# The cost of convenience the extent of the reasonable expectation of privacy in the internet age

2013

Justin Karpf
*University of Central Florida*

# THE COST OF CONVENIENCE: THE EXTENT OF THE REASONABLE EXPECTATION OF PRIVACY IN THE INTERNET AGE

by

JUSTIN KARPF

A thesis submitted in partial fulfillment of the requirements
for the Honors in the Major Program in Legal Studies
in the College of Health and Public Affairs
and in The Burnett Honors College
at the University of Central Florida Orlando, Florida

Spring Term 2013

Thesis Chair: Dr. Robert Wood

# ABSTRACT

Though the Internet and social media are fairly recent developments, the legal principles and issues embodied in them are well-represented in the Constitution. Take, for example, the freedom of expression enumerated in the First Amendment. Though traditionally in print, pamphlets, and film, recent developments in technology such as Facebook and blogs have become the new standard forms of communication. Like the physical mediums that arose before them, issues arise of what limits, if any, should be placed on the speech. Given the guise of anonymity, people on the Internet have less accountability in the comments they make, which has led to things ranging from passionate political speech to what is known as cyber-bullying, which is online harassment that has led people to suicide.

This thesis, however, will primarily focus on the Fourth Amendment's reasonable expectation of privacy. Because the information involved with the Internet and social media is digital, it is more difficult to identify when privacy has been breached. With a paper envelope, for example, one can tell if the seal was broken and the contents were potentially disclosed to an unwanted party. Electronically, however, no such seal exists to notify the sender or recipient of a communication.

Furthermore, the Government has found itself under stricter scrutiny for searches with these new developments in technology; the lack of physical intrusion poses difficult questions for courts that must decide how far a reasonable expectation of privacy goes in the social media age.

The thesis will also address how private companies obtain and use individuals' information through the services they provide and the issues that arise from them. Private companies have fewer restrictions than the Government, and both perspectives are important to keep in mind when trying to understand the policy implications rapid technological growth has brought about.

The thesis will conclude by identifying issues that courts and legislatures will have to address in the coming years to adequately deliver justice in a dynamic society that is prone to powerful technological change.

# DEDICATION

For my friends, family, professors, and anybody else who has helped me through my undergraduate career.

# ACKNOWLEDGEMENTS

I would like to first and foremost thank my committee for all of their feedback and support throughout the entire process. This thesis would not be what it is today without the expertise and encouragement of Dr. Robert Wood, Dr. Carol Bast, and Dr. Raymond Surette. I would also like to thank Denise Crisafi, Kelly Astro, and the rest of the Burnett staff for helping to keep me on track over the past year. Writing a thesis is an incredible challenge to undertake and they had answers to all of my questions and gave me the resources to guide me along the way. Finally, I would like to thank my family and friends that have been there for me over this past year; this thesis is just one of the many challenges I faced and I cannot thank you enough for all of your support every step of the way.

# TABLE OF CONTENTS

# I. **INTRODUCTION**

The purpose of this thesis is, above all else, to apply a reasonable expectation of privacy to the twenty-first century environment of digital content and social media. New developments in technology have made it increasingly difficult for courts to apply legal precedent to new issues, even though the fundamental principles behind them are well-established.

This thesis will first examine the basics of the Internet and social media. Without getting into overly technical details, it will explain how digital content works, in terms of the transmission of information from one user to another and an explanation of the channels in between. It will also look at Federal statutes that apply to these "electronic communications" and show how courts have interpreted them with regard to speech, privacy, and piracy. It will then explain the issues surrounding Internet law, such as freedom of speech and privacy, in a historical context and show how courts have applied these principles to the Internet. Once these foundations have been established, it will discuss citizens' protection from the Government, by focusing on statutes and criminal cases.

Printed political pamphlets have been circulating since before this country was founded. The First Amendment to the Constitution guarantees that "Congress shall make no law . . . abridging the freedom of speech, or of the press" which, in the context of social media, applies to postings on websites such as Facebook or comments on the website of a news organization.

It should be noted that free speech is not unlimited; one cannot jokingly scream "fire" in a crowded movie theater, for example, because it would disrupt the peace and potentially endanger others. Similarly, one cannot coerce another into committing suicide. Present on the

Internet is what is known as “cyber bullying,” in which one, sometimes anonymously, mocks or ridicules another using social media. One recent example is the case of Dharun Ravi, a Rutgers student who used a digital camera attached to a computer known as a “webcam” to take video of his roommate, Tyler Clementi, kissing another man. After discovering this and reading Ravi’s twitter feed, which also had derogatory remarks, Clementi committed suicide.

A conundrum with digital content, courts have found, is that the lack of physical parameters, such as a seal on an envelope or broken window to a home make it difficult to tell if one’s privacy has been breached. Privacy is a well-established concept, but digital content is not as simple as physical content under the scrutiny of the courts. The physical location of a computer, for example, is primarily used to establish where a defendant resides, rather than as a scene for law enforcement officials to investigate.

This thesis will then explain how the Internet and social media have affected civil cases. It will explain what consumers can assume is private when services such as Google collect information from them. It will also explain the distinction between content and non-content information, as well as how much control one has over the content one posts. If, for example, a user of a photo-sharing service uploads an image to the Internet, does the user still retain rights to the image, or have they been forfeited? The thesis will conclude by addressing the double standard users have when giving their information away online to Governmental entities and private entities.

The purpose of this thesis is to examine what courts and scholars have found about the Internet and social media and to speculate how future courts might address these issues in light of the ever-changing dynamic of the Internet.

# II. BACKGROUND

The purpose of this section is to explain some of the technical terminology involving the Internet that a lay person may be unfamiliar with. It will not elaborate on HTML code or any technical aspects, but it will provide a foundation for those unfamiliar with technical details how the technology works and provide a basic understanding of some common terminology the thesis will use.

## A. Internet

The Internet is defined as "an electronic communications network that connects computer networks and organizational computer facilities around the world." In a layman's terms, this means that the Internet is a means for users of a computer to send data to other computers through networks. It is sometimes referred to as the "(world-wide) web," because of how interconnected it has made people.

Though initially used for research and military purposes, the Internet has become a tool average people use to communicate with each other on a daily basis. Early forms of web-based communication, that still exist today, include forums and chat rooms. Both of these services provide a means for individuals to hold conversations with one another with no geographical boundaries and expressing any views they may hold, political or otherwise. Many of these services do not require formal identification; users may choose a username that does not disclose their actual identities. A user connects to the Internet through the use of a browser, which allows users with an Internet connection to access websites, which are pages on the Internet that individuals can access by specifying the appropriate location. This location is known as a

uniform resource locater (URL) and every website has them. Without getting too technical, a URL tells the web browser where on the Internet the page a user is trying to access is located. Websites, browsers, and other electronic services may also store cookies about a user, which are "small file[s] or part[s] of a file stored on a World Wide Web user's computer, created and subsequently read by a Web site server, and containing personal information (as a user identification code, customized preferences, or a record of pages visited)."[1]

**B. Network**

A network is a series of connected computers. They vary in size and can cover an entire University or a single building depending on the strength. Networks are generally wireless, using devices such as modems, which connect a computer to the Internet through a cable, and routers, which transmit a wireless signal that other computers can use to connect to the Internet. A network traditionally has clients, who send requests, and servers, who process the clients' requests.

