The path towards clear and convincing digital privacy rights

Frederick V. Greene
Purdue University

Follow this and additional works at: http://docs.lib.purdue.edu/open_access_dissertations

Part of the Intellectual Property Law Commons, and the Organizational Behavior and Theory Commons

Recommended Citation
Greene, Frederick V., "The path towards clear and convincing digital privacy rights" (2016). Open Access Dissertations. 765.
http://docs.lib.purdue.edu/open_access_dissertations/765

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.
This is to certify that the thesis/dissertation prepared

By Frederick V. Green

Entitled
The Path Towards Clear and Convincing Digital Privacy Rights

For the degree of Doctor of Philosophy

Is approved by the final examining committee:

Linda L. Naimi
Chair
Michael Harris
Jon Padfield
James L. Mohler

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University’s “Policy of Integrity in Research” and the use of copyright material.

Approved by Major Professor(s): Linda Naimi

Approved by: Kathryn Newton 7/19/2016
Head of the Departmental Graduate Program Date
THE PATH TOWARDS CLEAR AND CONVINCING DIGITAL PRIVACY RIGHTS

A Dissertation
Submitted to the Faculty
of
Purdue University
by
Frederick V. Greene

In Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy

August 2016
Purdue University
West Lafayette, Indiana
To my daughters, Brittany, Tiffany, Melody, and Chelsey, for their love and support. Remember Matthew 19:26 when “Jesus looked at them and said, ‘With man this is impossible, but with God all things are possible.’” To my mom, Mrs. Estella Greene for her continuous love, support, guidance and insistence on educational excellence. To Dr. Linda Naimi for her excellence, steadfastness, and continued support. In memory of my deceased father, Dr. Alfonzo Greene, for his lifelong belief in the importance of education. Above all, to God for giving me the strength to complete this project.
ACKNOWLEDGMENTS

I would like to thank Dr. Linda Naimi for her dedicated support and direction. Dr. Naimi has to rank amongst the top nationally in her quality leadership as an advisor, as well as her exceptional breadth and depth of knowledge in most areas of inquiry. To the other members of my committee who have guided me in this endeavor, including Dr. Michael T. Harris, Dr. James Mohler, and Dr. Jon Padfield. In special memory of Professor Bruce A. Harding and in memory of my mentor and friend Dr. Joseph Warren. To my siblings Dr. Alfonzo Greene, Jr., Dr. Anthony Greene and Crystal Greene Thomas, and Dr. Leon Thomas for believing I could accomplish this project and continuous encouragement, and prayer. To my many students over the years that have inspired me to continue down the road of academia. And to my Heavenly Father for demonstrating repeatedly that “…we know that in all things God works for the good of those who love him, who have been called according to his purpose.” Romans 8:28 (NIV).
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF TABLES</td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>viii</td>
</tr>
<tr>
<td>GLOSSARY</td>
<td>ix</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>xii</td>
</tr>
<tr>
<td>CHAPTER 1. INTRODUCTION</td>
<td></td>
</tr>
<tr>
<td>1.1 Statement Of The Problem</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Research Questions</td>
<td>2</td>
</tr>
<tr>
<td>1.3 Significance Of The Problem</td>
<td>2</td>
</tr>
<tr>
<td>1.4 Statement Of The Purpose</td>
<td>4</td>
</tr>
<tr>
<td>1.5 Assumptions</td>
<td>6</td>
</tr>
<tr>
<td>1.6 Limitations</td>
<td>6</td>
</tr>
<tr>
<td>1.7 Delimitations</td>
<td>7</td>
</tr>
<tr>
<td>1.8 Summary</td>
<td>8</td>
</tr>
<tr>
<td>CHAPTER 2. LITERATURE REVIEW</td>
<td></td>
</tr>
<tr>
<td>2.1 The Fourth Amendment</td>
<td>9</td>
</tr>
<tr>
<td>2.2 A Right To Privacy</td>
<td>11</td>
</tr>
<tr>
<td>2.3 Electronic Surveillance</td>
<td>13</td>
</tr>
<tr>
<td>2.4 The Wiretap Act And The Super Warrant</td>
<td>15</td>
</tr>
<tr>
<td>2.5 In The Case Of Email</td>
<td>17</td>
</tr>
<tr>
<td>2.6 The Push For Reform</td>
<td>19</td>
</tr>
<tr>
<td>2.7 In The Case Of The Iphone</td>
<td>19</td>
</tr>
<tr>
<td>2.8 Electronic Communications Privacy Act Of 1986</td>
<td>21</td>
</tr>
</tbody>
</table>
LIST OF REFERENCES ........................................................................................................... 108
VITA .................................................................................................................................... 114
LIST OF TABLES

Table 4.3 United States Circuit Court of Appeals Judicial ECPA Decisions ............... 36
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Distribution of ECPA Cases by Level of Impact</td>
<td>46</td>
</tr>
<tr>
<td>4.2</td>
<td>ECPA Cases by Federal Appellate Circuit and Level of Impact</td>
<td>46</td>
</tr>
<tr>
<td>4.3</td>
<td>ECPA Cases by Circuit Court that Expand or Limit Digital Privacy Rights</td>
<td>47</td>
</tr>
<tr>
<td>4.4</td>
<td>The Proportion of Cases that Expand or Limit Digital Privacy Right</td>
<td>48</td>
</tr>
<tr>
<td>4.5</td>
<td>ECPA Cases by Approximate Region and Percentage of Impact</td>
<td>49</td>
</tr>
</tbody>
</table>
GLOSSARY

Cellular Phone or Cellphone—A portable telephone that uses wireless cellular technology to send and receive phone signals. (dictionary.reference.com)

Cloud Computing—Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (nist.gov/groups/SNS/cloud-computing/)

Electronic Communication—means 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…(Electronic Communications Privacy Act of 1986, 18 USC 119).

Electronic Communications System—means any wire, radio, electromagnetic, photooptical or photo electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. (Electronic Communications Privacy Act of 1986, 18 USC 119).

Email—the system for using computers to send messages over the internet. (dictionary.cambridge.org)
GPS—Global Positioning System: a navigational system involving satellites and computers that can determine the latitude and longitude of a receiver on Earth by computing the time difference for signals from different satellites to reach the receiver (wordnetweb.princeton.edu).

Internet—The internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces manages by the Internet Corporation for Assigned Names and Numbers (ICANN). (nist.gov/publications)

Internet Protocol (IP)—Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. (nist.gov/publications)

Oral Communication—means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication (Electronic Communications Privacy Act of 1986, 18 USC 119).
Wire Communication—means any aural transfer made in whole or in part through the use of facilities for the transmission of communication by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications for communications affecting interstate or foreign commerce and such term includes any electronic storage of such communications. (Electronic Communications Privacy Act of 1986, 18 USC 119).

Wireless Technology—Technology that permits the transfer of information between separated points without physical connection. (nist.gov/publications)
ABSTRACT

Greene, Frederick V., J.D., Ph.D., Purdue University, August 2016. The Path Toward Clear and Convincing Digital Privacy Rights. Major Professor: Dr. Linda Naimi, J.D., Ed.D..

This study was a legal based inquiry to determine to what extend digital privacy rights are adequately protected by existing law. Because the major statutory vehicle that guides privacy rights in America was passed in 1986, the courts have had to address issues not contemplated by the statute. This study reviews the rulings of all twelve United States Courts of Appeal to determine whether or not digital privacy rights are expanded or limited. Comparisons are made between various circuits and different regions of the country. Three questions are addressed in this study, summarized as; a question about the current status of digital privacy laws; a question about the impact of court decisions on digital privacy rights; and a question and assessment about the adequacy of digital privacy laws. Also, recommendations are suggested for how digital privacy rights can be enhanced in the future. These recommendations would first change the standard needed to issue warrants and to access an individuals’ digital privacy rights to a “clear and convincing” analysis and standard. Secondly, the author recommends that digital privacy rights should become analogous to intellectual property rights and should have the same level of protection afforded intellectual property rights. Although digital privacy is not yet firmly recognized as more akin to Intellectual Property deserving of heightened protection, this study recommends that digital privacy, along with trade secret, copyright and patents, and trademark law should all be considered a type of intellectual capital that needs to be protected from those not authorized to access or utilize that intellectual property.
CHAPTER 1. INTRODUCTION

1.1 Statement of the Problem

The world has progressed to the point that, digital and electronic communications have evolved exponentially since the passage of the Electronic Communications Privacy Act of 1986. In 1986, the internet was in its infancy. Although, email existed it 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, totally unlike today where the average 12-year old caries a Smartphone. Social Networking had an entirely different meaning related to personal in-person relationships—clearly not the internet phenomena known as social networking today, where individuals might stay in close touch with someone else a continent or two away. “Cloud computing” was two words not typically found in the same sentence. In the ensuing years since 1986, digital communications have exploded. It is quite 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. Incursions have intruded from government entities to corporate entities and other members of the private sector.

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. 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.

1.2 Research Questions

The questions guiding this research are:

1. What is the current status of digital privacy laws in the United States?

2. How have judicial decisions affected the digital privacy rights of citizens since 1986?

3. Do current laws adequately protect the digital privacy rights of citizens?

1.3 Significance of the Problem

The world has changed significantly in the past twenty plus years. In that short timeframe electronic communications have blossomed in a multitude of ways. Twenty 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. Twenty-five years ago, Congress passed the Electronic Communications Privacy Act of 1986. This statute has only been revised in a few minor ways since its passage. 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 digital privacy rights should be weighed, analyzed and protected. Many decisions from various courts contradict decisions from other courts. Although the courts have used a Fourth Amendment framework to analyze digital privacy rights, the question remains as to how best those rights can be protected. 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. This study attempts to create a roadmap to showing the various conclusions that different courts have reached regarding the same constitutional rights, and providing an analysis of the impact these decisions have on the body of law affecting these new technologies.

This study was originally conceived to provide an accurate assessment of the inconsistencies and contradictions present in the case made rule of law regarding the impact of these new technologies on digital and electronic privacy rights. After a thorough assessment on the present state of affairs it became clear that while the original questions needed to be addressed, the ultimate direction of the dissertation needed to change. A pattern emerged that clearly shows the relevant choices various courts have made in applying constitutional principles to electronic and digital issues before the
Digital and electronic communications have become the paramount and ubiquitous manner of communication worldwide. The importance and significance of digital communications presents an entirely new challenge that could not have been envisioned in past eras – the issue of digital privacy rights. The need for serious digital privacy rights protection 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 communications. 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 study, recognizing the tenor of the times, evolved to present a theoretical analysis and frank assessment of the current state of affairs and future needs. To that extent, this research is transformative in its outlook, assessment, and prognosis. The changes recommended represent a complete paradigm shift in how the issue should be handled.

1.4 Statement of the Purpose

One general purpose of this research was 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 protective 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, the answer to the research question may still be –no, 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 the answer still indicates that the law has lagged behind the advancements in communications technology leaving electronic communication rights and associated data security rights vulnerable and unprotected. To answer the question in the affirmative, that is that digital and electronic privacy rights are adequately protected under the law would require an affirmative showing that nothing new has developed or happened since 1986 that requires that digital privacy deserves greater protection then in the past.

This research, although not initially designed to do anything other than to explore the research questions at hand, evolved into a recommendation for a complete paradigm shift in the area of digital and electronic privacy rights. After assessing the current status of digital communication and the relative importance of the privacy needs in this greatly enhanced area of communication, the facts cried out for a robust solution. This research presents a number of paradigmatic shifts in how we view electronic and digital
communications and the value we should place on the process for protecting that communications and the digital privacy rights associated with our communication.

1.5 Assumptions

The following assumptions were inherent to the pursuit of this study:

1. This study assumes that articulable factors exist in all cases evaluated that will allow the researcher to show the various results courts have reached in their judicial decisions.

2. Individual and collective rights of privacy can be articulated in a manner that fairly represents the right sought to be protected in court proceedings.

3. Courts make decisions based on a reasonably finite set of factors or variables that can be accurately determined in a discreet manner.

4. An evaluation can meaningfully express the results of the court holdings and court decisions.

5. The results of an evaluation study can and should provide relevant and appropriate information that allows reasonable inferences to be made relative to a theoretical framework explaining these decisions.

