WHY CONGRESS NEEDS TO ACT TO UPDATE PROTECTION FOR ELECTRONIC COMMUNICATIONS FROM MULTIPLE AND EXTENSIVE THREATS FROM AROUND THE WORLD.

Frederick Greene
Eastern New Mexico University
Linda Naimi
Purdue University

ABSTRACT

This article analyzes the extent that digital privacy acts are adequately protected by existing law. The authors look at the historical protection of these rights, and note that the last major piece of legislation in the area was 1986. An analysis of the changes in society from 1986 to the present indicates that changes to current law are long overdue. The authors review some recommended changes and call for Congress to act to update American laws related to electronic communication.

The last time Congress passed a major piece of legislation that radically altered electronic communications was over thirty years ago. Digital and electronic communications have evolved exponentially since the passage of the Electronic Communications Privacy Act of 1986. The internet was in its infancy. Email existed but was not generally available or used by the public, and was the exclusive province of geeks and nerds. Mobile technology barely existed and had extremely limited functionality. Social Networking had an entirely different meaning related to personal in-person relationships—clearly not the internet phenomena known as social networking today. "Cloud computing" was two words not typically found in the same sentence. In the ensuing years since 1986, digital communications have exploded. It is astounding to see the vast amounts of data and information available online. Along with that tremendous expansion, we have seen the rise of internet banking, ecommerce, and online shopping, accompanied by a rising wave of internet crime and intrusions into personal privacy. Private citizens have become increasingly concerned about their digital privacy.

Today, courts disagree on what the constitutional protections may be relative to electronic communications and surveillance. United States Circuit Courts have split on the question as to what sort of protections exist from police intrusion into communications as well as electronic surveillance of movement. Additionally, private corporations and other entities have unprecedented access to information that at one time was private. A greater threat exists from hackers and rogue actors that are willing to compromise and steal valuable information, and even compromise elections. Historically, the courts have used a fourth amendment analysis to determine what rights and privileges should be afforded to citizens regarding their digital privacy. Many modern scenarios present questions implicating how fourth amendment protections will be analyzed and implemented. The current statute appears to "miss the mark"

when it comes to protecting against the type of intrusions and violations of personal privacy that exist with present technology.

The world has changed significantly in the past thirty plus years. In that short timeframe electronic communications has blossomed in a multitude of ways. Thirty years ago very few people knew of the existence of the internet, cell phones, email, GPS, Social Networking, or cloud computing. Today these terms and technologies are an everyday part of most American's lives. Over thirty years ago Congress passed the Electronic Communications Privacy Act of 1986. This statute has only been revised in a few minor ways. The basic statute still exists as it did when enacted. The courts have heard and decided numerous cases and decisions concerning the above technologies without the benefit of new Congressional guidance as to how Fourth Amendment rights should be weighed and protected. Many decisions from various courts contradict decisions from other courts. The United States Supreme Court has weighed in on only a few sparse cases, and there is significant controversy as to what rights are protected versus which rights are not.

The US Supreme Court very early on recognized that for the right to be "secure in their persons, houses, papers and effects" to be effective, there naturally must occur a right to "privacy." Although the word privacy cannot be found in the United States Constitution, its presence can be found in numerous cases. The Supreme Court has indicated that the Right to Privacy is within the "penumbras" of the Bill of Rights (Oyama, 2006). Privacy has been defined in many ways, but it generally is "the right to be left alone." It is considered an individual, personal right (Lasprogata, King, & Pillay, 2004).

The right to privacy in many ways is like personal property that can be traded away or bargained away. In the absence of willingly trading or bargaining away the right, it is considered an enforceable right against others that would violate that right (Lasprogata, King, & Pillay, 2004). The first cases that dealt with this right of privacy were not in an electronic context but in cases involving the United States mail. These cases, long before federal law was passed regarding electronic communication, addressed privacy rights in mail delivered by the US Post Office. The concept of privacy as it relates to mail was first promulgated in a US Supreme Court case called Ex Parte Jackson as early as 1877 (Pikowsky, 2003). Ex Parte Jackson (96 US at 727) held that:

> [A] distinction is to be made between different kinds of mail matter, between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined. Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.
>
> The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands

> of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the Fourth Amendment of the Constitution (Pikowsky, 2003, p. quoting Ex Parte Jackson, 1877).

Later cases dealing with postal mail generally have held that there is a reasonable expectation of privacy in the mail that requires a warrant for a package or letter to be opened by law enforcement. In the case of United States v. Van Leeuwen, the United States Supreme Court upheld statutory provisions Congress passed that codified protection of the United States Mail from warrantless searches (Pikowsky, 2003).