**C. Peer to Peer**

Peer to Peer is a type of network that allows users to act as both a client and a server, thus bypassing the traditional middleman involved with file-sharing. These have been increasingly scrutinized lately, due to their common use with Internet piracy.

**D. Internet Service Provider (ISP)**

An Internet service provider is, as the name suggests, a service that provides a user access to the Internet, generally for a fee. It should be noted that in order to provide a customer with

[1] "Cookie." Merriam-Webster. (2011).

Internet access, the ISP needs to have information such as their name and physical address, as well as an IP address that the ISP issues.

**E. Internet Protocol (IP) Address**

An Internet Protocol (IP) Address is an identifying number assigned to a device, such as a computer, on a network.

**F. Social Media**

"Social media" refers to services on the Internet that allow people to connect to one another in various ways. Though it can be used for professional or networking purposes, most people choose to use social media for personal, recreational use. This thesis will outline some of these services and explain how users' privacy has been an issue for the courts over the past decade or so.

One common example is "Twitter." Twitter is a service that allows users to post short text-based messages that those who "follow" their profile can see. The messages are visible, however, to people who do not follow the user, or even necessarily have a Twitter account of their own.

Another example is Facebook, a popular service in which users create a personalized page, known as a profile, through which they can share photos, their location, and any text or picture-based content they choose through a method known as "posting." This information is visible to other users who the poster allows access to their profile known as "friends." Content posted includes "status updates," where a user posts a message for the user's friends to see.

Though there are millions of users on Facebook from many different countries, users have some control over who gets to see the content they post. The friends allowed to see one's profile, however, have wide discretion over what they share. So, for example, if a user posts a photograph for the user's friends to see, there is nothing stopping the friends from sharing the photograph with parties the original user did not intend to have access. This concept of shared information is not exclusive to digital concepts. The same principle applies to mailing a physical letter; once it reaches its destination, the original sender has no control over who gets to see the content.

**G. Speech**

Though a constitutionally guaranteed right to freedom of speech and expression exists, it is not unlimited. For example, in 1964, in *New York Times v. Sullivan*,[2] for defamation, the Supreme Court held that in order to recover damages, a public figure must prove "actual malice." The concept of "actual malice" is a restriction on what individuals are allowed to say about a public figure, which leads to difficult questions for modern courts. If, for example, individuals post content on the Internet, making it public information, does it make them a public figure?

Furthermore, "obscene" material is not constitutionally protected, as defined by the Supreme Court in the 1973 case *Miller v. California*.[3] In this case, the Court created a three-pronged test to determine what is obscene: "(a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest. . .(b) whether the work depicts or describes, in a patently offensive way, sexual

[2] *New York Times v. Sullivan*. 376 U.S. 254 (1964).
[3] *Miller v. California*. 413 U.S. 15. (1973).

conduct specifically defined by the applicable state law, and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value."[4]

**H. Searches and Seizures**

The Fourth Amendment to the Constitution protects individuals from unreasonable searches and seizures, although it is up to the courts to determine what is unreasonable. Though the privacy traditionally referred to privacy in one's own home, new technology has complicated the concept. The reasonableness of a seizure, for example, was traditionally determined by the individual's loss of liberty during the duration of the search. With digital content, however, a government entity searching through an individual's files may experience no tangible loss of liberty during the duration of the search, and the individual may not even be aware of the intrusion as it occurs. Despite the lack of physical inconvenience, however, courts have held that individuals do have a reasonable expectation of privacy with their digital files, although it is not unlimited. As the thesis will describe in detail later, the amount of privacy one has with a digital file is largely dependent on how the file is obtained, who it is being shared with, and how it is being used.

[4] Id.

## III. PROTECTION FROM GOVERNMENT (CRIMINAL CASES)

A growing concern in recent years has been over how much the Government can intrude into an individual's digital content. Though certain files, such as business and medical records, are meant to be private, they are sometimes required for investigations into criminal matters. This leads to a balancing act between an individual's expectation of privacy and the public's interest in adequate law enforcement. If crimes are being committed on the Internet, law enforcement must adapt accordingly. Furthermore, freedom of speech and expression are crucial to a democracy, but threats, for example, generally warrant an investigation to determine if they are credible. The First and Fourth Amendments to the Constitution are restrictions on the Federal Government, and apply to the states through the Fourteenth Amendment.

### A. First Amendment

The First Amendment provides that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances" and protects speech as one of our most cherished rights. Though originally intended to protect only political speech, courts have consistently expanded speech, regardless of whether or not it is digital, printed, or verbal, is constitutionally protected.

The Supreme Court addressed the Internet specifically in 1997, when Justice Stevens noted in his opinion for *Reno v. American Civil Liberties Union* that, in previous cases, " [the] Court relied on the history of extensive Government regulation of the broadcast medium…the scarcity of available frequencies at its inception…and its 'invasive' nature," with regards to the

need to regulate television and radio due to concerns of limitations on the ability to connect, such as interstate broadcast signals and radio frequencies.[5] The Court also upheld the district court decision that found no need "for qualifying the level of First Amendment scrutiny that should be applied to this medium." [6]

Those factors are not present in cyberspace. As the Court noted, "[never before] have the vast democratic forums of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry."[7]

Perhaps the most notorious controversy regarding Internet speech is that of Tyler Clementi, a gay student at Rutgers University in who was bullied online by his roommate and committed suicide in 2010. The roommate, Dharun Ravi, used a webcam, which is a digital camera attached to a computer, to spy on Clementi engaging in sexual activity with another man on two occasions. Clementi asked to have the room to himself to have a guest over, and Ravi used his computer's webcam to film Clementi while Ravi was out of the room, watching the feed from a friend's room and encouraging his Twitter "followers" to watch the video footage live, which is known as a "livestream," as well. "Follower," in the context of Twitter, refers to a user who subscribes to, or "follows" another user, and sees the content the user posts. Clementi was among Ravi's followers and saw the message, and turned the webcam off for his second romantic encounter. After seeing, and saving, some of Ravi's tweets, Clementi committed suicide by jumping off the George Washington Bridge.