1.6 Limitations

The following limitations were inherent to the pursuit of this study:
1. The study was limited to relevant federal cases that cite the Electronic Communications Privacy Act (ECPA) in its entirety and makes no assumptions about state cases or decisions, nor citations to laws or statutes that are subsets of the ECPA.

2. The study was limited to that portion of cases that involve or implicate “digital privacy rights,” or “electronic privacy rights” as those terms are understood, and that cases that cite the act but fail to implicate digital privacy rights in any way will be eliminated from the study as irrelevant.

3. The study was limited to actual cases filed and does not address disputes involving the right of privacy that may have been settled out of court prior to filing.

1.7 Delimitations

The following delimitations were inherent to the pursuit of this study:

1. This study does not purport to answer every question or to analyze every factor relative to the privacy decisions.

2. This study only analyzes the factors articulated in the study.

3. Published opinions of the United States Court of Appeals were the only cases considered.
1.8 Summary

This chapter provided an overview of the problem, purpose, and significance of the research. It presented research questions and discussed the underlying assumptions, limitations, and delimitations of the study.
CHAPTER 2. LITERATURE REVIEW

2.1 The Fourth Amendment

The Fourth Amendment to the United States Constitution states that “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized” (US Constitution, Fourth Amendment).

The purview of what it means to be “secure” has been the subject of numerous court cases. Almost every word in the Fourth Amendment has been the subject of some form of litigation over the past 200 years. One of those words that have been litigated is the word “warrant.” It is important to understand what the Fourth Amendment was designed to protect. According to Taylor, 2001, the “chief evil that the Fourth Amendment was intended to address was the issuance of warrants that were inappropriately general in nature. To that end, the proscription of ‘unreasonable searches and seizures’ was a reference to illegally general warrants, and not an independent standard governing searches and seizures” (Taylor, 2001, p.9).
The US Supreme Court has weighed in on the issue as to the sufficiency of a warrant authorizing law enforcement to seize items from a person’s home. In Stanford v. Texas, The US Supreme Court (1965) stated:

We need not decide in the present case whether the description of the things to be seized would have been too generalized to pass constitutional muster, had the things been weapons, narcotics, or cases of whiskey. . . . The point is that it was not any contraband of that kind which was ordered to be seized, but literary material – “books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments concerning the Communist Party of Texas, and the operations of the Communist Party in Texas.” The indiscriminate sweep of that language is constitutionally intolerable. To hold otherwise would be false to the terms of the Fourth Amendment, false to its meaning, and false to its history (Taylor, 2001, p. 10, quoting Stanford v. Texas, 379 US 476).

The Supreme Court went on in later cases to find that “reasonable expectations of privacy” provides the standard whereby it can be judged whether or not a person can be free from a warrantless search. The court discusses this idea in the case of Smith v. Maryland in which the court indicates that:

Situations can be imagined, of course, in which Katz's two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation or privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this
Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been “conditioned” by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a “legitimate expectation of privacy” existed in such cases, a normative inquiry would be proper (Smith v. Maryland, 442 US 735 [1979] as quoted by Taylor, 2001, p. 12).

2.2 A Right to Privacy

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. 7; 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).

2.3 Electronic Surveillance

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, purpose, 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).

2.4 The Wiretap Act and the Super Warrant

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 various provisions of this act are succinctly summarized by Mulligan, 2004:

First, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”), creating a statutory right of privacy in oral and wire communications, predated the advent of electronic communications. Written in 1968, the statute was directed at the “aural acquisition” of voice communications that passed, at least in part, over a wire. The wiretap provisions of Title III authorized law enforcement wiretapping of telephones within a framework designed to protect privacy and compensate for the uniquely intrusive aspects of electronic surveillance. Title III requires law enforcement to obtain what has been referred to as a “superwarrant” before intercepting phone conversations. While instinctually individuals using e-mail may have expected protections against interception to extend to this new means of communicating, courts had found that a literal reading of the statute did not provide protection. Electronic mail and data are not “oral” communications, nor are they subject to “aural” acquisition. Any
prohibition on intercepting electronic communications would thus have to be based on the Fourth Amendment itself (Mulligan, 2004, p. 1561).

Notwithstanding the prohibition of warrantless searches by law enforcement, J. Edgar Hoover routinely ordered federal agents of the FBI to conduct these warrantless searches throughout his tenure at the FBI from 1924-1972 (Horn, 2002).

Later as more and more people became involved with electronic communication, the need for additional statutory protection was apparent to Congress. In 1986 Congress adopted the Electronic Communications Privacy Act (ECPA). Although adopted at a time when electronic communications was growing, this act still preceded the explosive growth of the internet. As McDonough (2007) points out, “The words ‘Internet’, ‘World Wide Web,’ and ‘e-commerce’ appear in neither the ECPA nor its legislative history.” In effect the ECPA amends the wiretap act and makes many of the earlier provisions applicable to electronic communications. The ECPA is divided into three different areas as explained by Mulligan, 2004:

[T]he Wiretap Act, 18 U.S.C. §§ 2511-2522; the Pen Register statute, 18 U.S.C. §§ 3121-3127; and the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2711. The Wiretap Act and Pen Register statute regulate prospective surveillance of Internet communications (communications “in transit”), and the SCA governs retrospective surveillance (stored communications). Each of the titles operate in the same basic way generally prohibiting unauthorized access to communications and other personal information, but permitting specified exemptions, one of which provides the government with the ability to obtain direct access or to compel a third party to turn over information (Mulligan, 2004, p. 1565).
2.5 In the Case of Email

Each of the provisions of the Wiretap Act, The Pen Register statute, and The Stored Communications Act (SCA) have different provisions for enforcement and interpretation. This has allowed for different levels of protection for electronic communications depending on where it is in the transmission chain. Emails, for example, are subject to different regulations depending on whether or not they have been sent, opened, unopened, viewed and/or stored (Albrecht, 2003). It is important to note that analogies about email are not based on express mention of the term “email” in the ECPA. In 1986 when the ECPA was adopted, email was in its infancy and not considered something in need of statutory protection in and of itself. Dombrow (1998) cites a 1995 Dunn and Bradstreet study that shows:

While e-mail in the workplace continues to grow, its use by businesses is not a new phenomenon. In a 1995 survey of 272 small to mid-size businesses, fifty-six percent reported use of e-mail within the company, forty-one percent exchanged e-mail with off site employees, twenty-three percent exchanged e-mail with suppliers, and eighteen percent exchanged e-mail with business advisors. These companies also reported thirty-eight percent as having regularly telecommuting employees. Already in 1995, eighty-seven percent of the Fortune 100 companies reported using e-mail for person to person messaging (Dombrow, 1998, p.695).

This 1995 study was conducted some nine years after the 1986 act (ECPA) was passed. At that time the vast majority of email usage was intra-company with only 23% of companies in the survey exchanging email with non-company entities. In 1986, email
was not on the radar screen of Congress. The word email is not even mentioned in the ECPA (Dombrow, 1998). Other technologies in use today had not for the most part been invented or discovered as the case may be. Peer to Peer communications, Cloud Computing, social networks, The World Wide Web, and most of what has become common in everyday usage did not exist at the time of the ECPA’s adoption. The ECPA does provide three different methods for obtaining communication under the act. These three methods are; 1. The warrant, 2. The Administrative Subpoena, and 3. The National Security Letter (NSL). The use of NSL’s grew tremendously after 9/11 and the enactment of the USA Patriot Act (McNerney, 2010).

Although the ECPA fails in many ways to protect the newer technologies, some courts have forged ahead with judicial protection. The U.S. Sixth Circuit Court of Appeals in Ohio decided a case that generally upheld the idea of privacy protection for email:

The United States Court of Appeals for the Sixth Circuit ultimately held that when a user does not expect a third party to access one's e-mail in the normal course of business, “the party maintains a reasonable expectation of privacy, and subpoenaing the entity with mere custody over the documents is insufficient to trump the Fourth Amendment warrant requirement.” On remand, the Court permitted the government to seize private e-mails in electronic storage under the following circumstances: (1) by obtaining a search warrant under the Fourth Amendment; (2) by providing notice to the account holder when seeking a court order; or (3) by showing specific, articulable facts, demonstrating that the ISP or other entity has complete access to the e-mails in the normal course of its
business, which demonstrates that the user has waived any expectation of privacy (Wright, 2007-2008, pp.548-549, citing Warshak v US).

2.6 The Push for Reform

Various courts have issued opinions all over the board when it comes to the privacy protections afforded electronic communications. The uncertainty has led many groups to advocate for reform of the law by Congress. One such group advocating reform is called Digital Due Process (DDP). DDP is a “broad coalition of technology and communications companies, trade associations, advocacy groups, and think tanks, as well as academics and individual lawyers” (Comments of Digital Due Process, 2010). The coalition generally advocates that the warrant requirement apply for electronic searches. The DDP has six guiding principles: “Technology and Platform Neutrality…Assurance of Law Enforcement Access…Equality Between Transit and Storage…Consistency…Simplicity and Clarity…Recognition of All Existing Exceptions” (Comments of Digital Due Process, 2010).

2.7 In the Case of the iPhone

Apple has fought a number of cases relative to the desire of the federal government to force it to create a backdoor to the Apple iPhone. Although there have been past cases where Apple has cooperated with the government, there appears to be a number of recent cases where Apple has drawn the line in the sand (Los Angeles Times).
One case in 2016, deals with the San Bernardino terrorist gunmen. These terrorists owned an Apple iPhone 5C. The Apple iPhone 5C has an encryption program that if a wrong password is entered into the phone ten successive times, all of the data on the phone will be destroyed. The FBI had attempted to break the password on nine occasions unsuccessfully (Retrieved from https://www.nbcnews.com/storyline/san-bernardino-shooting/Apple-FBI-face-Congressional-hearing-encryption-N528841). They were concerned that if they tried one more time, all of the data they were trying to retrieve would be destroyed (The Washington Post. Retrieved from https://www.washingtonpost.com/news/post-nation/wp/2016/02/17/apple-ceo-the-u-s-government-wants-something-we-consider-too-dangerous-to-create/?utm_term=.1f213d33c2bd).

The FBI obtained a search warrant and court order against Apple to force Apple Computer to write a program that would disable the ten wrong password security feature. Apple continually refused. Apple indicated that to create such a program would compromise the security of all Apple iPhones. Their argument was that once this program existed, not only would there be no limit as to when it would be used, but also, other hackers and those who do not have a purported right to the information would be in a better position to disable the same feature that Apple had designed into the iPhone. The legal issues before the judge were actually quite complex. Not only are privacy and other constitutional issues involved, but statutory interpretation was also involved. Most amazingly, the FBI was relying on The “All Writs Act of 1789.” This 200+ year old act
was all the government could find to make a clear case. Apple CEO, Tim Cook, has indicated that the United States government “wants something we considered too dangerous to create.” Apple CEO, Tim Cook goes on to indicate “we have great respect for the professionals at the FBI, and we believe their intentions are good.” Up to this point, we have done everything that is both within our power and within the law to help them. But now the US government has asked us for something we simply do not have and something we considered too dangerous to create. They have asked us to build a backdoor to the iPhone.”

In the past decade, it has become clear that privacy rights would become and have become one of the major concerns that most individuals should have regarding protecting their valuable personal information. A number of cases that have garnered publicity tells us how important privacy rights are to everyday Americans.

2.8 Electronic Communications Privacy Act of 1986

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 electronic 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 would 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 communications would be worldwide and instantaneous was more of a science fiction idea, than the reality that it has become. Some of the major flaws that Congress could not have foreseen came about, partly, because of the dramatic reduction in the cost of electronic storage.

Many of you like me, may remember when storage was extremely expensive. My first computer in 1984 was a Kaypro II. Because of the prohibitive cost of storage and hard drives, my first computer did not even have a hard drive. The way you saved information was from 5 ¼ floppy disks to 5 ¼ floppy disks. Kaypro had two floppy disk drives specifically so that you could save information from one to the other. I recall my first IBM PC with an MS-DOS operating system which I purchased sometime in 1987. This first “Windows-based system” had a 40 MB hard drive. I now carry in my pocket a smart phone with a 64 GB storage capacity (1600 times more storage capability). A law that was written in 1986 when storage was at a premium, necessarily focused on real-time surveillance. The law heavily prohibits access to real-time data but is quite weak in enforcing access for 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 protected at a high level that would assure an absolute level of confidence that other entities or individuals that had no right to the information would not be able to access that information.

