healthier balance between the needs of law enforcement and individual privacy needs.

The third party doctrine is necessary to define the privacy of information conveyed to third parties. However, electronic communications present a more complicated privacy dilemma, and the third party doctrine should be amended in its application to new methods of communication. Most communications today involve third parties, which would traditionally call for application of the third party doctrine. However, there are no practical alternatives to electronic communications; courts cannot presume that if an individual wanted privacy in communications that she or he would use another means of communicating that information. Our modes of communication should not automatically forfeit the expectation to privacy in that information. In general, it is reasonable to expect privacy in content material. Privacy ensures the ability to freely express oneself without fear of government search and seizure, and the Framers attempted to guard against warrantless invasions of privacy when developing the Fourth Amendment. Context information, however, is voluntarily delivered to third parties for use of that information, and so it may be less reasonable to expect privacy in this information.

The third party doctrine should apply to context information, while content information should retain Fourth Amendment protections. *Ex parte Jackson* and *Warshak v. United States* provide prior court guidelines to help ensure content information protection. As discussed previously, *Ex parte Jackson* established the privacy of mailed letters. Similarly, although the constitutional arguments were not ultimately addressed, the court in *Warshak* declared that citizens hold a reasonable expectation to privacy in

email content.[4] Although content information may be incidentally communicated to a third party for a service, the individual usually presumes privacy in that information, just as someone would presume privacy in the contents of a mailed letter. *Katz* provides an example in which the Supreme Court declared that that simply because information, such as a telephone call, is accessible by a third party, Fourth Amendment rights or the reasonable expectation to privacy in that information is not automatically extinguished. Although our means of communication have changed, use of electronic communications does not forfeit our right to privacy. Only if, for example, an individual made a phone call in public or if an email was projected on a public screen should the third party doctrine apply. Otherwise, the Fourth Amendment should govern content information conveyed to third parties for a communication service. Including content information under the Fourth Amendment ensures that the government cannot obtain revealing content information with a court order or subpoena and instead must show probable cause in order to search and seize data.

Although content information should fall under the Fourth Amendment, context information should follow third party doctrine jurisprudence. Context information is voluntarily revealed to a third party to use that information. Similar to a mailing address on an envelope, context information is revealed to an electronic communications company or servers to facilitate a service. Although privacy policies and the SCA limit the ability of third parties to disseminate information to others, allowing the government to collect some information serves a legitimate and compelling government interest.

---

[4] United States of America v. Steven Warshak et al., 631 F.3d 266, 6th Cir. (2010), in USCourts.gov, http://www.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf, accessed March 20, 2014.

Context information can aid efficiency of the law enforcement system. Furthermore, the law requires a subpoena or court order before information can be accessed, thus helping to protect against arbitrary data collection and ensuring that information cannot be willingly forfeited to the government. As information communicated to a third party to use that information, context information should be governed by the third party doctrine.

Distinguishing between content and context information helps to provide clarity to the application of the Fourth Amendment to electronic communications, however, the line between content and context information is blurred in some cases. Whereas email messages and addresses are more simply separated into content and context data, the issue becomes convoluted when considering online activity. IP addresses, which are computer-identifying strings of code, have traditionally been considered context information and are accessible by court order or subpoena under the provisions of the Pen Register Act, which is the third section of the ECPA.[5] IP addresses are communicated across networks when websites are visited, and because they are recorded by individual websites, IP addresses can be just as revealing as content information protected by the Fourth Amendment. The government could conceivably collect each website an individual has visited, which could reveal a great amount of information about the targeted individual, such as her religion or political beliefs. Although this information can be just as revealing as content information, because the information is voluntarily relayed to a third party as a means of facilitating a service, the information should be ruled as context information and thus should not be protected under the Fourth Amendment. The

[5] Daniel J. Solove and Paul M. Schwartz, "Privacy, Information, and Technology, (New York: Aspen Publishers 2009): 185.

courts may face the difficulty of this issue in the next few years as the NSA's internet information collection program is challenged.

A Necessary Tool in Our Legal System

The third party doctrine serves a compelling government interest, because it allows law enforcement to efficiently gather evidence to a crime, whereas information protected by the Fourth Amendment may be more difficult to obtain. Because context information is relayed to third parties to use that information for a specific service, the third party doctrine should apply to this information. Content information, on the other hand, is reasonably expected as private information. The digital age has complicated the third party doctrine's application, however, fundamental principles of information privacy, as demonstrated in cases such as *Ex parte Jackson,* should be applied to new methods of communication in order to guarantee Fourth Amendment protection to content information.