[5] *Reno v. American Civil Liberties Union*. 521 U.S. 844. (1997).
[6] Id. at *Reno*
[7] Id. at *Reno*

This case did not involve a reasonable expectation of privacy protection under the Fourth Amendment because Ravi was not an agent of the Government; he was a private individual with whom the deceased shared a room. There were, however, criminal charges brought against Ravi by the State of New Jersey. Although Ravi was within his rights to post messages, known as "tweets," such as "roommate asked for the room until midnight. I went into molly's room and turned on my webcam. I saw him making out with a dude. Yay" or "I dare you to chat me between the hours of 9:30 and midnight. Yes, it's happening again." Both tweets referred to the webcam Ravi left on for others to view Clementi's sexual encounter and these communications were made with malicious intent. Though nothing expressly unlawful was stated, courts must address if Ravi's right to post content outweigh the violation of privacy Clementi experienced. It is reasonable to assume that Clementi's privacy in his place of residence would be the stronger interest, but legislatures have yet to codify that sentiment.

Furthermore, Ravi was found guilty of tampering with physical evidence by deleting his tweets and text messages. The key phrase in this charge was "physical," because an electronic communication is digital, not physical. Though the same conditions applied, this is a distinction that legislatures should address in the near future; if the nature of the evidence is not physical, the charge should be distinguished accordingly.

This incident occurred in a school setting, and Courts have consistently held that schools can restrict students' speech in certain scenarios according to certain factors.

As Katherine Hokenson notes, "Supreme Court precedent [was] made before the Internet."[8] The most famous Supreme Court case dealing with student speech was *Tinker v. Des Moines*, where students wore black armbands to protest the war in Vietnam and were suspended. [9] On appeal, the Court famously held that "it can hardly be argued that either students or teachers shed their constitutional rights to freedom of speech or expression at the schoolhouse gate," although it noted that speech can be limited if the action "was caused by something more than a mere desire to avoid the discomfort and unpleasantness that always accompany an unpopular viewpoint."[10] For example, "1) if the speech materially and substantially interferes with the requirements of appropriate discipline in the operation of the school, or 2) if it interferes with the rights of others," it can be censored.[11]

An example of speech that warranted censorship was the Second Circuit's *Wisniewski* case, where a middle school student created a violent image with the message "kill Mr. VanderMolen," who was his English teacher at the time, on the Internet from a computer located outside of the school and sent it to some of his friends.[12] When the teacher in question was made aware of the image, the student was disciplined. In its ruling, the court held that "the potentially threatening content of the icon and the extensive distribution of it, which encompassed 15 recipients, including some of Aaron's classmates, during a three-week circulation period, made this risk at least foreseeable to a reasonable person, if not inevitable. And there can be no doubt that the icon, once made known to the teacher and other school officials, would foreseeably

[8] Hokenson, Katherine, MY TEACHER SUX! [CENSORED]: PROTECTING STUDENTS' RIGHT TO FREE SPEECH ON THE INTERNET. 28 J.Marshall J. Computer & Info. L. 385 (2011).
[9] *Tinker v. Des Moines Independent Community School Dist.* 393 U.S. 503 (1969).
[10] Id.
[11] Id.
[12] *Wisniewski v. Board of Educ. of Weedsport Cent.* School Dist.494 F.3d 34 (2d Cir. 2007).

create a risk of substantial disruption within the school environment."[13] So, even though the electronic speech was not made on school grounds, the fact that it had the potential to disrupt school operations gave the school board authority.

Universities, however, are not necessarily bound by the same restrictions as lower institutions. If, for example, Rutgers provided the Internet access to Clementi and Ravi, who lived in the dorms, should they have monitored the postings more carefully? Though monitoring students' Internet activity may have prevented this particular tragedy, society may not be willing to accept this practice as a solution It is too early to tell how legislatures and courts will rule on this particular issue, but a reasonable method would be to treat the University that provides Internet access the same way as an ISP, which diminishes an individual's expectation of privacy but does not diminish it completely.

**B. Anonymity**

An important issue that complicates Internet privacy law is the concept of anonymity. The Supreme Court held in a 1960 case, *Talley v. California*, that "anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all."[14] In *Talley*, the Court discussed the constitutionality of distributing political pamphlets that did not have the author's name or information and held that speech is protected regardless of whether the author takes credit for the work. Further, in *Reno*, the Court also held that "this dynamic, multifaceted category of

[13] Id. at *Wisniewski*
[14] *Talley v. California*. 362 U.S. 60 (1960).

communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer."[15]

Thus, this same principle of freedom of expression applies to the Internet. Because it has been held that the Internet is protected, any anonymous speech on the Internet is held to the same standard as conventional speech, which means that an individual in a forum or chat room does not lose First Amendment protection because an individual's username does not reveal personal information. As the thesis will address later, however, law enforcement has legal methods of obtaining warrants to reveal an anonymous user's personal information through their ISP.

**C. Fourth Amendment**

Most crucial to this thesis is the Fourth Amendment, which protects "the right of the people to be secure…against unreasonable searches and seizures." The Supreme Court has since interpreted this to guarantee a "reasonable expectation of privacy."[16] Though it traditionally applies to physical locations, such as one's home, person, or vehicle, several jurisdictions have established that this expectation still exists with electronic communications and digital content such as files, though this expectation is diminished due to several factors.

One such factor is that any information communicated over the Internet is not exclusive to a user's computer, in that it is accomplished via a network by definition. Furthermore, an

[15] Id. at *Reno*
[16] *Katz v. United States*, 389 U.S. 347 (1967).

internet user's ISP sees the information in the process of sending it to the intended server, so it is not strictly private.

One method of determining whether there is an expectation of privacy is through making the distinction between content and non-content information. As Stanford Professor Orin Kerr explained, "online, non-content surveillance is usually surveillance related to identity, location, and time; content surveillance is surveillance of private thoughts and speech."[17] Kerr further explained how the very function of networks promotes this theory: "communications networks are mechanisms for delivering contents that would otherwise have to be delivered in person, and the non-content information on the network is the information needed to deliver the communication that substitutes for the public act of delivering contents."[18]

The rationale behind this theory is similar to mailing a physical letter through the postal service. To mail a letter, one must postmark it and state a return address and the address to which it is being sent. Under Kerr's theory, this information would be non-content, which in the context of the internet would be the parties' name and subscriber information, such as ISP and physical address. The statements in the letter itself, on the other hand, would be content information. The letter, like the information in an electronic communication, "isn't handled by the Post Office; the contents are of no concern to the Post Office, as the contents are only the concern of the sender and receiver."[19] As the Sixth Circuit noted in *Warshak*, "given the

[17] Kerr, Orin. Applying the Fourth Amendment to the Internet: A General Approach. 62 Stan. L. Rev. 1005. (2010).
[18] Id.
[19] Id.

fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[20]

Furthermore, an individual's address is not private information, because anybody with a phone book can look up someone's personal information. Simply knowing the location of a person's residence, however, does not give one the right to invade the person's personal belongings and see items in their home. This is known as the inside-outside distinction. As Kerr noted, watching somebody drive home and seeing where they park the car is outside information; it is simply information about the person's whereabouts.