2.9 Digital Due Process Coalition

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. 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, are all a part of this coalition. 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 (Retrieved from https://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. (Retrieved from http://digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163).

While these four major principles are certainly a step forward from the antiquated and nonexistent 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. To properly analyze this idea, we must go back to the United States Constitution and try to understand what exactly the fourth amendment was designed to protect. When the Bill of Rights was passed by Congress in 1794 and ratified in 1795, the ideas embodied in the fourth amendment had a particular meaning. The fourth amendment to the United States Constitution states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. …… (https://www.law.cornell.edu/constitution/fourth_amendment).

The Fourth Amendment was adopted to protect Americans from physical violations and physical incursions. The founding fathers obviously had no reason to think in terms of protection of electronic or digital privacy rights. Physical incursions are by nature, limited in scope and breadth. Limitations on manpower alone conceivably would limit the scope of a search or seizure. Certainly a massive army could execute a large scale search or seizure, but this necessitates tremendous resources and effort. Electronic communications, on the other hand, can be accessed with digital equipment that allows for the massive accumulation of all sorts of data and information, including sensitive digital privacy information.
2.10 The Case of Edward Snowden

Edward Snowden was a former Central intelligence agency employee and a former US government subcontractor who copied and intentionally leaked classified government information from the national security agency in 2013. After leaking this information, Edward Snowden was forced to flee the United States and to seek asylum in other countries. Ultimately, he ended up in Russia. Edward Snowden received help from a number of whistleblower organizations including the Government Accountability Project (GAP). GAP is a nonprofit organization that supports whistleblower activity, and is a nonprofit organization that has been around since 1977 (Retrieved from https://info.whistleblower.org).


The author takes no position as to the propriety or impropriety of Snowden’s actions. What is important for purposes of this dissertation is that we now know with certainty that the National Security Agency (NSA), as well as many other government agencies, are involved in a massive collection of private data, from not only citizens, and businesses, but also from various governments. We learned from the Edward Snowden
disclosures that this amassing of information is unbelievably large in breadth and depth. The question that arises, is to what extent should private data be protected from government surveillance? Should the government be able to amass any amount of information and intercept any communications that they wish to amass from US citizens and others?

The Edward Snowden case demonstrates that no one is outside of the reach of government data collection activities. The question before us today—is should the government be able to collect this massive information unencumbered? The vast majority of the information collected by the NSA is not collected pursuant to any sort of specific warrant for information. There appears to be an ongoing program of data collection not in any way tied to the need to obtain probable cause warrants. This massive collection of data is a clear violation of the privacy rights of millions of Americans. Many would argue that the government has to be able to collect this data to keep us safe. This is a false argument. Terrorism exists in totalitarian countries as well as free societies. Americans should not have to give up their privacy rights to remain safe.

2.11 Summary

This chapter explored the evolution of case law and legislation dealing with protection of personal information and rights to privacy in the digital age. Prior to the 1986 Electronic Communications Privacy Act (ECPA) there were numerous laws that protected some of the earlier communications devices like telephones, telegraph, and facsimile. The court always utilized the standard used in the Fourth Amendment to the
US Constitution of “Probable Cause” to determine the parameters of privacy rights and their protection from government intrusion. The world has changed rapidly since 1986. Because we now live in a digital environment, the idea of privacy has grown exponentially in significance. The 12-year old child at school needs protection from those that may attempt to do her harm by befriending her online first. The Snowden case, and data breaches at numerous retail establishments have made it transparently clear that many citizens, businesses and even the government needs robust protection of privacy rights.
CHAPTER 3. METHODOLOGY

This analytical study investigated the question as to whether or not the United States’ laws adequately protect digital and electronic communications privacy rights. This inquiry is by nature a legal inquiry. Legal inquiries are quite different than most types of inquiries in technology, science and/or the social sciences. Legal inquiries have typically focused on case results from the courts in a sequential manner, when the researcher is evaluating cases that may have established precedent on a particular topic. Each case is dissected based on the particular fact pattern, and an analysis is conducted as to how the court ruled and why. Legal researchers have also used various other research methods including the analysis of statutes, laws and ordinances. This study by nature is a qualitative study that attempts to shed light and information on the laws as they exist, namely the ECPA, and what has been done to adapt or change, limit or expand the impact of these laws to address the factually specific contingencies that could not have been foreseen at the time of passage.

3.1 Legal Inquiries

There are a number of methodologies for conceptualizing how legal research is presented. One of the most famous methodologies for analyzing a court opinion is called
“IRAC.” IRAC is an acronym for “Issue, Rule, Analysis, and Conclusion.” This approach calls for each case to be analyzed separately, and for the conclusions to be compared with other cases. By reviewing cases on a case-by-case basis, clear descriptions emerge as to what each particular case may attempt to accomplish within the context of the fact pattern presented by the parties.

This type of research is clearly qualitative in nature. The present study utilized a qualitative framework but with a slightly different focus than most types of legal research. The method envisioned has been termed “Evaluation Studies” (Leeuw, 2011). Evaluation studies are a type of qualitative study that attempts to take a broader view of the cases that have been decided. It attempts to succeed at “applying different theories, methodologies, and (research) designs” (Leeuw, 2011). The general goal is to evaluate the criteria, rules and factors that played a role in the court decision. Many courts reach their decision based upon factors that are clearly identifiable and quite similar to factors present in many other cases. Would a broad view of these cases help to shed light on general factors that are constant in their effect on the outcome?

3.2 Research Design

The specific method used in this study was to evaluate the relevant number or portion of the Federal cases that cite the “Electronic Communications Privacy Act” (ECPA) since the act’s passage in 1986. Although only two of these decisions are United States Supreme Court decisions, the remainder are reported by various Courts of Appeals. A total of 199 cases have been adjudicated by the fourteen United States Courts of
Appeal. Although the focus is on the ECPA and how those decisions that were made pursuant to the ECPA affected the outcome of the case, other factors were also explored. Additionally, the ideas that digital privacy must always remain limited by the prevailing legal theories are challenged. Many other legal theories have been advanced to protect privacy rights. Some theories generally allude to intellectual property theories, while other theories look at privacy as a “Public Good.” Relevant theories are evaluated and analyzed.

A number of questions can be answered by such a study. To what extent has a prevailing legal ideology developed that is largely fact dependent? The study will be a cross between a “qualitative analysis,” and a “grounded theory study.” That is to say that the study will take a broad perspective of important relevant decisions relating to the ECPA and privacy in general and not over-analyze the ruling or conclusion reached by the court. This study attempted to answer some broad questions related to the first general research question: “Does the United States adequately protect Digital Privacy Rights?” The remaining two questions presented are also analyzed.

3.3 Process and Procedures

This study was conducted utilizing relevant cases and statutes. The legal research service “Westlaw” (https://www.westlaw.com) was used to find cases that matched the subject matter of cases dealing with the Electronic Communications Privacy Act (ECPA). Two cases were from the United States Supreme Court. These two cases are dealt with separately and not included in Chart 4.1. Cases were limited to the cases at the federal
appellate level to assure that these cases were not mere anomalies or “one offs,” but truly represented common law precedent in the federal courts with stare decisis impact.

Westlaw is one of two major commercial legal research platforms in the United States. The other legal research source is LexisNexis (https://www.lexisnexis.com). Westlaw gives the researcher the assurance that every published case in any court in the United States can be searched and found. After a number of efforts to isolate the relevant cases for analysis, it was determined that two search terms provided the level of reliability needed in identifying the cases.

The relevant search terms involved finding cases that used the four letter acronym “ECPA” as well as expanding that search to cases where the parties and the court never used the acronym but always referred to the statute by its formal name of the “Electronic Communications Privacy Act.” A Boolean search term was constructed to search the entire database of United States Courts of Appeal cases. The Boolean search term that worked the best was; electronic /s communication /s privacy /s act. This search term identified every case that had those four terms in a single sentence or line. After identifying the 199 cases from the various US Courts of Appeal, the cases were studied to determine what impact, if any, the case would have on ECPA precedent and digital privacy. Three categories were created to compile results into a meaningful and cohesive matrix for further analysis. The three categories are:

Expands Digital Privacy Rights

Limits Digital Privacy Rights

Does Not Impact on Digital Privacy rights
Because the study was focused on whether or not judicial decisions have helped to either expand or limit electronic or digital privacy rights, those cases constituted the major focus. Cases that were analyzed to have “Expand[ed] Digital Privacy Rights” became the cases to evaluate where and how the courts had interpreted the ECPA in a manner to further digital privacy rights. The converse is true with cases that limited digital privacy rights. In addition to the question regarding the present state of the ECPA, this research endeavored to study the history and efficacy of intellectual property rights as they may either impact or inform privacy rights. In reviewing the cases and laws, majority, concurring and dissenting opinions of the judges were considered. If the cases dealt with either the violation of digital privacy rights or intellectual property regarding patents and copyrights, they were considered and analyzed.

The cases were also analyzed that dealt with privacy rights that were protected to see if particular rulings involved either violations of privacy rights, or possibly legislation to correct or change those privacy rights issues that arose. Since 1986, no comprehensive legislation has been adopted to deal with privacy rights in the digital age. The results of what was determined from studying the 199 cases follows in a later section. It is fair to state now that there is a patchwork quilt of laws that have failed to protect private citizens and their rapidly emerging digital rights.
3.4 Summary

This chapter discussed methodology used in this study. This research was conducted as a legal inquiry into past and present laws dealing with privacy rights in the digital, electronic, and communications arenas. Cases involving violations of privacy rights were examined and the efforts were made to identify patterns in the judgments of judges as case law around digital privacy rights evolved.
CHAPTER 4. PRESENTATION OF THE DATA

4.1 Analysis of Case Law

The data in this study represented a legal inquiry into legal cases that had a direct bearing on the issue of privacy rights, as protected and expanded in the 1986 Electronic Communications Privacy Act. Each of the 199 cases were qualitatively evaluated to determine what rights were involved and how these rights were affected. In many cases it was quite clear that the person or persons asserting privacy rights prevailed. These cases were all grouped together in the category of “Expands Digital Privacy Rights.” In other cases, the person or persons that asserted privacy rights were defeated or limited in the result the court implemented. These cases were all identified with the designator of “Limits Digital Privacy Rights.” Some cases involved rulings that ultimately were decided on other grounds or were decided in such a way as to not affect any digital privacy rights. Although the subject matters were different in the varied cases, they were all able to be reduced to one of the three categories above. Because of the qualitative nature of this study, no quantitative analyses of the data were indicated.

Although the study focused on cases citing the ECPA, it is important to note hat the earliest instance of where privacy rights were discussed was in 1890 in the Harvard Law Review (Harvard Law Review, 4, 5, 1890). Since then, the U.S. courts have recognized the right to privacy, in various forms. This study, of course, focuses on digital privacy rights and how laws, particularly the ECPA has affected digital privacy rights.
4.2 Relevant Legislation

The advent of the microcomputer and the rapid growth of the internet swamped any effort to properly regulate this technology. The failure of Congress and state legislatures to properly keep up with this rapid growth resulted in the courts’, by necessity, addressing these issues. The courts, restrained by precedent and stare decisis, have been unable to keep up with this massive growth in technology, particularly in a systematic and comprehensive manner. This has resulted in incongruity, depending on which jurisdiction you may reside in, or which federal circuit where you may reside.