The third party doctrine provides clarity to law enforcement and the courts in determining the privacy rights of information conveyed electronically. Because most of our communications are revealed to third parties today, the third party doctrine helps to distinguish which information falls under the Fourth Amendment, thus helping to clarify privacy rights and helping to facilitate law enforcement's ability to collect information from third parties. Although this understanding of the third party doctrine may not guarantee privacy to all of our information, and it does not allow law enforcement to easily access all data, the third party doctrine helps to define our privacy rights and facilitate effective and efficient law enforcement.

Amendments to the SCA

Similar to the third party doctrine, the SCA has several faults that should be amended to reconcile with the enormous amount of data transmitted through phones and the internet each day. The SCA provides appropriate groundwork to outline privacy protections in the digital age, however, the statute should be updated in order to provide clarity in application and to ensure privacy protections for content and context data. Many courts have had difficulty in applying the SCA consistently.[6] In some cases, judges have misconstrued the statute to apply to web browser cookies, which are not addressed in the SCA.[7] While many of the SCA's provisions are still surprisingly relevant after nearly thirty years, several aspects of the statute's language complicate its application to current technology. Updating the SCA's provisions to more applicably address the situations in which our information can be accessed without a warrant will give clarity to law enforcement and the courts, as well as to citizens to define when to expect information privacy and when information can be accessed by court order or subpoena.

As mentioned previously and as outlined by Justice Harlan's concurrence in *Katz* and by the Court in *Ex parte Jackson,* Americans usually have an expectation to privacy in content material. It is usually assumed that the content of emails, video calls on the internet, phone conversations, and text messages are private. The content of communication – in most cases – is not conveyed to the public or to a third party for use of that information, thus individuals retain a reasonable expectation to privacy in that

---

[6] Melissa Medina, "The Stored Communications Act: An Old Statute for Modern Times," *American University Law Review,* vol. 63, 2013, 10.
[7] Orin S. Kerr, "A User's Guide to the Stored Communications Act – And a Legislator's Guide to Amending It," *George Washington Law Review* 72, (2004): 8.

information. The SCA allows law enforcement to obtain content data from third party organizations if the message is unopened and 180 days old or opened and stored. Content data only retains its Fourth Amendment protections when it is less than 180 days old and unopened. This distinction is no longer relevant in current terms – it is common store to old emails on accounts for long periods of time and cloud storage services, such as Google Drive, offer long-term file storage. Under the current SCA, very few emails in our inboxes, for example, require a warrant for law enforcement to obtain. Instead, the court's logic in *Warshak* should be upheld and the SCA should not allow warrantless searches of content material.[8] Much like the distinction discussed in the prior section, Congress should amend the SCA to require warrants for content information, while keeping context information under the current rules of the SCA.

Aligning the distinctions of the third party doctrine with the SCA will help to provide clarity for courts and for law enforcement in applying the SCA. The complications of applying the SCA are demonstrated by *Warshak,* in which the court ruled that the "good faith" provisions of the SCA should prevail, but that the government violated Warshak's Fourth Amendment rights by accessing his email messages. Amending the SCA to distinguish between content and context information will remove the discrepancy between Fourth Amendment jurisprudence and the provisions of the SCA.

Aside from amending the SCA's application to content information, the Act's irrelevant distinction between RCS and ECS communications should be eliminated, thus implementing one standard for content and context communication. This bright-line rule

[8] United States of America v. Steven Warshak et al.

would ensure more streamlined application by law enforcement and clarity for courts evaluating SCA cases. As previously mentioned, Congress wrote the SCA in a time period before email accounts stored large amounts of messages and before large amounts of information were stored and communicated through third parties. It is much more common for individuals to keep emails long term, thus the SCA should not distinguish stored communications based on the amount of time the individual has possessed them and should not allot different levels of privacy for unopened or stored emails. Our right to privacy in content information should not hinge on the age of a message, and the expectation to privacy should be maintained with the development new technologies that facilitate long term storage of electronic communications.