Inside information, on the other hand, is the functional equivalent of content information. Using the example of somebody's house, inside information would consist of a person's belongings inside the home. Some inside information may be visible, just as items sitting on a desk by an open window might be visible to a passerby. But just as storing an item in a drawer or a room with no windows increases the expectation of privacy of an item, "storing the file on a password-protected server is the virtual equivalent of keeping it in a home." [21]

It should be noted that the reasonable expectation of privacy only exists until the information reaches its intended recipients. Once an e-mail reaches its intended recipient(s), for example, the sender no longer has a reasonable expectation of privacy because those receiving the content are free to disclose its contents to others, assuming that no legal duty of confidentiality exists that would otherwise protect the contents from exposure. This is the equivalent of somebody making a photocopy of a letter that they receive and handing copies out

[20] *U.S. v. Warshak*. 631 F.3d 266 (2011).
[21] Id. At *Kerr*

to others, because the original sender has no control over what the recipient does with the content.

**D. Electronic Communication Statutes**

In addition to the protections afforded by the, Congress has created a criminal statute that further limit the government's ability to intrude on an individual's privacy, The Electronic Communications Privacy Act of 1986 ("ECPA") sets guidelines for how digital information may be intercepted and used as evidence in court.

First and foremost, the statutory definition of "electronic communication" under federal law is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[22] This statute also defines a user as "any person or entity who uses an electronic communication service and is duly authorized by the provider of such service to engage in such use." Furthermore, "electronic communications system" is defined as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[23] An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[24]

Additionally, a "computer trespasser" is defined as "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any

[22] 18 U.S.C § 2510 (2006 & Supp. 2012).
[23] Id.
[24] Id.

communication transmitted to, through, or from the protected computer; and does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."[25]

The ECPA states that not all electronic communications are meant to be private.[26] A user's post in an online chat room that other users can view, for example, would not be protected by the Act, because posting in such a manner waives any expectation of privacy. Title 18 U.S.C § 2511 also imposes a fine or imprisonment for no more than five years, or both for anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any…electronic communication [and] uses…any electronic, mechanical, or other device to intercept any oral communication."[27]

Later statutes in the ECPA dictate some exceptions, such as having a warrant signed by a judge, but, as a general rule, "intentionally disclosing or endeavoring to disclose, to any other person the contents of [an] electronic communication, [or knowing] that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection" is a crime.[28] Furthermore, anybody who discloses the contents of an unlawfully intercepted electronic communication is also subject to penalties.

Though electronic communications are not physical in nature, the devices that intercept them are. The next statute in the ECPA, 18 U.S.C.A. § 2512, regulates the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting

[25] Id.
[26] 18 U.S.C § 2511 (2006 & Supp. 2012).
[27] Id.
[28] Id.

devices and prohibits individuals from manufacturing or mailing devices if "the design of such device renders it primarily useful for the purpose of the surreptitious interception of…electronic communications."[29]

The statute makes exceptions for "[providers] of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, " as well as "an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof," who are permitted under this statute "to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications."[30]

Furthermore, "[it is not] unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device." [31] The ECPA also authorizes the confiscation of devices "used, sent, carried, manufactured, assembled, possessed, sold, or advertised" that violate the earlier sections.[32]

[29] 18 U.S.C § 2512 (2006 & Supp. 2012).
[30] Id.
[31] Id.
[32] 18 U.S.C § 2513 (2006 & Supp. 2012).

Though the government does have the authority to confiscate devices involved, "whenever any…communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any [criminal proceeding]."[33]

Furthermore, the government does not have unlimited discretion in what it intercepts. The ECPA outlines the scenarios in which law enforcement is authorized to intercept electronic communications. A federal judge, for example, "may grant…an order authorizing or approving the interception of…communications by the Federal Bureau of Investigation, or [another Government Agency] if certain conditions are met."[34] This does not apply to all offenses, but some applicable criminal offenses are violent crimes, counterfeit, or any communications involving the location of a fugitive.

Just because a law enforcement officer knows the content of an electronic communication does not mean that the information is admissible in court. The officer may, however, "disclose such contents to another investigative or law enforcement officer [if such disclosure is relevant to the scope of their duties]."[35] Furthermore, "any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information."[36]

The ECPA then goes into detail about the procedure of intercepting these communications in 18 U.S.C.A. § 2518. Any law enforcement official who wants to intercept an

[33] 18 U.S.C § 2515 (2006 & Supp. 2012).
[34] 18 U.S.C § 2516 (2006 & Supp. 2012).
[35] 18 U.S.C § 2517 (2006 & Supp. 2012).
[36] Id.

electronic or digital communication to help an investigation must provide the individual's name and the nature of the crime they suspect is about to be committed, is being committed, or has been committed. An officer cannot, for example, simply search an individual's computer on a hunch. The officer must articulate a clear reason to the judge issuing the warrant and explain the facts and measures up to that point in order to have a legal search.

Furthermore, the searches authorized under the statute are very limited in scope. An officer may not "authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days."[37] Judges must also create reports detailing the type of orders granted, as well as their results.[38]

The ECPA only regulates law enforcement obtaining access to these electronic communications. There are, however, additional laws that address unauthorized access to electronic communications, known as the Stored Communications Act ("SCA"). Under this Act, "whoever intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility" shall be fined or given prison time. Furthermore, an individual who works for an internet service provider is prohibited from disclosing the contents of communications the individual works with while performing the job.[39] For example, if somebody is repairing a company's server and sees a user's communications, the employee is not allowed to disclose the contents, even though the employee came upon them legally.

[37] 18 U.S.C § 2518 (2006 & Supp. 2012).
[38] 18 U.S.C § 2519 (2006 & Supp. 2012).
[39] 18 U.S.C. § 2702 (2006 & Supp. 2012).

This prohibition may be waived by the sender or intended recipient of the communication, disclosed to the provider of the service if it is necessary to the rendition of that service or to a law enforcement or government entity if "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[40] An example of this last exception would be if somebody lawfully executing their duties as a service provider notices a threat of violence that they believe to be credible, because society's interest of preventing serious harm outweighs an expectation of privacy if it can stop a serious crime from being committed.

This rationale applies to private individuals working as service providers. The government may not simply access a provider's records to look for violent threats. If the government have reason to believe there is a crime about to be committed, they must obtain a warrant as per 18 U.S.C. § 2518.

Providers may, however, be required to disclose electronic communications if certain conditions are met. For example, if a warrant is issued pursuant to 18 U.S. C. § 2518, the warrant will be served to the service provider in order to obtain the access, without letting the owner of the contents know.[41] The providers under this statute are required to disclose an individual's name, address, records pertaining to use of the service, telephone number or IP address, and means of payment for the service. This is common in Internet piracy cases, where individuals download content, such as music or movies, illegally at no cost.

[40] Id.
[41] 18 U.S.C. § 2703 (2006 & Supp. 2012).