4.3 A Comparison of Relevant Cases

After evaluating the 199 cases, a chart was developed to easily ascertain the effect each case has on digital privacy rights. An examination of the cases revealed 31 of the 199 demonstrating some expansion of digital privacy rights. 73 cases showed little or no impact on digital privacy rights. But the majority of the cases, 95 to be specific, revealed limitations and curtailments of digital privacy rights. The factors that were considered to determine whether or not a case was classified as (E) Expansion of Digital Privacy Rights, (L) Limitation of Digital Privacy Rights, or (D) Does not impact Digital Privacy Rights are as follows:

a. Did the party that was asserting a digital privacy right prevail in protecting that right or was that right not protected?
b. Did the party that was opposed to the asserted digital privacy right successfully achieve their goals in contravention of the asserted digital privacy right.

c. Did the court decide the case on grounds that were unrelated to the asserted digital privacy right?

d. Did the case involve factors that did not involve a digital privacy right, but was related to some of the criminal provisions of the ECPA, resulting in no impact on any ascertainable digital privacy rights?

e. Does the case represent a situation that general privacy rights are implicated and affected, although the impact in the instant case may be tenuous?

f. Considering all of the factors in a-e above, can it fairly be said that by a preponderance of evidence the privacy rights were either expanded, limited, or not affected?

Table 4.3 presents the 199 cases according to whether the judicial decision limited, expanded or had no impact on digital privacy rights. The table lists each case, identifying the year and the court from which the decision was rendered and the citation where it can be found, along with the level of impact on digital privacy rights.
Table 4.3
United States Circuit Court of Appeals Judicial ECPA Decisions

<table>
<thead>
<tr>
<th>Case Name</th>
<th>Year</th>
<th>Citation</th>
<th>Appeals Court</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>In re Nickelodeon Consumer Privacy Litigation</td>
<td>2016</td>
<td>---F.3d----</td>
<td>Third Circuit</td>
<td>L</td>
</tr>
<tr>
<td>United States v. Graham</td>
<td>2016</td>
<td>--- F.3d ----</td>
<td>Fourth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Scurry</td>
<td>2016</td>
<td>821 F.3d 1</td>
<td>District of Columbia Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Jane Doe No. 1 v. Backpage.com, LLC</td>
<td>2016</td>
<td>817 F.3d 12</td>
<td>First Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Vista Marketing, LLC v. Burkett</td>
<td>2016</td>
<td>812 F.3d 954</td>
<td>Eleventh Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Jewel v. National Sec. Agency</td>
<td>2015</td>
<td>810 F.3d 622</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>In re Google Inc. Cookie Placement Consumer Privacy Litigation</td>
<td>2015</td>
<td>806 F.3d 125</td>
<td>Third Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Long v. Insight Communications of Cent. Ohio, LLC.</td>
<td>2015</td>
<td>804 F.3d 791</td>
<td>Sixth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Daniels</td>
<td>2015</td>
<td>803 F.3d 335</td>
<td>Seventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>United States v. Christensen</td>
<td>2015</td>
<td>801 F.3d 970</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Graham</td>
<td>2015</td>
<td>796 F.3d 332</td>
<td>Fourth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Anzaldua v. Northeast Ambulance and Fire Protection Dist.</td>
<td>2015</td>
<td>793 F.3d 822</td>
<td>Eighth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>American Civil Liberties Union v. Clapper</td>
<td>2015</td>
<td>785 F.3d 787</td>
<td>Second Circuit</td>
<td>E</td>
</tr>
<tr>
<td>U.S. v. Davis</td>
<td>2015</td>
<td>758 F.3d 498</td>
<td>Eleventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Byrd v. Aaron’s Inc.</td>
<td>2015</td>
<td>784 F.3d 154</td>
<td>Third Circuit</td>
<td>D</td>
</tr>
</tbody>
</table>
Table 4.3 Continued

United States Circuit Court of Appeals Judicial ECPA Decisions

<table>
<thead>
<tr>
<th>Case Name</th>
<th>Year</th>
<th>Citation</th>
<th>Appeals Court</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>In re Zynga Privacy Litigation</td>
<td>2014</td>
<td>750 F.3d 1098</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Telecommunications Regulatory Board of Puerto Rico v. CTIA-Wireless Ass’n</td>
<td>2014</td>
<td>752 F.3d 60</td>
<td>First Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Electronic Frontier Foundation v. U.S. Dept. of Justice</td>
<td>2014</td>
<td>739 F.3d 1</td>
<td>District of Columbia Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Joffe v. Google, Inc.</td>
<td>2013</td>
<td>746 F.3d 920</td>
<td>Ninth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Joffe v. Google, Inc.</td>
<td>2013</td>
<td>729 F.3d 1262</td>
<td>Ninth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>In re U.S. Historical Cell Site Data</td>
<td>2013</td>
<td>724 F.3d 600</td>
<td>Fifth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Mortensen v. Bresnan Communications, LLC.</td>
<td>2013</td>
<td>722 F.3d 1151</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Seitz v. City of Elgin</td>
<td>2013</td>
<td>719 F.3d 654</td>
<td>Seventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Sams v. Yahoo! Inc.</td>
<td>2013</td>
<td>713 F.3d 1175</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Barajas</td>
<td>2013</td>
<td>710 F.3d 1102</td>
<td>Tenth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Lane v. Facebook, Inc.</td>
<td>2013</td>
<td>709 F.3d 791</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>In re U.S. for an Order Pursuant to 18 U.S.C. Section 2703(D)</td>
<td>2013</td>
<td>707 F.3d 283</td>
<td>Fourth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Kirch v. Embarq Management Co.</td>
<td>2012</td>
<td>702 F.3d 1245</td>
<td>Tenth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Garcia v. City of Laredo, Tex.</td>
<td>2012</td>
<td>702 F.3d 788</td>
<td>Fifth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Lane v. Facebook, Inc.</td>
<td>2012</td>
<td>696 F.3d 811</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Schnabel v. Trilegiant Corp.</td>
<td>2012</td>
<td>967 F.3d 110</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Electronic Privacy Information Center v. National Sec. Agency</td>
<td>2012</td>
<td>678 F.3d 926</td>
<td>District of Columbia Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Case Name</td>
<td>Year</td>
<td>Citation</td>
<td>Appeals Court</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>In re National Sec. Agency Telecommunications Records Litigation</td>
<td>2011</td>
<td>671 F.3d 881</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Nachshin v. AOL, LLC</td>
<td>2011</td>
<td>663 F.3d 1034</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Suzion Energy Ltd. V. Microsoft Corp.</td>
<td>2011</td>
<td>671 F.3d 726</td>
<td>Ninth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>American Civil Liberties Union v. U.S. Dept. of Justice</td>
<td>2011</td>
<td>655 F.3d 1</td>
<td>District of Columbia Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Bowden v. Kirkland &amp; Ellis LLP</td>
<td>2011</td>
<td>432 Fed.Appx. 596</td>
<td>Seventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Clenney</td>
<td>2011</td>
<td>631 F.3d 658</td>
<td>Fourth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Warshak</td>
<td>2010</td>
<td>631 F.3d 266</td>
<td>Sixth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Szymuszkiewicz</td>
<td>2010</td>
<td>622 F.3d 701</td>
<td>Seventh Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Beaven v. U.S. Dept. of Justice</td>
<td>2010</td>
<td>622 F.3d 540</td>
<td>Sixth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government</td>
<td>2010</td>
<td>620 F.3d 304</td>
<td>Third Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Bott v. Vistaprint USA Inc.</td>
<td>2010</td>
<td>392 Fed.Appx. 327</td>
<td>Fifth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Shlahtichman v. 1-800 Contacts, Inc.</td>
<td>2010</td>
<td>615 F.3d 794</td>
<td>Seventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Amanuel</td>
<td>2010</td>
<td>615 F.3d 117</td>
<td>Second Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Mink v. Knox</td>
<td>2010</td>
<td>613 F.3d 995</td>
<td>Tenth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Case Name</td>
<td>Year</td>
<td>Citation</td>
<td>Appeals Court</td>
<td>Result</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>------</td>
<td>--------------------------</td>
<td>------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>U.S. v. Navas</td>
<td>2010</td>
<td>597 F.3d 492</td>
<td>Second Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Walden v. City of Providence, R.I.</td>
<td>2010</td>
<td>596 F.3d 38</td>
<td>First Circuit</td>
<td>L</td>
</tr>
<tr>
<td>School Dist. Of City of Pontiac v. Secretary of U.S. Dept. of Educ.</td>
<td>2009</td>
<td>584 F.3d 253</td>
<td>Sixth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Noel v. Hall</td>
<td>2009</td>
<td>568 F.3d 743</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Van Alstyne v. Electronic Scriptorium, Ltd.</td>
<td>2009</td>
<td>560 F.3d 199</td>
<td>Fourth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Doe 1 v. AOL LLC</td>
<td>2009</td>
<td>552 F.3d 1077</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>DirectTV, Inc. v. Webb</td>
<td>2008</td>
<td>545 F.3d 837</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Warshak v. U.S.</td>
<td>2008</td>
<td>532 F.3d 521</td>
<td>Sixth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Harrell</td>
<td>2008</td>
<td>530 F.3d 1051</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Quon v. Arch Wireless Operating Co., Inc.</td>
<td>2008</td>
<td>529 F.3d 892</td>
<td>Ninth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>DIRECTTV, Inc. v. Rawlins</td>
<td>2008</td>
<td>523 F.3d 318</td>
<td>Fourth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Fair Housing Council of San Fernando Valley v. Roommates.com, LLC</td>
<td>2008</td>
<td>521 F.3d 1157</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Perrine</td>
<td>2008</td>
<td>518 F.3d 1196</td>
<td>Tenth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>DIRECTV, Inc. v. Seijas</td>
<td>2007</td>
<td>508 F.3d 123</td>
<td>Third Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Motorola Credit Corp. v. Uzan</td>
<td>2007</td>
<td>509 F.3d 74</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>DIRECTTV, Inc. v. Hoa Huynh</td>
<td>2007</td>
<td>503 F.3d 847</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Case Name</td>
<td>Year</td>
<td>Citation</td>
<td>Appeals Court</td>
<td>Result</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------</td>
<td>------------------------</td>
<td>------------------</td>
<td>--------</td>
</tr>
<tr>
<td>DirectTV v. Crespin</td>
<td>2007</td>
<td>224 Fed.Appx. 741</td>
<td>Tenth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Universal Communication Systems, Inc. v. Lycos, Inc.</td>
<td>2007</td>
<td>478 F.3d 413</td>
<td>First Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Comprehensive Drug Testing, Inc.</td>
<td>2006</td>
<td>473 F.3d 915</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Williams v. City of Tulsa, Okla.</td>
<td>2006</td>
<td>204 Fed.Appx. 762</td>
<td>Tenth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Abdi</td>
<td>2006</td>
<td>463 F.3d 547</td>
<td>Sixth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Freeman v. DirectTV, Inc.</td>
<td>2006</td>
<td>457 F.3d 1001</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>McCready v. eBay, Inc.</td>
<td>2006</td>
<td>453 F.3d 882</td>
<td>Seventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Almeida v. Amazon.com, Inc.</td>
<td>2006</td>
<td>456 F.3d 1316</td>
<td>Eleventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Moore</td>
<td>2006</td>
<td>452 F.3d 382</td>
<td>Fifth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Snow v. DirectTV, Inc.</td>
<td>2006</td>
<td>450 F.3d 1314</td>
<td>Eleventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Doe v. Gonzales</td>
<td>2006</td>
<td>449 F.3d 415</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Weindorf v. Netscape Communications Corp.</td>
<td>2006</td>
<td>173 Fed.Appx. 44</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>DirectTV, Inc. v. Pepe</td>
<td>2005</td>
<td>431 F.3d 162</td>
<td>Third Circuit</td>
<td>E</td>
</tr>
<tr>
<td>U. S. v. Councilman</td>
<td>2005</td>
<td>418 F.3d 67</td>
<td>First Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Kehoe v. Fidelity Federal Bank &amp; Trust</td>
<td>2005</td>
<td>421 F.3d 1209</td>
<td>Eleventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>DirectV, Inc. v. Nicholas</td>
<td>2005</td>
<td>403 F.3d 223</td>
<td>Fourth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Ameritech Corp. v. McCann</td>
<td>2005</td>
<td>403 F.3d 908</td>
<td>Seventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Hall v. EarthLink Network, Inc.</td>
<td>2005</td>
<td>396 F.3d 500</td>
<td>Second Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Motorola Credit Corp. v. Uzan</td>
<td>2004</td>
<td>388 F.3d 39</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Councilman</td>
<td>2004</td>
<td>373 F.3d 197</td>
<td>First Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Case Name</td>
<td>Year</td>
<td>Citation</td>
<td>Appeals Court</td>
<td>Result</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------</td>
<td>---------------------</td>
<td>-----------------</td>
<td>--------</td>
</tr>
<tr>
<td>DirectTV, Inc. v. Treworgy</td>
<td>2004</td>
<td>373 F.3d 1124</td>
<td>Eleventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>DIRECTV, Inc. v. Brown</td>
<td>2004</td>
<td>371 F.3d 814</td>
<td>Eleventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>In re U.S. for an Order Authorizing Roving Interception of Oral Communications</td>
<td>2003</td>
<td>349 F.3d 1132</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Clemons v. Waller</td>
<td>2003</td>
<td>82 Fed.Appx. 436</td>
<td>Sixth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Doe v. GTE Corp.</td>
<td>2003</td>
<td>347 F.3d 655</td>
<td>Seventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Theofel v. Farey-Jones</td>
<td>2003</td>
<td>359 F.3d 1066</td>
<td>Ninth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>U.S. v. Corona-Chavez</td>
<td>2003</td>
<td>328 F.3d 974</td>
<td>Eighth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>In re Pharmatrak, Inc.</td>
<td>2003</td>
<td>329 F.3d 9</td>
<td>First Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Quigley v. Rosenthal</td>
<td>2003</td>
<td>327 F.3d 1044</td>
<td>Tenth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Motorola Credit Corp. v. Uzan</td>
<td>2003</td>
<td>322 F.3d 130</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U. S. v. Steiger</td>
<td>2003</td>
<td>318 F.3d 1039</td>
<td>Eleventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Sparshott v. Feld Entertainment, Inc.</td>
<td>2002</td>
<td>311 F.3d 425</td>
<td>District of Columbia Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Bach</td>
<td>2002</td>
<td>310 F.3d 1063</td>
<td>Eighth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. McGuire</td>
<td>2002</td>
<td>307 F.3d 1192</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Specht v. Netscape Communications Corp.</td>
<td>2002</td>
<td>306 F.3d 17</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Doe v. Chao</td>
<td>2002</td>
<td>306 F.3d 170</td>
<td>Fourth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Konop v. Hawaiian Airlines, Inc.</td>
<td>2002</td>
<td>302 F.3d 868</td>
<td>Ninth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Ameritech Corp. v. McCann</td>
<td>2002</td>
<td>297 F.3d 582</td>
<td>Seventh Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Case Name</td>
<td>Year</td>
<td>Citation</td>
<td>Appeals Court</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------</td>
<td>----------------------</td>
<td>-------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Price v. Turner</td>
<td>2001</td>
<td>260 F.3d 1144</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Ramirez-Garcia</td>
<td>2001</td>
<td>269 F.3d 945</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Guest v. Leis</td>
<td>2001</td>
<td>255 F.3d 325</td>
<td>Sixth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Adams v. City of Battle Creek</td>
<td>2001</td>
<td>250 F.3d 980</td>
<td>Sixth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Smoot v. United Transp. Union</td>
<td>2001</td>
<td>246 F.3d 633</td>
<td>Sixth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Kee v. City of Rowlett, Tex.</td>
<td>2001</td>
<td>247 F.3d 206</td>
<td>Fifth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Konop v. Hawaiian Airlines, Inc.</td>
<td>2001</td>
<td>236 F.3d 1035</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Marbly v. Kay</td>
<td>2000</td>
<td>238 F.3d 422</td>
<td>Sixth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Coronado v. Bank Atlantic Bancorp, Inc.</td>
<td>2000</td>
<td>222 F.3d 1315</td>
<td>Eleventh Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Hambrick</td>
<td>2000</td>
<td>225 F.3d 656</td>
<td>Fourth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. Telecom Ass’n v. F.C.C</td>
<td>2000</td>
<td>227 F.3d 450</td>
<td>District of Columbia Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Peavy v. WFAA-TV, Inc.</td>
<td>2000</td>
<td>221 F.3d 158</td>
<td>Fifth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>U.S. v. Jackson</td>
<td>2000</td>
<td>213 F.3d 1269</td>
<td>Tenth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Tapley v. Collins</td>
<td>2000</td>
<td>211 F.3d 1210</td>
<td>Eleventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Barnhart v. Federal Express Corp.</td>
<td>2000</td>
<td>210 F.3d 371</td>
<td>Sixth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Bartnicki v. Vopper</td>
<td>1999</td>
<td>200 F.3d 109</td>
<td>Third Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Boehner v. McDermott</td>
<td>1999</td>
<td>191 F.3d 463</td>
<td>District of Columbia Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Blake v. Wright</td>
<td>1999</td>
<td>179 F.3d 1003</td>
<td>Sixth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Desilets v. Wal-Mart Stores, Inc.</td>
<td>1999</td>
<td>171 F.3d 711</td>
<td>First Circuit</td>
<td>E</td>
</tr>
<tr>
<td>Basch v. America Online, Inc.</td>
<td>1999</td>
<td>172 F.3d 52</td>
<td>Seventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Condon v. Reno</td>
<td>1998</td>
<td>155 F.3d 453</td>
<td>Fourth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Case Name</td>
<td>Year</td>
<td>Citation</td>
<td>Appeals Court</td>
<td>Result</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>U.S. v. Biro</td>
<td>1998</td>
<td>143 F.3d 1421</td>
<td>Eleventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Ruskin</td>
<td>1998</td>
<td>145 F.3d 360</td>
<td>Fifth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Crooks v. William</td>
<td>1997</td>
<td>121 F.3d 697</td>
<td>Fourth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Organizacion Jd Ltda. V. U.S. Dept. of Justice</td>
<td>1997</td>
<td>124 F.3d 354</td>
<td>Second Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Pervaz</td>
<td>1997</td>
<td>118 F.3d 1</td>
<td>First Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Davis v. Gracey</td>
<td>1997</td>
<td>111 F.3d 1472</td>
<td>Tenth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Meharg v. Poznick</td>
<td>1997</td>
<td>111 F.3d 129</td>
<td>Fourth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Thompson v. Johnson County Community College</td>
<td>1997</td>
<td>108 F.3d 1388</td>
<td>Tenth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>U.S. v. Mathis</td>
<td>1996</td>
<td>96 F.3d 1577</td>
<td>Eleventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Reynolds v. Spears</td>
<td>1996</td>
<td>93 F.3d 428</td>
<td>Eighth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>U.S. v. Ford</td>
<td>1996</td>
<td>88 F.3d 1350</td>
<td>Fourth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Tucker v. Waddell</td>
<td>1996</td>
<td>83 F.3d 688</td>
<td>Fourth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Murdock</td>
<td>1995</td>
<td>63 F.3d 1391</td>
<td>Sixth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>McKamey v. Roach</td>
<td>1995</td>
<td>55 F.3d 1236</td>
<td>Sixth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Crawford</td>
<td>1995</td>
<td>52 F.3d 1303</td>
<td>Fifth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>In re Askin</td>
<td>1995</td>
<td>47 F.3d 100</td>
<td>Fourth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Bennett v. Tidwell</td>
<td>1995</td>
<td>46 F.3d 1138</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Steve Jackson Games, Inc. v. U.S. Secret Service</td>
<td>1994</td>
<td>36 F.3d 457</td>
<td>Fifth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Bailey</td>
<td>1994</td>
<td>41 F.3d 413</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Falls</td>
<td>1994</td>
<td>34 F.3d 674</td>
<td>Eighth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Cablevision of Michigan, Inc. v. Sports Palace, Inc.</td>
<td>1994</td>
<td>27 F.3d 566</td>
<td>Sixth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Vastola</td>
<td>1994</td>
<td>25 F.3d 164</td>
<td>Third Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Williams</td>
<td>1994</td>
<td>23 F.3d 629</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Forsyth v. Barr</td>
<td>1994</td>
<td>19 F.3d 1527</td>
<td>Fifth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Organizacion JD Ltda. V. U.S. Dept. of Justice</td>
<td>1994</td>
<td>18 F.3d 91</td>
<td>Second Circuit</td>
<td>L</td>
</tr>
</tbody>
</table>
Table 4.3 Continued  
*United States Circuit Court of Appeals Judicial ECPA Decisions*