The first case that ever dealt with the issue of electronic surveillance was decided by the US Supreme Court in 1928 in the case of Olmstead v. United States (Horn, 2002). This case was decided almost 50 years after the telephone was invented by Alexander Graham Bell. Unfortunately, the case held that warrantless wiretaps of telephones were not a violation Fourth Amendment rights (Horn, 2002). This interpretation ultimately led to an act of Congress to curtail the warrantless wiretapping of telephones.

The Communications Act of 1934 said that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person" (Horn, 2002). Federal agencies routinely got around this congressionally mandated prohibition by claiming that the statute required two acts to become applicable; namely interception and divulgence. Federal agencies made it a point to indicate that they were only intercepting not divulging the information, so the act should not apply to their activities.

Ironically, Justice Brandeis dissented in the Olmstead case and provided what is considered to be one of the most visionary quotes from the bench nearly 70 years ahead of its time. Brandeis' dissent said;

> Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.... Can it be that the Constitution affords no protection against such invasions of individual security" (Olmstead v. United States, 277 U.S. 438, 48 S. Ct. 564, 1928. P. 474)

The practice of ignoring a warrant requirement continued until 1937 when the Supreme Court indicated that the Wiretap Act prevented federal agencies from warrantless wiretaps even without their divulgence of the information (Horn, 2002).

Two more US Supreme Court decisions in the next decade played a major role in defining the rights that individuals had in electronic telecommunications. Berger v. New York, and Katz v. United States. The Berger decision struck down a New York statute that authorized governmental warrantless wiretapping. The court noted that conversations are protected under the US Constitution, and that seizure of these conversations amounts to a search (Horn, 2002).

The Katz decision affirmatively held that law enforcement had to obtain a search warrant based upon the usual probable cause standard to monitor telephone calls placed from a telephone booth (Oyama, 2006). These decisions were tempered by a later decision in United States v. Miller that held that these

privacy rights did not exist where the contents of a private communication is revealed to third parties (Oyama, 2006).

Much of what the Supreme Court decided in Berger and Katz was ultimately codified into law with the 1968 passage of Title III of the Omnibus Crime Control and Safe Streets Act. Certain provisions of this legislation are commonly referred to as the Wiretap Act (Mulligan, 2004).

The pattern that emerges shows that in the thirty (30) years since passage of the ECPA, the world had changed drastically. Digital and electronic communications have become the paramount and ubiquitous manner of communication worldwide. The importance and significance of digital communication presents an entirely new challenge that could not have been envisioned in past eras. The need for digital privacy rights have far outstripped the need in years past. Simultaneously, society recognized that terrorism presented a real threat to the peace and security Americans want and enjoy. After the dreadful events on September 11, 2001, Congress immediately passed the Patriot Act that increased law enforcement's ability to snoop, spy, and track any person's electronic and digital communication. In the aftermath of that massive expansion of surveillance rights, US citizens have been left with a weakened or non-existent level of protection in digital and electronic communication. This article recognizes the tenor of the times and frank assessment of the current state of affairs and future needs. To that extent, this paper identifies numerous problems, looks at some proposed solutions and makes the clarion call for change.

The purpose of this article is to analyze the current status of digital and electronic privacy protection laws. The analysis was intended to gauge the status of protection afforded digital and electronic communications today with the protection levels of digital, electronic and non-electronic communications in bygone decades. Although the protection levels may be the same, and courts may be enforcing modern-day electronic and digital communications privacy rights in a similar manner as communications in the past, we can see that the United States does not adequately protect electronic and digital privacy rights with present laws and judicial rulings.

If various types of communication common today in the expanded electronic world do not enjoy the same level of protection that communications, electronic and non-electronic, had in the past, then it is clear that the law has lagged behind the advancements in communications technology leaving electronic communication rights and associated data security rights vulnerable and unprotected.

Congress could not have conceived in 1986 when it passed the Electronic Communications Privacy Act (ECPA) that was designed to regulate access by the government to Internet communications and records that the world of electronic communications would have grown to the dimensions that it has grown to today. The very assumptions that existed in 1986 are no longer applicable. The Internet was barely operational in 1986. Now a substantial part of commerce worldwide is conducted through the Internet. Additionally, the idea of social media had not even been born yet. Social media now accounts for a huge percentage of traffic on the Internet. Congress could not have even understood that the world itself which shrink, metaphorically, when the ability to post something in the Middle East that could be instantly read in China that could be instantly commented on in North America. The idea that indications would be