In *ACHTE*, for example, individuals who downloaded music over the Internet were given notice by their ISPs that their identifying information had been requested.[42] Upon being given subpoenas with the IP address of their computers, along with the date and time they were alleged to have used the Internet to download or upload the particular movie, the defendants filed motions to quash the subpoenas.[43] The motions were denied, because the information requested was given in a lawful manner. The distribution company had a lawful claim of ownership over the digital content, and the individuals did not have a reasonable expectation of privacy with regard to their non-content information.

Furthermore, as the U.S. District Court held in *First Time Videos*, "alleged [copyright] infringers' First Amendment right to anonymous speech on the Internet [was not more compelling than the] right of [owners] of adult videos and photographs to use the judicial process to pursue its prima facie copyright infringement claims by serving the subpoenas on alleged infringers' [ISP to obtain identifying information]."[44] The Court held that the identifying information is not privileged or confidential enough to quash a warrant, and that their First Amendment right to expression in the context of downloading files does not outweigh First Time Video's "claim of actual harm under a theory of copyright infringement."[45]

It should be noted that the information, as stated earlier, is given by the user to the service provider to access the Internet, so it is the service provider disclosing the information to the law enforcement agency, not the user. Because the user does not have a reasonable expectation of privacy with information the users give to the service provider, the service

[42] *ACHTE/NEUNTE BOLL KINO BETEILIGUNGS GMBH & Co. v. DOES.* 736 F. Supp. 2d 212 (Ct. 2010).
[43] Id.
[44] *First Time Videos, LLC v. Does 1-500*. 276 F.R.D. 241 (2011).
[45] Id.

provider disclosing the information to a government agency does not violate the user's Fourth Amendment expectation of privacy. This concept is crucial for Internet piracy cases.

An interesting distinction regarding these warrants or court orders and traditional ones is that an officer's presence is not required to execute the warrant, while with a traditional search warrant an officer would go to the location specified and execute the warrant in person.[46]

These statutes can also be problematic with regard to the Fourth Amendment. In *Warshak*, for example, the Sixth Circuit held that a violation of the an individual's reasonable expectation of privacy does not necessarily mean that evidence is not admissible in court. In this case, Warshak "enjoyed [a] reasonable expectation of privacy in his e-mails vis-a-vis his Internet service provider (ISP) and government agents violated his Fourth Amendment rights by compelling ISP to turn over email without first obtaining warrant based on probable cause," but, "because agents relied in good faith on provisions of [the SCA],[the] exclusionary rule did not apply." In simpler terms, this means that unlawfully obtained electronic communications are not always make the inadmissible as evidence and good-faith exceptions apply just as they do with physical evidence.

**E. Ontario v. Quon**

The Supreme Court addressed the reasonableness of searching electronic communications for government employees in the 2010 case *Ontario v. Quon*.[47] In *Quon*, the Court addressed a law enforcement officer's reasonable expectation of privacy with regard to messages on his work-provided cell phone.

[46] 18 U.S.C. § 2703 (2006 & Supp. 2012).
[47] *Ontario v. Quon*. 130 S.Ct. 2619 (2010).

In this case, Quon was a member of the Ontario, California police department, which had a contract with Arch Wireless, which provided the department mobile service that, contractually, had a "monthly limit on the characters each pager could send or receive," and if a pager went over its character limit, there would be a fee.[48] As government employees, members of the department were subject to the City's "Computer Usage, Internet, and E-mail Policy" that went into effect before the pagers were distributed. This policy stated that the City "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources," and Quon signed a statement acknowledging that he had read and understood the policy.[49]

Though the policy did not outline text messages explicitly, Lieutenant Steven Duke, the officer responsible for the contract with Arch Wireless, told Quon and other officers that messages sent on the pagers would be treated as e-mails and were, thus, subject to audit. The significance of this distinction is that text messages were transmitted through Arch Wireless' radio station frequencies from an individual pager while e-mails were sent through the City's own data servers.[50]

After going over his character limit on several occasions, Quon's messages were audited by Chief Scharf, his superior, in order to determine if the City needed to increase its monthly character limit for the pagers. Lt. Duke, the individual responsible for conducting the audit, "reviewed the transcripts and discovered that many of the messages sent and received on Quon's

[48] Id.
[49] Id.
[50] Id.

pager were not work related, and some were sexually explicit."[51] After the police department's internal affairs division was notified of this conduct, Quon was disciplined.

Quon alleged that his Fourth Amendment reasonable expectation of privacy was violated when his text messages were audited, arguing that the audits were unwarranted because he paid all of the overage fees himself. He also alleged that Arch Wireless violated 18 U.S.C.A. § 2701 by disclosing the contents of his messages.

The issue was whether or not the search was reasonable, and the Court held that it was. It had been previously held in *O'Connor v. Ortega* that "individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer."[52] In his concurring opinion to *Quon*, Justice Scalia wrote that "government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable in the private-employer context—do not violate the Fourth Amendment."[53] Furthermore, the City's policy made it clear that the messages on the pagers were not to be considered private and could be audited at any time. The Court held that "reviewing the transcripts was reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use," and was not "excessively intrusive."[54] Furthermore, the Court held, "it may have been reasonable as well…to review transcripts of all the months in which Quon exceeded his allowance, it was certainly reasonable…to review messages for just two months in order to obtain a large enough sample to decide whether the character limits were efficacious," which is

[51] Id.
[52] *O'Connor v. Ortega*. 480 U.S. 709 (1987).
[53] Id. at *Quon*
[54] Id. at *Quon*

reinforced by the fact that all of Quon's off-duty messages were redacted.[55] The Court also found that "because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope…it was reasonable.[56]

Justice Kennedy, who wrote the opinion, explicitly noted how the effect of new technology on law is complicated. For example, he wrote, "rapid changes in the dynamics of communication and information transmission are [evidenced] not just in the technology itself but in what society accepts as proper behavior."[57] He reinforced this point by quoting *amici* briefs which noted that employers' acceptance, and even expectation, that employees use mobile devices such as pagers because they can often increase worker efficiency. The Ontario police department in *Quon*, for example, got the pagers as a way for SWAT members to communicate quickly and effectively on the job. Kennedy also wrote that "cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification," a point that can either strengthen the case for an expectation of privacy," or, conversely, that their affordability could mean that employees should be responsible for obtaining their own mobile devices for personal use.[58]

*Quon* raises issues that courts will have to address in the near future in order to adapt existing law to our rapidly changing society. If mobile technology such as cell phones are truly as accessible and prevalent as Kennedy implies, courts must decide how far a reasonable expectation of privacy goes. In *O'Connor*, the Court held that "the question of whether an

[55] Id. at *Quon*
[56] Id. at *Quon*
[57] Id. at *Quon*
[58] Id. at *Quon*

employee has a reasonable expectation of privacy must be addressed on a case-by-case basis," but this approach could create too many issues for courts to handle-- a framework must be established so that the average, reasonable person can be educated as to how far their privacy rights go.[59] This is especially important because Kerr's content, non-content distinction is not codified; it is simply an approach that one may use to interpret existing law.