<table>
<thead>
<tr>
<th>Case Name</th>
<th>Year</th>
<th>Citation</th>
<th>Appeals Court</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>In re U.S.</td>
<td>1993</td>
<td>10 F.3d 931</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Daccarett</td>
<td>1993</td>
<td>6 F.3d 37</td>
<td>Second Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Blanco</td>
<td>1993</td>
<td>998 F.2d 1112</td>
<td>Second Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Herring</td>
<td>1993</td>
<td>993 F.2d 784</td>
<td>Eleventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Aguilar</td>
<td>1993</td>
<td>994 F.2d 609</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Townsend</td>
<td>1993</td>
<td>987 F.2d 927</td>
<td>Second Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. One Macom Video Cipher II, SN A6J0073</td>
<td>1993</td>
<td>985 F.2d 258</td>
<td>Sixth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Foster</td>
<td>1993</td>
<td>985 F.2d 466</td>
<td>Ninth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Diaz-Lizaraza</td>
<td>1993</td>
<td>981 F.2d 1216</td>
<td>Eleventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Splain</td>
<td>1992</td>
<td>982 F.2d 414</td>
<td>Tenth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Shriver</td>
<td>1992</td>
<td>989 F.2d 898</td>
<td>Seventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Smith</td>
<td>1992</td>
<td>978 F.2d 171</td>
<td>Fifth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Davis</td>
<td>1992</td>
<td>978 F.2d 415</td>
<td>Eighth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Petti</td>
<td>1992</td>
<td>973 F.2d 1441</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Koyomejian</td>
<td>1992</td>
<td>970 F.2d 536</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U. S. v. Lande</td>
<td>1992</td>
<td>968 F.2d 907</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>U.S. v. Koyomejian</td>
<td>1991</td>
<td>946 F.2d 1450</td>
<td>Ninth Circuit</td>
<td>L</td>
</tr>
<tr>
<td>Heggy v. Heggy</td>
<td>1991</td>
<td>944 F.2d 1537</td>
<td>Tenth Circuit</td>
<td>E</td>
</tr>
<tr>
<td>U.S. v. Hux</td>
<td>1991</td>
<td>940 F.2d 314</td>
<td>Eighth Circuit</td>
<td>D</td>
</tr>
<tr>
<td>U.S. v. Herring</td>
<td>1991</td>
<td>933 F.2d 932</td>
<td>Eleventh Circuit</td>
<td>D</td>
</tr>
<tr>
<td>Shubert v. Metrophone, Inc.</td>
<td>1990</td>
<td>898 F.2d 401</td>
<td>Third Circuit</td>
<td>L</td>
</tr>
</tbody>
</table>
In Figure 4.1, the cases are presented graphically according to the level of impact. As the figure illustrates, nearly 48% of judicial decisions in the United States Courts of Appeal resulted in a limitation of digital privacy rights. Approximately 16% of cases actually led to an expansion of digital privacy rights. And finally, about 37% of cases had little or no impact on individual digital privacy rights.
Judicial decisions within the U.S. Courts of Appeal can vary widely. As Figure 4.2 illustrates, the twelve Circuit Courts of Appeal arrive at decisions independently. The graph demonstrates the extent to which each Circuit Court decided to expand or limit digital privacy rights.

*Figure 4.1 Distribution of ECPA Cases by Level of Impact*

*Figure 4.2 ECPA Cases by Federal Appellate Circuit and Level of Impact*
When examining judicial cases before the Circuit Courts of Appeal, it became clear that although a case involved the ECPA, the judicial decisions were often made on other legal grounds that resulted in no impact on digital privacy rights. In the next few figures those (no impact) cases were ignored. For those cases that did have an impact, Figure 4.3 shows the comparison between cases that limited digital privacy rights versus cases that expanded such rights.