Protecting content information helps to better protect intimate details. That is not to say that context information cannot reveal important details about an individual, such as the dilemma regarding IP addresses mentioned in the previous section, but by strictly limiting access to content and allowing easier legal means to obtain context information, a more harmonious balance between privacy rights and the needs of the government to ensure national security can be reached. If necessary, the government can still obtain content with a warrant or by providing cause to an impending threat to national security. In addition, these amendments to the SCA will help to govern the instances in which third parties themselves can disseminate information the government, thus further protecting against unlawful access to third party information. The SCA provides important guidelines, however, it should be amended to provide stronger protections to content information and to appropriately address updated use of third parties for content information storage.

The four recommendations outlined in this section will help to align our laws and institutions with the right to privacy. The current system sways toward government acquisition of personal communications data, and while it is important to facilitate efficient and effective law enforcement, privacy rights are necessary to maintain some of our most prized democratic ideals. Both traditional searches of communications data and the NSA's surveillance program are currently too far reaching; our laws and court jurisprudence require changes to protect our right to privacy.

CONCLUSION

The balance between privacy, technology, and the needs of law enforcement are complicated. As demonstrated by the NSA's surveillance program and the public outcry in response to the Snowden leaks, our personal privacy is an important issue that warrants discussion. The Framers wanted to protect against unwarranted searches and seizures into private areas, and the ease at which the government can access content information is a threat to the fundamental rights that the Framers sought to protect. Electronic communications content information can reveal a great deal of information about an individual, including controversial information such as religious beliefs, medical information, political preferences, and sexuality. Allowing warrantless government access to this kind of information endangers democratic freedoms and violates constitutional principles.

Our institutions and the minds of our citizens have not developed "hand in hand" while technology has revolutionized our world, as Thomas Jefferson argued that they should. The great controversy regarding individual privacy in the digital age suggests that our institutions and expectations are out of step and require reform in order to ensure a just society. It is unlikely that we will strike a true balance between information privacy and the ability for law enforcement to collect data. Even with updated laws and court doctrines, there will likely be a discrepancy between privacy and the government's ability to collect data. Nonetheless, the current system demands updated laws and doctrines to govern our information privacy in the twenty-first century. The Constitution does not guarantee a right to privacy, but statutory law and some of our most prominent

constitutional scholars have discussed the necessity of preserving privacy in reasonable situations.

The issue will not likely be resolved soon, however, as acknowledged recently by Obama and by many American citizens, the current NSA program may extend beyond the acceptable means of data collection. Matters of national security demand consideration of extenuating factors compelling to the safety of our nation, however, many citizens and organizations have filed suit against the NSA. Despite suggestions for the Supreme Court to take up the issue, many have expressed that the Supreme Court may not be a suitable institution to decide a matter involving national security. Addressing the NSA cases petitioned to the Supreme Court, Justice Antonin Scalia stated, "[w]e know nothing about the degree of the risk. The executive knows. The Congress knows. We don't know anything, and we're going to be the one to decide that question?"[1] Furthermore, the Supreme Court has suggested that they intend to rely on the FISC to monitor the constitutionality of the NSA's program.[2]

On the other hand, if Congress decides the issue, they may continue to sway toward allowing easier government access to communications data. Congress is likely to favor enhanced national security over personal privacy. However, if the current program's problems are not adequately resolved by the Obama administration and Congress in the coming months as they have suggested, the Supreme Court may have to

---

[1] Trevor Eischen, "Ginsburg, Scalia discuss NSA, freedoms," *Politico,* last modified April 17, 2014, accessed April 17, 2014, http://www.politico.com/story/2014/04/supreme-court-ruth-bader-ginsburg-antonin-scalia-105807.html.

[2] Clapper v. Amnesty Int'l USA, 133 S. Ct. at 1146 (2013), in Cornell University Law School Legal Information Institute, http://www.law.cornell.edu/supct/cert/11-1025, accessed April 20, 2014.

step in to prevent invasions of privacy, particularly if leaked information confirms the government's surveillance of content information.

Regardless of which branch resolves our present privacy problems, the current balance between serving the government interest and the reasonable expectation to privacy in communications is skewed, both in regard to the NSA's program and in regular application of the third party doctrine and the SCA to electronic communications. The SCA and the third party doctrine favor the government's ability to obtain information, and to achieve a more sound balance, both the SCA and the third party doctrine should distinguish between content and context information, thus ensuring Fourth Amendment protections to content information and keeping context information under the third party doctrine and the current rules of the SCA. Our right to privacy is critical in maintaining democracy, and the Jeffersonian vision that "[l]aws and institutions must go hand in hand with the progress of the human mind" challenges us to advance privacy protection in the digital age.