It is also difficult to say whether the Courts or Congress should be responsible for addressing these issues. Though Congress has written statutes that deal with electronic communications and privacy, there are still many issues for Courts to address.

[59] Id. at *O'Connor*

## IV. PROTECTION FROM OTHERS (CIVIL CASES)

Because the Constitution and statutes only apply to government actors and most digital content is given to a service provider, there are also civil legal issues pertaining to the Internet that must be addressed. Furthermore, while Internet users have little expectation of privacy with the information they provide, they maintain some control over how the information is shared.

It should be noted that many ISPs and web-based service providers have terms of service and privacy policies that users must agree to. Some of these terms of service address how a user's information will be used. In one such example, the Court addressed an individual's expectation of privacy with regard to his e-mail. In the majority opinion, the Court held that the defendant was "afforded more privacy than similar messages on the Internet, because [his e-mails were] privately stored for retrieval on AOL's centralized and privately-owned computer bank."[60] Furthermore, AOL's policy was not to read or disclose subscribers' e-mail to anyone except authorized users, which gave additional privacy protection in addition to any federal statutory protections and it was AOL's practice to guard these "private communications" and only disclose them to third parties if given a court order.[61] Kennedy also wrote that "while implicit promises or contractual guarantees of privacy by commercial entities do not guarantee a constitutional expectation of privacy, we conclude that under the circumstances here appellant possessed a reasonable expectation of privacy, albeit a limited one, in the e-mail messages that he sent and/or received on AOL. Expectations of privacy, however, have limitations, and this case illustrates some of them."[62]

[60] *U.S. v. Maxwell*. 45 M.J. 406 U.S. Armed Forces (1996).
[61] Id.
[62] Id.

It should also be noted that the location of the server is not generally an issue in these cases, because the Government contacts the service provider directly for access to electronic communications. Furthermore, *Maxwell* was a military case; there are different procedural rules to the average individual, but the legal reasoning behind it is still relevant.

There are, however, cases where the physical location of the computer is material. Whether or not a student's statement was made using a school computer, for example, could give jurisdiction over online content, but the concept is not limited to students. In *White v. White,* for example, a New Jersey Court addressed a divorce case where the wife accessed her husband's e-mails on a computer in their home.[63] After finding a letter from her husband's girlfriend, White hired an investigator. The investigator copied files from the computer's hard drive and sent copies of the electronic communications to White and her attorney. It is important to note, however, that they did not actually access her husband's password-protected America Online (AOL) account to get this information, but rather accessed e-mails that were saved on the computer.

This was possible because AOL allows users to save e-mails, once they have logged into their password-protected account, to their computer for offline access. The case was decided in 2001, when Internet connection was primarily dial-up, a method that was not as readily available or convenient as wireless networks are today. As an expert witness testified, "[an] AOL user must voluntarily choose to save the e-mail, attachment or address to his [computer]. The AOL user can save e-mail, attachments or addresses either by using the automatic AOL feature or

[63] *White v. White*. 344 N.J. Super. 211. 781 A.2d 85 (2001).

manually."[64] Though the AOL account is password-protected, the saved e-mails do not have password-protection by default; they can be accessed from a user's computer without using a password. Because White did not unlawfully use her husband's password to access the content, his expectation of privacy was not violated.

The physical location of the computer was also relevant to the analysis because it was in the family's sun room, which White and her children had access to and utilized often. Her husband, the Court held, had no reasonable expectation of privacy for files saved on the hard drive of a computer that other people have access to and are not password-protected. If White had used her husband's password to access the files, rather than accessing the files on the family computer, then she would have violated the SCA.

Furthermore, the expectation of privacy diminished when an e-mail was sent; once the file was saved on a computer that others had access to, those others could access them lawfully. If the husband had password-protected the files on the hard drive, then there would have been a reasonable expectation of privacy, because a password on a computer is the functional equivalent of a lock and key on a file cabinet.

**A. Google**

Google, founded in 1998 by Larry Page and Sergey Brin, is one of the largest Internet-based companies in the world. Though it started as a crawler-based search engine, which is a website where a user inputs a phrase or topic and the search engine finds websites that has those terms, it has since expanded to include a social media platform, mobile applications, and

[64] Id.

electronic mail. As a premier Internet-based company, many issues that have arisen in recent years have been through Google's services.

Such is the case with Google Buzz, a social media platform. Before going into detail about this service, one must understand the interconnectivity between Google's services. By making an account with Google, a user has access to several different features including electronic mail, YouTube, which is a popular video sharing service, Google Chrome, which is a web browser, and many others. Google's current social media platform, Google+, has addressed many of these issues, largely due to the problems encountered by its predecessor.

The Federal Trade Commission (FTC) was established in 1914 to prevent anti-competitive business practices, and its jurisdiction has since expanded to include the authority to punish companies for using "misleading and deceptive practices" to exploit consumers over the Internet. In 2012, the FTC issued a complaint against Google for a controversy surrounding a social networking service called "Google Buzz," which allowed user to follow people they had in their contact book with Gmail, Google's electronic mail service. When Google Buzz was first implemented, Gmail users were given options to opt-out of the new service, but there was still a tab for Google Buzz in their inbox. Clicking the tab, even by mistake, would cause a user to "be taken to the Buzz welcome screen and automatically enrolled in Buzz, without any disclosure of that fact and without any further action."[65] Though users from October 2004 to October 2010 were given notice that "Gmail stores, processes and maintains your messages, contact lists and other data related to your account in order to provide the service to you," information about how Google would use the information was not provided until October 2005,

[65] Leibowitz , Jon, William Kovacic, J. Thomas Rosch, Edith Ramirez, and Julie Brill. United States of America. Federal Trade Commission. In the Matter of Google Inc., a corporation. Web. (2011)

when the company added "when you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use," to its privacy policy.[66] The issue this presented for users was that contacts they had previously blocked from seeing their personal information in Gmail were able to see that information in Buzz. In addition to people blocked in Gmail, users without public Google profiles or those who did not provide their first and last name when setting up their Google account could not be blocked. Among the information available to followers on Google Buzz was a list of contacts, which many clients need to be confidential.

The visibility of personal information to unauthorized parties is particularly problematic for users such as doctors and attorneys, whose contacts include clients that value confidentiality. In addition to professionals, some users had clients such as ex-husbands with restraining orders against them, who were able to get more information about their ex-spouse through the Google Buzz profile.[67]

Though Google eventually remedied the situation by adding features that allowed users to keep their information more private, such as by being able to block any follower, even if they did not have a profile, it violated federal law, as written by the FTC, for its "misleading and deceptive practices." The option "nah, go to my inbox," that was given to users on the day Google launched its Buzz service, according to the FTC, meant that users had "represented, expressly or by implication, that [users] who clicked on these options would not be enrolled in

[66] Id.
[67] Id.