![Comparison of impact for ECPA Cases by Circuit](image)

*Figure 4.3 ECPA Cases by Circuit Court that Expand or Limit Digital Privacy Rights*

Considering the cases that had an impact, 63% or 126 of the original 199 relevant cases showed positive or negative impact. As the pie chart in Figure 4.4 shows, only 24.6% of cases expanded digital privacy rights while 75.4% limited digital privacy rights. Although we can see some differences, the overall result of limiting privacy rights was observed. A later study could explore the possible reasons for these differences.
Figure 4.4 The Proportion of Cases that Expand or Limit Digital Privacy Rights

There are twelve United States Courts of Appeal. In some cases, these Circuits do not follow exact parameters for regions of the country. In grouping them by region and level of impact, a picture can be drawn that helps us to visualize the differences in how the courts are deciding digital privacy cases. Figure 4.5 depicts cases that expanded or limited digital privacy rights by region. As the figure shows, 85% of these cases in the Southern region limited digital privacy rights, while only 15% expanded rights. For Midwestern Courts of Appeal, 78% of cases limited digital privacy rights while 22% expanded such rights. Approximately 75% of Eastern Courts of Appeal limited digital privacy rights while 25% expanded these rights. And for those Courts of Appeal identified as lying in the Western region, about 70% of cases resulted in limiting digital privacy rights while 30% expanded such rights.
For purposes of designation into approximate region, the courts were divided in the following manner:

South = Fifth and Eleventh Circuits.

Midwest = Sixth, Seventh, and Eighth Circuits.

West = Ninth and Tenth Circuits.

East = First, Second, Third, Fourth, and DC Circuits.

4.4 In the Matter of Probable Cause and the Right to Privacy

The history of privacy rights in America are inextricably tied to the history of fourth amendment probable cause law. Because privacy is a judicially made philosophy, found in the penumbras of various amendments to the Constitution, its implementation
has been tied to the history and development of constitutional law as it relates to the various amendments. The fourth amendment prohibiting unreasonable searches and seizures has been the primary vehicle to test and ascertain the boundaries of how privacy laws is enforced.

Probable cause has a troubled history. As early as 1949, the Supreme Court of the United States was grappling with the idea of what it means for probable cause to be necessary for warrants to issue. Of historical importance, is the idea that probable cause is considered by the court to be the relevant standard for both parts of the fourth amendment. The fourth amendment states in the first part that “the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated...” (Retrieved from https://www.law.cornell.edu/wex/fourth_amendment).

This right to be secure in our persons, houses, papers and effects is a right that protects against intrusions by government officials into our private lives without some sort of reasonableness. The court has usee the idea of probable cause to supply that reasonableness.

The same probable cause and reasonableness is pulled from the second half of the amendment. The amendment goes on to state that “... And no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” (Retrieved from http://constitution.findlaw.com/amendment4.html).

The court has consistently ruled that probable cause is a standard for the entire amendment and that the security referenced in the first part of the amendment is protected
by the same probable cause that exists in the second part of the amendment. There are numerous Law Review articles and legal scholars that have taken exception with that approach. For purposes of this study, we do not need to analyze those theories. It is sufficient to understand that although there are criticisms of the instability of probable cause doctrine, that instability is based upon what the court should have actually ruled, and the limitations they have imposed.

The real crux of the issue as it relates to privacy rights, is that the fourth amendment was never when adopted contemplated to address electronic and digital information, and the Fourth Amendment could not have possibly been drafted in a manner to protect those important rights. Nevertheless, and amazingly, the concept and doctrine of probable cause has been consistently unstable over the years. The instability in Fourth Amendment rulings have resulted in instability in the concept of privacy.

In early Supreme Court cases like the Brennegan case in 1949, the United States Supreme Court saw the need to make sure that probable cause was a serious standard that protected citizens from not only unlawful arrests but also from unreasonable seizures. Two cases in the 1960s solidified that approach. The first case was Aguilar v Texas decided in 1964 (Aguilar v. Tex., 378 U.S. 108 U.S., 1964). This case implemented what became known as the two-pronged test. The second case was known as Spinelli v United States (393 U.S. 410, 89 S. CT. 584, 21 L. ED. 2D 637 (1969), this case solidified and upheld the idea of a two-pronged test. The two-pronged test is described as follows:

(1) the affidavit for search warrant must set forth underlying circumstances necessary to enable the magistrate independently to judge validity of informants conclusion and (2) affiant- officers must support their claim that their informant was
credible or his information reliable.” (Retrieved from http://definitions.uslegal.com/a/aguilar-spinelli-test/).

This two-pronged test was an important part of American jurisprudence for nearly 20 years. It was a clear and rigid test that assured that false information was not used to obtain warrants. It also assured that magistrates and judges were conscientious in ascertaining the veracity of the information that was presented to them to support affidavits for warrants.

By 1983, the U. S. Supreme Court had become far more conservative, under the leadership of Justice William Rehnquist. Fourth amendment probable cause was redefined to limit a person’s expectations of privacy under the Fourth Amendment (Tomkovicv, 2013). A series of cases severely limited the ability of citizens to prevent warrantless searches. This new definition also changed what it meant to have probable cause, and what was necessary to obtain a probable cause warrant from a magistrate or judge. This is not the first sea-change in the Supreme Court’s jurisprudence relative to fourth amendment law. But this particular change has an interesting effect on privacy rights. In the case of Illinois v Gates (462 U.S. 213, 1983), the United States Supreme Court implemented a new test. They abandoned the two-pronged test under Aguilar and Spinelli, and implemented a quote “totality of the circumstances” test that did not have multiple parts. This new test also implemented two other doctrines that severely limited the protection of probable cause. One doctrine was the idea of the “four corners doctrine” (Pendergast, 1993)

This doctrine postulates that magistrates and judges that are hearing testimony in support of issuance of a warrant, only need to look within the four corners of the affidavit
to determine whether or not probable cause exists. This essentially meant that inquiries as to the veracity of the person submitting the affidavit no longer played a role in determining whether or not probable cause truly existed. In only looking within the four corners of the document a judge or magistrate may conclude that sufficient information has been provided for probable cause to exists, and a warrant should issue. Amazingly, the idea of the totality of circumstances is in many ways oxymoronic. What the court phrased as a “totality of circumstances” in reality was a severe limit on inquiry about circumstances. Magistrates and judges were no longer required to independently verify or inquire about the veracity of the officer presenting the affidavit, and the underlying veracity of the affiants themselves. It simply was enough that when they looked at the four corners of the document and read what was presented to them in the affidavit, that if they could conclude that under the “totality of the circumstances” the court could conclude that probable cause existed, then a warrant should issue.

This notion of probable cause became embedded in the court’s cases from that point forward. So much so that it is now considered precedential, and even the purported liberal wing of the court no longer vigorously attacks this idea. At the time it was decided, in a 5 to 4 decision, the four more liberal justices of the Supreme Court strenuously and vigorously objected to this reinterpretation of probable cause law. They believed that this new test, or lack of a test, would ultimately lead to the breakdown of Fourth Amendment protections that the Constitution was trying to support for American citizens. By the year 2013, the idea that probable cause no longer had a two-pronged test, but was simply a totality of the circumstances test, was well-established jurisprudence. In that year in Florida v. Harris, a decidedly liberal judge, Justice Elena Kagan wrote a
unanimous decision that upheld the idea that the totality of the circumstances test was a common sense standard of probable cause. One only needs to look back at the dissenting opinions that were filed in the US v Gates case to realize that probable cause had been irrevocably and demonstrably weakened.

More importantly to this discussion, is the general idea that electronic and digital privacy rights are not the same as fourth amendment rights protecting physical space. Electronic and digital privacy rights encompass part and parcel of an enhanced idea of privacy as it relates to Americans today. Privacy, or the right to be left alone, is one of the most important rights that allows individuals to function in a modern-day society.

Whether with computers; within our personal space; with tablets and cell phones; or on social media with the requisite relationships and connections, our privacy rights should protect almost all of our daily activities. Incursions by police into physical space as contemplated by the fourth amendment are by necessity limited in scope. Even in high police presence areas, the vast majority of citizens do not come in contact with the police or other government actors attempting to invade their space. When you look at the probable cause laws that developed around automobiles, houses, and other personal effects, you have to realize immediately that there aren’t enough police, investigators, and other government officials to compromise everyone’s fourth amendment rights.

On the other hand, if we start looking at electronic and digital rights, the technology exists presently to wreck-havoc on a persons’ life by violating their privacy. We now know that as shown by NSA surveillance, and private company security breaches, that everyday citizens’ rights could all be affected in a major, extensive and pervasive manner, without the need for the physical presence of police, other government
actors and/or private sector entities. Just the pure scope of the capability of government entities, and corporate entities, to infiltrate, compromise, and utilize personal information is astounding and mind-boggling.

This dissertation makes the case that probable cause has not been, nor ever will provide sufficient protection to protect Americans rights to digital privacy from incursions by government. Digital privacy incursions by other entities; including corporations and individuals, are likewise not protected by existing jurisprudential norms. Digital privacy deserves a much higher standard of care then ordinary privacy! The higher standard of Clear and Convincing Evidence, as discussed in the next chapter, will allow for the adequate protection of these important digital privacy rights.

4.5 The Doctrine of Clear and Convincing

Before clearly articulating the history of the law behind “clear and convincing evidence,” it is important to briefly look at a partial spectrum of levels of proof recognized in the American judicial system. While this is not a comprehensive review, it does take a look at the four most prevalent standards. There are other standards such as articulable suspicion, or rational basis test, to name a few, that are present in American jurisprudence. While acknowledging that these other standards exist, we focus on the four discussed here because they are necessary to understand where in the spectrum of legal analysis the concept of clear and convincing fits within the panoply of standards.
We have already mentioned probable cause. Of the four standards that we are briefly reviewing, “probable cause” is the most lenient, weakest, standard available. It simply means, in laymen’s terms that something is more likely than not likely. Another standard that is tougher, and the standard in use to determine whether or not a plaintiff wins in a civil case, is the standard of “preponderance of the evidence.” A preponderance of the evidence is simply the idea that when all of the evidence is weighted, one side has shown that the evidence is stronger on their side versus on the other side. Many people visualize this test as the test most analogous to the scales of justice. Using the scales of justice analogy, if the evidence on one side outweighs the evidence on the other side, by ever so slight a margin, then the weightier side wins.

The toughest test that we have, of the four that we are looking at, and actually one of the toughest tests of all, is the standard used in criminal cases. It is the well-known standard of “beyond a reasonable doubt.” The standard articulated in a test called “clear and convincing” falls between a “preponderance of the evidence” and beyond a reasonable doubt. It is certainly a higher standard than “probable cause” by a long shot. The history of the “clear and convincing” standard is not nearly as muddled and troubled as the probable cause standard. This “clear and convincing” standard is used in many areas of the law, most notably for our purposes in patent invalidity cases and patent conflicts (Microsoft v Limited partnership, 2011).

This case was decided by a unanimous Supreme Court and thereby leaves no doubt as to the parameters and meaning of the ruling. “Clear and convincing” is also described by the court as “clear and cogent.” The court indicated that there was a presumption of validity to a patent that has already been issued by the Copyright and
Patent Office, and that this presumption can only be rebutted with the “clear and convincing” evidence standard, (Microsoft v Limited partnership, 2011). Other cases also make it clear that the clear and convincing standard is well understood and rationally interpreted.
CHAPTER 5. FINDINGS, DISCUSSION AND CONCLUSION

The idea of privacy as a type of intellectual property is a novel concept at the intersection of two disciplines. This dissertation submitted to Purdue University Polytechnic Institute is part of the PhD in Technology program and the Technology Leadership and Innovation Department. As part of that degree process, the College of Technology (now Polytechnic Institute) in conjunction with the Graduate School, granted the author permission to complete one of his cognates necessary for his degree, in Intellectual Property at the McKinney School of Law of Indiana University at IUPUI. All of the information concerning Intellectual Property was a part of that effort where the author received an LL.M. degree in Intellectual Property Law. Because this entire section that discusses intellectual property law is contained within that thesis, multiple citations are eliminated. Excerpts from the unpublished thesis “Ascertaining a Coherent Theory for Differences in Criminal versus non-Criminal Treatment of Copyright Infringers versus Patent Law Infringers” are reproduced here in Chapter Five, and in other sections of this document, to complete the effort to merge the two disciplines into one cohesive whole, effectuating the dual nature of one of the cognates, intellectual property law, synergistically interacting with the subject of technology leadership and innovation. This joint effort represents the first publication of that work.
5.1 Findings

It is important to go back and look at the research questions that were asked and to look to the research to answer those questions.