worldwide and instantaneous was more of a science fiction idea, than the reality that has become. Some of the major flaws that Congress could not have foreseen with the dramatic reduction in the cost of electronic storage. Many of you like us, may remember when storage was extremely expensive. Because of the prohibitive cost of storage and hard drives, most computers in the early 1980's did not even have a hard drive. The way you saved information was from 5 ¼ floppy disk to 5 ¼ floppy disk. Many computers had two floppy disk drives specifically so that you could save information from one to the other. The first "Windows-based system" had a 40 MB hard drive. Most of us now carry in our pockets smart phones with anywhere from 64-512 GB storage capacity. A law that was written in 1986 when storage was at a premium, by necessity focused on real-time surveillance. The law heavily prohibits access to real-time data but is quite weak in enforcing access into stored records. The idea of stored records doesn't even make sense today. Not only do we store things on our individual devices, but we have access to unlimited storage in the cloud. The idea that there should be a distinction between the government or any other entity having access to real-time information versus stored information is now nonsensical. Yet the 1986 Electronic Communications Privacy Act is heavily based on that distinction. Any new law or any new protection has to recognize that privacy rights are not contingent upon the storage medium, but that privacy rights should be absolute.

Some of the major proposals that exist today for fixing the problem related to lack of privacy protections in electronic communications, are promulgated by what is known as the Digital Due Process Coalition. This coalition, including many companies that are household names, including; Apple Computer, Facebook, Alphabet Inc. (the owner of Google), Amazon, Adobe, AOL, eBay, Hewlett Packard, Microsoft, as well as the American Civil Liberties Union, to name a few. This Digital Due Process Coalition (digitaldueprocess.org) has as a motto, "modernizing surveillance laws for the Internet age." If you go to their website you can see that they have a comprehensive and extensive approach to updating privacy laws in the United States. They list as their guiding principle:

> To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public (digitaldueprocess.org)

The Digital Due Process Coalition promotes four major principles. They are as follows;

1. The government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online.
2. The government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.
3. Before obtaining transactional data in real time about when and with whom an individual communicates using email, instant messaging, text messaging, the telephone or any other communications technology, the government should demonstrate to a court that such data is relevant to an authorized criminal investigation.

4. Before obtaining transactional data about multiple unidentified users of communications or other online services when trying to track down a suspect, the government should first demonstrate to a court that the data is needed for its criminal investigation. (digitaldueprocess.org).

While these four major principles are certainly a step forward from the antiquated and non-existent coverage now afforded by the ECPA, it really only involves tinkering at the edges. The idea that our electronic privacy should be held hostage to mere notions of probable cause that judges can ascertain based upon the flimsiest of evidence, really does not provide adequate protection of Americans privacy rights.

Without privacy there can be no liberty, liberty and privacy are intricately tied together. Privacy encompasses the ability to be left alone. Without the ability to be left alone, a major aspect of liberty is compromised. We all need the ability to engage in our own affairs without the involvement of others. Whether this occurs inside the home, the workplace, our automobiles, or any other place we may be, it is important right to simply not be bothered. Without privacy this right cannot exist. Privacy must be protected for liberty to thrive.

In light of the astounding number of breaches to security that we see today, our digital privacy rights need to be expanded and protected. After more than thirty years, it is time for Congress to pass expansive new legislation that will protect our elections, business communications, private communications as well as all other forms of electronic communications.

REFERENCES

Digital Due Process.Org (2016) Recommendations to modernize ECPA.

Greene, F. (2016) The path towards clear and convincing privacy rights. A dissertation submitted to Purdue University Graduate School. Published by Proquest, LLC. # 10172338.
(The current article is taken almost verbatim from selected portions of the 2016 dissertation with additional commentary and analysis.)

Horn, K. A. (2002) Privacy versus protection: Exploring the boundaries of electronic surveillance in the internet age. *Fordham Urban Law Review*, 29, 2233-2269.

Lasprogata, G., King, N. & Pillay, S. (2004) Regulations of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stanford Technology Law Review*, 2004, 4-62.

McDonough, T. Y. (2007). Internet communications privacy after United States V. Councilman. *Seton Hall Law Review*, 37, 1051-1073.

Mendez, N. (2008). Patent Infringers, Come Out With Your Hands Up! Should the United States Criminalize Patent Infringement?, 6 Buff. Intell. Prop. L.J. 34 (2008).

Mossoff, A. (2007). Who Cares What Thomas Jefferson Thought About Patents? Reevaluating the Patent "Privilege" in Historical Context, 92 Cor. L. Rev. 953.

Mulligan, D. K. (2004). Reasonable expectations in electronic communications: A critical perspective on the Electronic Communications Privacy Act. *George Washington Law Review*, 72, 1557-1597.

Oyama, K. A. (2006) E-mail privacy after United States V. Councilman: Legislative options for amending ECPA. *Berkeley Technology Law Journal*, 21, 499-524.

Pikowsky, R. A. (2003). The need for revisions to the law of wiretapping and interception of email. *Michigan Telecommunications and Technology Law Review*, 10, 1-71.