Buzz."[68] Users who selected this option and later clicked the Buzz tab would still be enrolled in the service. Furthermore, the FTC found the method of disabling Buzz once a user had been enrolled was complicated, and many users were unable to opt-out of the service once they had been enrolled. In addition to the FTC Act, Google had violated its own privacy policy to consumers; users were told that their information would only be stored and used to improve their Gmail experience and that if it were to be used for any other purposes, Google would ask for their consent.[69] Since many users were automatically enrolled in Buzz, there was no express consent for many users. Since Buzz went beyond the scope of an electronic mail and messaging service because others could see a user's information, Google was ultimately forced to modify its privacy policy and take steps to ensure that users had greater awareness and control over what information would be shared and how it would be used, or else they would face fines.[70]

As a result of the FTC's actions, Google's current privacy policy is now divided into two parts: information that the user provides and information that Google gets through the use of their services. For example, giving identifying information to create a profile that allows a user to utilize Google's services such as name, phone number, credit card number, or photograph would fall under the former category. Information covered by the latter would include search terms a user inputs into Google's search engine, or location if a user is using a Google application on a mobile device.

This use of a middleman diminishes an individual's expectation of privacy. Google is not an ISP, but it does provide an internet-based service. The distinction is significant because

[68] Id.
[69] Id.
[70] Ratté, Kathryn. United States of America. Federal Trade Commission. In the Matter of Google Inc., a corporation. Web. (2011).

Google does not provide access to the Internet, but rather provide services to users who already have an internet connection. For example, if an individual uses Comcast as the service provider and Google Chrome as their web-browser, both Comcast and Google have access to the information a user posts and their online activities, as well as any cookies that might have been saved.

Returning to Google's privacy policy, it is stated that "Google does not rent, sell or share information that personally identifies you for marketing purposes without your express permission.[71] No email content or other personally identifiable information is provided to advertisers." This raises an important concept-- express permission. It should be noted that users must agree to these policies in order to use Google's services, so it is crucial that a user understands how Google uses the information it collects.

Google outlines how the information it collects from users, such as IP address, location, and search queries is used. They use the information they collect from their services to "provide, maintain, protect and improve them, to develop new ones, and to protect Google and its users" and use this information to personalize the content a user sees.[72]

Furthermore, they reserve the right to use the name a user provides for their Google Profile for other services that require an account. They may show a user's publicly visible information, such as their name and photo if other users already have their email or other identifying information.

[71] Google Privacy Policy
[72] Id.

Their policy also outlines how they use information collected from cookies and other technologies. As it states, for example, "by saving [a user's] language preferences, [Google's] services appear in the language [they] prefer." [73] They also consolidate information from their services to maximize a user's interactivity with other users of their services. Google's policy also assures users that "[Google] will [obtain a user's] consent before using information for a purpose other than those that are set out in this Privacy Policy."[74]

It is important that users have discretion over what information is shared with companies such as Google through methods such as personalizing their profiles to not include sensitive information and disabling their browser from storing cookies. Furthermore, user accounts are password-protected.

**B. Facebook**

Facebook is probably the most popular social media tool that people use on a regular basis, and perhaps the easiest to understand in terms of data. Since, like Google Plus, users create a personalized profile for themselves, some of the basic information collected about a user is submitted expressly by the user themselves when creating their profile and agreeing to the terms of service.

Facebook also has a privacy policy that controls how a user's information is obtained and can be shared. Like Google, users of Facebook voluntarily submit personal information, but may not always be aware of how the services use it. A user's birthday, for example, "allows

[73] Id.
[74] Id.

[Facebook] to do things like show you age-appropriate content and advertisements."[75] This practice is a relatively new phenomenon, but one that brings about complicates issues and implications. With such a vast array of information about their users, Facebook is able to personalize the advertisements a user sees based on things like their location and common activities.

Because it is accessible from mobile devices such as cell phones, Facebook "[receives] data from the computer, mobile phone or other device [used] to access Facebook, including when multiple users log in from the same device. This may include [an] IP address and other information about things like [a user's] internet service, location, the type (including identifiers) of browser [one uses], or the pages [a user visits]."[76] As the policy outlines, the GPS information is sometimes used to let a user know if their "friends" are near them.

Users are able to post pictures and videos from their mobile devices to Facebook, which is one of the most popular features, but some may not be aware that they are also giving Facebook "additional related data […] such as the time, date, and place [the user] took the photo or video."[77] For example, if a user takes a photograph in a park on their mobile phone, Facebook will not only have that photograph, but also the location of the park as well as which of the user's "friends" are in the area.

Though no current legislation exists to address this issue, Senator Al Franken of Minnesota introduced a bill that has yet to pass called the "Location Privacy Protection Act of 2012," which would require non-governmental entities such as Facebook or an advertiser to

[75] Facebook Privacy Policy
[76] Id.
[77] Id.

expressly tell a user if the user's GPS location is being tracked by the device or application and how the information will be used.[78] The bill is still in committee.

Though these data-collecting practices might seem unethical, they are clearly outlined in the data policy, which states "[sometimes Facebook gets] data from…affiliates or…advertising partners, customers and other third parties that helps…deliver ads, understand online activity, and generally make Facebook better." Advertisers, for example may provide Facebook information about users, such as a summary of the advertisements they click, "in order to measure the effectiveness of - and improve the quality of – ads."[79]

An important distinction to make about this information as opposed to the Government's access to electronic communications is that these are voluntary services, even if a user is not familiar with the terms they agreed to in order to make the account. So, for example, information people might want to hide from a law enforcement officer, such as daily activities and locations, is often voluntarily disclosed through Facebook and other social media. Even though users have a diminished expectation of privacy for information on the Internet, users must be careful about what they post. Though a user can customize their security settings to limit who can see what they post, there are drawbacks to having anybody able to access this information if a user wishes to keep it private.

Using the content and non-content letter analogy, a Facebook post that is made available for others to see has no expectation of privacy. Even if a user has very strict privacy settings, anybody who has access to the user's profile and posts can legally send the information to a law

[78] S. 1223--112th Congress: Location Privacy Protection Act of 2012." www.GovTrack.us. 2011. <http://www.govtrack.us/congress/bills/112/s1223>
[79] Id. at Facebook

enforcement agency just as they would be able to make a copy of a physical letter that they received in the mail. Once a letter is sent, or a post is made on Facebook, a reasonable expectation of privacy all but vanishes.

It is possible for a user to delete their Facebook account, but that takes approximately one month. Once an account is deleted, the information may appear in Facebook's backup copies and logs for an additional ninety days, but that is limited to the information that a user expressly provides, such as name and demographic information. Other content, such as posts a user made in a group or message sent to one of their "friends" through Facebook, will not be deleted because the other party or parties who were given access to this communication will still have access to the communications.

**C. Ownership of Content**

The thesis has outlined the distinction between content and non-content information, but it is unclear if they retain ownership of that content once it is shared on the Internet If, for example, a user uploads a photograph using a service such as Facebook, that service may retain the right to that content.