1. What is the current status of digital privacy laws in the United States?

This question is best answered by demonstrating the stagnant nature of digital privacy laws. Because Congress has failed to enact any comprehensive updates of the Electronic Communications Privacy Act, the courts have had to deal with many cases of first impression without any statutory guidance. With twelve federal circuits and most cases being heard by three judge panels, a lot of variation in results occurs. Depending on which circuit you live in, your chances may differ as to which result or outcome you may receive. The lack of guidance at the United States Courts of Appeal level also manifests itself in the hundreds of decisions rendered by both the federal lower courts, as well as state courts in all fifty states. Digital privacy rights, like liberty, should not depend on what state you live in or by the luck of which judge you may have had assigned to your case.

2. How have judicial decisions affected the digital privacy rights of citizens since 1986?

There is no question that the ECPA in 1986 was a forward-looking act. The problem Congress faced in 1986 was that they did not have “tea leaves” or a crystal ball that they could use to foresee the future. They could not possibly have anticipated the explosion of
technological growth over the past 30 years. Because Congress has not acted in a comprehensive fashion since the ECPA, courts were left to “pick up the slack.” With numerous court decisions coming from the state and federal level, the anomalies are readily apparent. Some courts have routinely found in favor of the person attempting to assert their digital privacy rights. Other courts have routinely found a way to limit digital privacy rights. As the availability and presence of electronic devices have continued to grow exponentially, areas of the law that were not designed to address the complexities of a modern digital economy have had to be improvised. This improvisation has resulted in vastly different results.

3. Do current laws adequately protect the digital and electronic privacy rights of citizens?

No. Digital privacy rights are not well protected. This dissertation presents two paradigm shifts that would forever change the parameters of digital privacy protection. These new paradigms are:

   a. Clear and convincing as the standard needed to justify an incursion or violation of a person’s digital privacy rights.

   b. Digital privacy as intellectual property.

The idea that we have an entire body of law that exists to protect IP rights and even allows for criminal sanctions in the case of Copyright violations, is quite instructive as to the premium society places on protecting intangible property rights.

Digital privacy is a type of Intellectual Property(IP) that needs protection to the same extent as copyrights and patents. Our failure to recognize that digital privacy
deserves the same level of protection as historically recognized types of intellectual property shortchanges the importance of digital privacy rights.

This chapter focuses on five related concepts that play a role in how digital privacy rights are interrelated to intellectual property rights. The basic idea that the United States of America would protect intellectual property was an idea that originated in the first constitutional document. This chapter will accomplish a number of things: One, we will look at the historical basis as found in the Constitution for the protection of intellectual property; Two, we will look at the historical basis for the protection of intellectual property prior to the adoption of the Constitution as adopted by other societies prior to the founding of the United States; Three, we will look at an extremely early biblical example of what could be described as copyright and by extension privacy protection. The biblical example is certainly on the creative side. But it does suggest that the idea protecting images dates way before the historical analysis given by most scholars; Four, this analysis will trace the historical divide between copyright law and patent law; Five, a case will be made that digital privacy should be recognized as an intellectual property right. Recognizing digital privacy as an intellectual property right would enhance the legal protections and enhance the ability to collect damages for breaches. This chapter will look extensively at how the differences between Copyright law and Patent law came about. This analysis is important to the final argument, made extensively later, that no real difference should exist in how we as a society protect patent rights, copyright interests, and digital privacy rights. First, we look at the differences between Copyright and Patent laws. Both of these types of intellectual property, patent and copyright, emanate from within the exact same clause in the Constitution. At some
point we will see that they detoured on completely separate paths. The one path we will call the copyright path. This particular path ended up with dual enforcement mechanisms for copyright infringers. One method is civil enforcement of copyright violations. The other method is criminal enforcement of copyright violations. Obviously, when you are able to harness the power of the state (criminal enforcement) to protect individual property rights you have accomplished something worth noting. The other path we will call the patent path. The patent path does not generally have two types of enforcement. The patent path consists only of private or civil enforcement. After reviewing these anomalies, the subject of how these concepts may protect or enhance digital privacy rights will be explored. This subject area has been explored, to some extent, in two cases without particular success.

This analysis is extremely important to the discussion of privacy rights because privacy rights are impacted by multiple actors. On the one hand, you have government intrusion on individual and corporate digital privacy rights. On another hand, you have corporate and individual intrusions on digital privacy rights. Business speaks the language of money. Governments speak the language of power. Individuals speak the language of liberty. That is to say, that if you want to have an impact on a business or corporation, simply affect their bottom line in such a manner as to cause pain to the investors. Fines, judgments, and any other type of financial penalty ultimately will convince businesses to change their ways, or to abandon certain behaviors. This is clearly the idea behind punitive damages. It sends a signal to the tortfeasor as well as other potential tortfeasors that the financial costs of engaging in certain types of behavior are prohibitive.
The same does not apply for government, particularly the federal government. Governments by their nature have almost unlimited resources. Whatever resources they don’t have, they generally can raise by either increasing taxes, or local governments can raise money by floating bonds. Financial incentives have some impact, but not to the same extent that they impact businesses. Power is the language of government. Limited capability to do certain things, and you can expect to see certain results that are reflective of preventing the limitations. Governments want to go about doing what they want to do unencumbered. The last major player in effecting privacy rights are individuals. Individuals deal in the currency of liberty, and money. But to someone who does not have significant sums of money, no financial disincentive exists to prevent certain types of behavior. Criminal penalties on the other hand would be very effective. Relative recently, Congress implemented bills like Dodd-Frank that provides criminal penalties for corporate directors and officers. The same deterrent effect could impact corporations and other legal entities by impacting the officers and directors. The discussion regarding differences in how patent offenders and copyright offenders are treated relative to criminal and civil penalties is quite informative to the general need to enforce digital privacy rights with both civil and criminal options.

The question this research poses is simple but important. Why have we not as a society started to think of digital privacy rights as a type of intellectual property? The similarities are great. For example, trade secrets are for the exclusive purpose of protecting information that you do not want others to have. Not unlike digital privacy.
The two cases where privacy has been asserted as intellectual property reach some rather bizarre results, clearly demonstrating the need for Congress and society to rethink the relationship between intellectual property and digital privacy.

In Bollea v. Gawker Media, LLC., The plaintiff, Bollea, attempted to use copyright laws to protect his privacy in a video of him having sex with a woman that was not his wife. The court refused to allow Mr. Bollea to use what the court described as an invalid Copyright claim to prevent the distribution of this video. This raises question of how a valid copyright claim may be able to be used to protect digital privacy claims. The Bollea case also raises questions concerning the relatively new field related to the “Right of Publicity.” The right of publicity is another concept worth exploring as it relates to intellectual property and digital privacy rights, but that discussion is beyond the purview of this study and may be a ripe area for further study. A second case in the United States Circuit Court for the Ninth Circuit reached a similar result. In the case of Garcia v Google, the Plaintiff, Ms. Garcia attempted to block the distribution of an inflammatory anti-Islamic video that included footage of her that was shot for what she was told was a different video. She had no intention of appearing in an anti-Islamic video, and was misled to believe that the video she agreed to appear in would not be anti-Islamic. The court concluded that as a non-owner of the video, she had no proprietary recognizable interest in the video footage that would allow her to prevent its dissemination.

Once again though, the question remains open as to how an individual or individuals that actually have a valid digital privacy interest that could either be characterized similarly as a copyright or patent claim; a trade secret claim or any other recognized intellectual property right. The core argument of this chapter embodies the
idea that the same mechanisms used to protect IP rights, could also be used to protect
digital privacy rights invasions. In analyzing the impact that intellectual property has on
privacy rights, it is important to first look at the historical differences between how
copyright and patent violations have been treated differently under American
Jurisprudence. There’ve been a number of authors over the years who have looked at this anomaly.

This legal inquiry takes a completely different path. This study does address many
of the historical arguments as to why this distinction between patent law and copyright
law came into existence. Although, in exploring the various areas and theories that have
been promulgated, this paper will conclude that none of the rationales that have been
postulated so far fully explains the different treatment between the two intellectual
property areas. Ultimately, the paper will apply theoretical paradigms not heretofore
applied to the area of intellectual property law. These theories are well known and well
respected theories in the area of criminology and criminal justice. There are also theories
that sociologists have long recognized as playing a major part in the development of
laws, policies, and the rules and regulations that govern our society. In short, one theory
is called by many “conflict theory.” Although there are other names for the theory, it is
generally recognized as “conflict theory” with variations, depending on the scholar and
scope. Conflict theory postulates that laws, rules and regulations reflect the disparate
power relationship between the “haves and the have-nots.” Those in society who actually
have money, influence, and power, make the rules. A colloquial way of saying this is that
“he who has the gold makes the rules.” (Author unknown, citations omitted. Some have
argued that a comic strip in 1964 first used the expression, but that history is contradicted
by other scholars). We will see there's a lot of truth to this statement. I will argue in this presentation that conflict theory accounts for more of the practical difference in how copyrights are handled versus how patents are handled. It would be disingenuous for me to suggest that this theory is the only theory that accounts for the variation. I do not make that claim. We live in a society that is complex and complicated.

A well-known adage in the area of criminology is that you cannot account for all crime with one theory. You can only account for a portion of crime with various theories. Criminal behavior is so complex that you need a multitude of theories to be able to even remotely account for criminal behavior. Intellectual property law is no less complicated. Numerous motives, theories, and rationales account for various types of behavior. If anyone suggests that they have the magic answer as to why things are the way they are, they are not being intellectually honest. I do not make that claim either. What I do claim, is that one of the theories underlying the anomalous and unique difference between patents and copyrights can be traced to behavior that comports with the theoretical underpinnings of conflict theory. To the extent that no one has, to my knowledge, and as far as my research indicates, tied intellectual property law to the theoretical paradigm of conflict theory, this study breaks new ground.

Additionally, to the extent that theories regarding the power elite are tied to theories related to intellectual property law, they are unique and groundbreaking. Notwithstanding this new understanding and theory, I reiterate that you cannot account for all behavior by the courts, federal legislature, federal executive branch, and all the parties involved in promulgating intellectual property rules and regulations with one theory. I do propose though, that without these theories, i.e. conflict theory, and the
power elite theories, a true understanding of the reasons why there are anomalous differences between patent law and copyright law, our understanding is incomplete. These theories help to demonstrate that class conflict differences, money, power, and political connectedness play a major role in how laws, rules and regulations are adopted and applied.

5.2 Discussion

5.2.1 Origins of American Intellectual Property Law

The United States Constitution, article 1, section 8 indicates that “the Congress shall have power to… Promote the progress of Science and useful Arts, by securing for limited times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.” (U.S. Const. art. 1, § 8, cl. 6.) These 26 words constitute the entire constitutional foundation for American intellectual property Law. Our founding fathers clearly intended to protect intellectual property and to provide a mechanism for Congress to regulate in this area of law. Congress wasted no time in passing legislation and the first Intellectual Property law was passed on May 31, 1790. (1790 Copyright Act) The act was a copyright act that dealt with “maps, charts, and books not exceeding one year.” Some of the relevant portions of the May 1790 Act indicate:

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, that from and after the passing of this act, the author and authors of any map, chart, book or books already printed within these United States, being a citizen or citizens thereof, a resident within the same, his or
their executors, administrators or assigns, who hath or have purchased were legally acquired the copyright of any such map, chart, book or books in order to print, reprinted, published work in the same, shall have the sole right and liberty of printing, reprinting, publishing and vending such map, chart, book or books, for the term of fourteen years from the recording entitled thereof in the clerk's office, as is herein after directed. (1970 Act)

For the next 100 years, copyright enforcement was a civil matter. Not until Congress passed a new Copyright Act in 1897 did criminal penalties become a part of copyright law (1897 Copyright Act). That act stated that;

any person publicly performing or representing any dramatic or musical composition for which copyright has been obtained, without the consent of the proprietor said dramatic or musical composition, or his heirs or assigns, shall be liable for damages therefore, such damages in all cases to be assessed at such sum, not less than one hundred dollars for the first and fifty dollars for every subsequent performance, as to the court shall appear to be just. If the unlawful performance and representation be willful and for profit, such person or persons shall be guilty of a misdemeanor and upon conviction be imprisoned for a period not exceeding one year (1897 Act).