Facebook's data use policy refers to information that a user posts as "public," which a reasonable person could construe to imply a forfeiture of ownership. An educated guess as to how far an individual can retain ownership to the content would depend on who has access to it. If a photograph taken with a cell phone is sent directly to a user's computer and is never posted on the Internet, there can be a reasonable expectation of privacy. If a user posts a picture to Facebook for others to see, that expectation would be diminished. It is not being used for

commercial purposes, and any other Facebook user with access to the content is able to download the photograph and post it elsewhere. Furthermore, Facebook has an option called "share," which allows users to re-post somebody else's content, although the original poster is given credit. This language does not explicitly state where the ownership of content ends, and Courts must address the boundaries.

# V. CONCLUSION

Considering that there is so much information about individuals on the Internet, it is interesting that people tend to have a double standard about privacy when the service provided is for their own convenience. With cell phones and other mobile devices that have Internet access, users are more than willing to allow private companies to track their location, but there are statutory protections that stop the Government from doing that. If, for example, a law enforcement agency were to ask a user for an individual's name, address, demographic information, and photographs, the average person would be uncomfortable complying unless they had a legal obligation to do so. When Facebook asks for this information, on the other hand, users are willing to post their personal information for the world to see.

It is too early in the social media age to tell exactly why this is, but an educated guess would be that GPS and social media services provide an automatic convenience to individuals, whereas many people have a fundamental mistrust of Government. Since many younger individuals are used to this technology and feel comfortable divulging so much information, it is appropriate to consider disclosing personal information from the angle of a reasonable expectation of distribution rather than privacy. It is interesting to note that people are willing to give their information to private entities, but hesitant to give it to the Government, which has much greater restrictions than social media platforms. It is also too early to tell if the fact that so much information about us is productive or destructive to society. Communication and commerce are certainly more open than ever before, but there is a growing concern that people are getting too detached from reality by having so much focus on their digital presence. Employers and schools look at people's social media presence when making decisions of who to

hire or admit, so people need to be cognizant of the fact that information they post can potentially stay on the Internet forever, and that once somebody else has access to the content they post, their expectation of privacy is severely diminished, if not destroyed.

Courts thus far have addressed the issue of privacy to a degree, but there are still concepts, such as ownership of digital content, that must be addressed in greater detail and codified. Simply put, the greatest digital expectation of privacy exists when an individual saves a file on a physical hard drive or disk and puts a password on it, just as somebody would put an important physical document in a locked drawer or cabinet. If that individual then e-mails that file to a friend or colleague, they have a reasonable expectation of privacy as to the content of the e-mail until it is received, but their Internet Service Provider and web browser have access to the identifying information of all the parties, because they are the means by which digital content is sent. Furthermore, once the receiving party has access to the content, the sender's expectation of privacy is gone. The recipient is able to redistribute the information as the recipient sees fit, unless some sort of legal duty of confidentiality applies. The Government can obtain search warrants from ISPs to find identifying information, and ISPs can sometimes divulge customers' information to the Government.

Outside of our expectation of privacy from Government intrusion, individuals have a lot of discretion in terms of the information they post. All social media and mobile technology is completely voluntary. Though people are concerned about the amount of information about them that is available online, they are generally the ones to provide that information in the first place. The issue at the heart of this phenomenon is essentially a question of how much we as a society are willing to sacrifice privacy in exchange for convenience. Being able to bring up

directions through a GPS in one's phone is an incredibly convenient technological breakthrough, but it may not worth the cost of allowing oneself to be monitored at all times. It is too early to answer that question, but it is still perfectly reasonable to expect courts and legislatures to address these issues as they arise and continue to follow them. The Internet is very dynamic by nature, and traditional precedent may not always apply, and the legal community as a whole must stay vigilant in following legal developments to assist their clients, constitutions, and fellow citizens.

# REFERENCES


1. 92 A.L.R. 5th 15 (2001)
2. 18 U.S.C. § 2510 (2006 & Supp. 2012).
3. 18 U.S.C. § 2515 (2006 & Supp. 2012).
4. 18 U.S.C. § 2518 (2006 & Supp. 2012).
5. 18 U.S.C. § 2701 (2006 & Supp. 2012).
6. 18 U.S.C. § 2702 (2006 & Supp. 2012).
7. 18 U.S.C. § 2703 (2006 & Supp. 2012).
8. *ACHTE/NEUNTE BOLL KINO BETEILIGUNGS GMBH & Co. v. DOES*. 736 F. Supp. 2d 212 (Ct. 2010).
9. "Cookie." Merriam-Webster. (2011).
10. Facebook Data Use Policy.
11. *First Time Videos, LLC v. Does 1-500*. 276 F.R.D. 241 (2011).
12. Google Privacy Policy.
13. Hokenson, Katherine, MY TEACHER SUX! [CENSORED]: PROTECTING STUDENTS' RIGHT TO FREE SPEECH ON THE INTERNET. 28 J.Marshall J. Computer & Info. L. 385 (2011).
14. *Katz v. United States*, 389 U.S. 347 (1967).
15. Kerr, Orin. *Applying the Fourth Amendment to the Internet: A General Approach*. 62 Stan. L. Rev. 1005. (2010).

16. Leibowitz , Jon, William Kovacic, J. Thomas Rosch, Edith Ramirez, and Julie Brill. United States of America. Federal Trade Commission. *In the Matter of Google Inc., a corporation*. Web. (2011).

17. *Miller v. California.* 413 U.S. 15. (1973).

18. *New York Times v. Sullivan*. 376 U.S. 254 (1964).

19. *O'Connor v. Ortega*. 480 U.S. 709 (1987).

20. *Ontario v. Quon*. 130 S.Ct. 2619 (2010).

21. Ratté, Kathryn. United States of America. Federal Trade Commission. *In the Matter of Google Inc., a corporation*. Web. (2011).

22. *Reno v. American Civil Liberties Union*. 521 U.S. 844. (1997).

23. S. 1223--112th Congress: Location Privacy Protection Act of 2012." www.GovTrack.us. 2011. March 28, 2013 <http://www.govtrack.us/congress/bills/112/s1223>

24. Schweber, Nate. "Rutgers Student Saw Twitter Posts by Roommate About Spying." *New York Times*. (2012): n. page. Web. 25 Mar. 2013. <http://www.nytimes.com/2012/03/07/nyregion/tyler-clementi-monitored-dharun-ravis-twitter-posts-about-him.html?ref=nyregion&_r=1&>.

25. *Talley v. California*. 362 U.S. 60 (1960).

26. *Tinker v. Des Moines Independent Community School Dist*. 393 U.S. 503 (1969).

27. *U.S. v. Maxwell*. 45 M.J. 406 U.S. Armed Forces (1996).

28. *U.S. v. Warshak*. 631 F.3d 266 (2011).

29. *White v. White*. 344 N.J. Super. 211. 781 A.2d 85 (2001).

*30. Wisniewski v. Board of Educ. of Weedsport Cent. School Dist.*494 F.3d 34 (2d Cir. 2007).