It is quite interesting to note that the criminalization involved public performances of copyrighted works. It is also important to note that this law differentiates between “willful and for profit” conduct and other conduct presumably either not willful and/or not for a profit. (1897 Act) The point of who was covered by this first act that
criminalized copyright violations, is an important point. Performers were the primary target. Later on, in 1909 Congress amended the copyright act to include “aiding and abetting willful and for-profit infringement” (1909 Act.). Many scholars have suggested that the reason the act was expanded in 1909 was because the performers that were covered by the 1897 act, were primarily transient performers who move from town to town. It was next to impossible to sue them because to try to find their permanent home address, for service of process, was quite difficult. The 1909 act was passed to allow those who believed their copyrighted music and material was violated, could go after bar owners, theater managers, and others who were not quite as transient as the performers themselves (Copyright Act of 1909). The 1909 Act was far more comprehensive than the 1897 act and included coverage for the following:

   Section 4. That the works for which copyright may be secured under this act shall include all the writings of an author.

   Section 5. That the application for registration shall specify to which of the following classes the work in which copyright is claimed belongs:

   (a) Books, including composite an cyclopedic works, directories, gazetteers and other compilations;

   (b) Periodicals, including newspapers;

   (c) Lecturers, sermons, addresses, prepared for oral delivery;

   (d) Dramatic or dramatico-musical compositions;

   (e) Musical compositions;

   (f) Maps;

   (g) Works of art; models or designs for works of art;
(h) Reproductions of a work of art;

(i) Photographs;

(j) Prints and pictorial illustrations: (Copyright Act of 1909)

The 1909 Act provided that the above subsections were not intended to limit the applicability of copyright law only to categorize the areas. It extended coverage to foreigners that were domiciled in the United States at the time first publication of their work. That 1909 act spelled out copyright registration requirements, and generally provided for 28 years of protection for the copyrighted work, with the possibility of a 28 year renewal. For purposes of this discussion, the most important provisions of the 1909 act included:

Section 25 (e) which provided:

Whenever the owner of a musical copyright has used or permitted the use of the copyrighted work upon the parts of musical instruments serving to reproduce mechanically the musical work, then in case of infringement of such copyright by the unauthorized manufacture, use, or sale of interchangeable parts, such as disks, rolls, bands or cylinders for use in mechanical music-producing machines adapted to reproduce the copyrighted music, no criminal action shall be brought, but in a civil action an injunction may be granted upon such terms as the court may impose, and the plaintiff shall be entitled to recover in lieu of profits and damages a royalty as provided in section one subsection (e) of this act. Provided also, that whenever any person, in the absence of a license agreement, intends to use a copyrighted musical composition upon the parts of instruments serving to
reproduce mechanically the musical work, relying upon the compulsory license provision of this act, he shall serve notice of such intention by registered mail, upon the copyright proprietor at his last address disclosed by the records of the copyright office, sending to the copyright office a duplicate of such notice; and in case of his failure to do so, the court may, in its discretion, in addition to sums hereinabove mentioned, award the complainant further sums, not to exceed three times the amount provided by section one, subsection (e), by way of damages and not as a penalty, and also a temporary injunction until the full award is paid.

Section 28. That any person who willfully and for-profit shall infringe any copyright secured by this act, or who shall knowingly and willfully aid or abet such infringement, shall be deemed guilty of a misdemeanor, and upon conviction thereof shall be punished by imprisonment for not exceeding one year or by a fine of not less than one hundred dollars nor more than one thousand dollars, or both, in the discretion of the court; (1909 Copyright Act).

These provisions are quite important to review because the beginnings of a division in applicability of the act becomes apparent. Once again performers themselves are subject to criminal penalties. Others who willfully and knowingly aid or abet performers violating these provisions are also subject to criminal penalties. Excluded from criminal penalties are individuals who violate someone’s copyright by mechanical method. This is an ironic distinction. In 1909 the cost of reproduction equipment was quite expensive. The phonograph was invented in 1977 by Thomas Edison and mechanical reproduction of music had started.
Common ordinary performers and common ordinary citizens would not have access to reproduction equipment. The act essentially allows for violation of someone's copyright by mechanical means provided that royalties are paid as provided for in the act. The gist of this provision is to allow smalltime performers and artists to be charged criminally for violating the copyright act, but allowing large corporations, businesses and wealthy individuals that have mechanical recording devices to avoid criminal liability provided they pay royalties. It is important to note that even if the violation by mechanical means is willful and knowing, it is specifically precluded from criminal liability. Thus begins the very first clear demarcation between social economic classes in copyright law. The same differentiation between social economic classes and how they're treated weaves its way throughout intellectual property law for the next generations.

Fast forward almost another 100 years to see other major changes affecting the criminal nature of copyright violations. Acts in 1971, 1974, and 1976 all expanded the criminal penalties for copyright violations beyond the 1909 act (1909 Act). These acts continued to raise the penalties for copyright violations and the 1971 act finally included sound recordings, specifically. First offenses have penalties as much as $10,000 and second and repeat offenses have penalties as high as $25,000 (1976 Act).

The 1971 Act also recognized that willful infringement for-profit of mechanically reproduced recording parts should also be subject to criminal liability (1971 Act). The 1971 act provided a number of provisions including the requirement that copyrighted music and/or publications should indicate they are copyrighted on the first page. The act further gives a better definition of what it means to be a sound recording (1971 Act).
Nevertheless, sound recordings that are mechanically produced did not have full copyright protection. The 1971 Act spells out the purpose of the act as:

“Existing federal copyright law title 17, United States Code, protects the owners of copyright in musical works from an authorized and uncompensated duplication but there is no federal protection of sound recordings as such. As a result, so-called “record pirates” if they satisfy the claim of the owner of the musical copyright can and do engage in widespread unauthorized reproduction of phonograph records and tapes without violating federal copyright law. It is also true under existing law that the protection given to owners of copyright in musical works with respect to recordings of their works is special and limited. The purpose of section 646 as amended is twofold. First, section one of the bill creates a limited copyright in sound recordings, as such making unlawful the unauthorized reproduction and sell of copyrighted sound recordings. (1971 Act).

5.2.2 Applicability of the Legislation

The 1971 Act is quite extensive in the changes that it makes to the law. This was in large part to the voluminous findings as indicated in the act. The act goes on to indicate:

The attention of the Committee has been directed to the widespread unauthorized reproduction of phonograph records and tapes. While it is difficult to establish the exact volume or dollar value of current piracy activity, it is estimated by reliable trade sources that the annual volume of such piracy is now in excess of $100 million. It has been estimated that legitimate prerecorded tape sales have an
annual value of approximately $400 million. The pirating of records and tapes is not only depriving legitimate manufacturers of substantial income, but of equal importance is denying performing artists and musicians of royalties and contributions to pension and welfare funds and Federal and State governments are losing tax revenues.

If the unauthorized producers pay the statutory mechanical royalty required by the Copyright Act for the use of copyrighted music there is no federal remedy currently available to combat the unauthorized reproduction of the recording. Eight States have enacted statutes intended to suppress record piracy, but in other jurisdictions the only remedy available to the legitimate producers is to seek relief in state courts on the theory of unfair competition. A number of suits have been filed in various states but even when a case is brought to a successful conclusion the remedies available are limited. In addition, the jurisdiction of States to adopt legislation specifically aimed at the elimination of record and tape piracy has been challenged on the theory that the copyright clause of the Federal Constitution has preempted the field even if Congress has not granted any copyright protection to sound recordings. While the committee expresses no opinion concerning this legal question, it is clear that the extension of copyright protection to sound recordings would resolve many of the problems which have arisen in connection with the efforts to combat piracy in state courts. (1971 Act)

It is quite clear from the passage above, that Congress recognized a serious problem with the failure to protect sound recordings. The automatic royalty provisions of the 1909 act allowed unscrupulous businessmen to sell some recordings by musicians
even though these musicians were not under contract to them for their particular recordings. The remedy of only being able to collect the actual royalty fees put the recording industry and artists at a serious disadvantage. Congress saw this problem and corrected it. While this correction may have had a benefit to artists, it was primarily passed at the behest of recording studios. After signing artists and producing records they had no way to protect themselves from third-party manufacturers that reproduced the sound recordings paid the royalty fee, which allow them to sell these records to the public. Powerful recording industry tycoons and executives lobbied Congress for these changes.

Both the 1974 act and the 1976 act cleared up other issues and the 1976 act raised fines to $25,000 for a first offense and up to $50,000 for repeat offenders (1976 Act). In 1982 Congress passed the Piracy and Counterfeiting Amendments Act of 1982. This act was intended to stem a growing amount of piracy for songs and software. This act in relevant part states as follows:

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act // 18 USC 2311 // may be cited as the “Piracy and Counterfeiting Amendments Act of 1982. (1982 Act)

The 1982 Act implements even greater changes to the law by expanding the coverage to software as well as expanding the scope. It broadens the criminal reach.
Section 2 indicates:

Sec. 2. Section 2318 of title 18, United States Code, is amended to read as follows: Section 2318. Trafficking in counterfeit labels for phonorecords, and copies of motion pictures or other audiovisual works;

(a) Whoever, in any of the circumstances described in subsection (c) of this section, knowingly traffics in a counterfeit label affixed or designed to be affixed to a phonorecord, or a copy of a motion picture or other audiovisual work, shall be fined not more than $250,000 or imprisoned for not more than five years, or both…

(e) Except to the extent they are inconsistent with the provisions of this title, all provisions of section 509, title 17, United States Code, are applicable to violations of subsection (a).

Sec. 3. Title 18, United States Code, is amended by inserting after section 2318 the following new section:

Section. 2319. // 18 USC 2319. // Criminal infringement of a copyright

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsection (b) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

(b) Any person who commits an offense under subsection (a) of this section—,

(1) shall be fined not more than $250,000 or imprisoned for not more than five years, or both, if the offense—,
(A) involves the reproduction or distribution, during any one–hundred–and–eighty–day period, of at least one thousand phonorecords or copies infringing the copyright in one or more sound recordings (1982 Act).

This act once again raised the possible fines for violation to up to $250,000.00.

The 1982 Piracy and Counterfeiting Amendments act of 1982 was by far the most aggressive and repressive copyright act passed by Congress, it goes on to indicate:

(B) involves the reproduction or distribution, during any one–hundred–and–eighty–day period, of at least sixty—, five copies infringing the copyright in one or more motion pictures or other audiovisual works; or

(C) is a second or subsequent offense under either of subsection (b)(1) or (b)(2) of this section, where a prior offense involved a sound recording, or a motion picture or other audiovisual work;

(2) shall be fined not more than $250,000 or imprisoned for not more than two years, or both, if the offense—,

(A) involves the reproduction or distribution, during any one–hundred–and–eighty–day period, of more than one hundred but less than one thousand phonorecords or copies infringing the copyright in one or more sound recordings; or

(B) involves the reproduction or distribution, during any one–hundred–and–eighty–day period, of more than seven but less than sixty–five copies infringing the copyright in one or more motion pictures or other audiovisual works; and
(3) shall be fined not more than $25,000 or imprisoned for not more than one year, or both, in any other case…(1982 Act).

Amazingly, someone who was guilty of copying as few as seven videotapes could be fined as much as $25,000 each, and can spend up to one year in jail. This provision was enforced against a number of college students that simply copied movies for personal use. Clearly a violation of copyright law, but fines of $25,000? One year in jail? In this instance, the 1982 act was passed at the behest of the recording industry in America. They were determined to protect their financial interests. Interestingly enough, the same industry, recording industry in America battled and lost one of the major cases that would define the era. In the case of Sony Corporation of America versus Universal City Studios Incorporated, 464 US 417 (1984), Universal Studios attempted to force Sony to remove Betamax players from the market. Universal City Studios along with other recording industry executives and companies claimed that Sony’s Betamax recorder was designed specifically to violate their copyrights and copyright protected music and videos. Sony countered that the Betamax player had other non-infringing uses and that simply because it had the capacity to copy videos did not make it illegal. In a landmark ruling in 1984 the United States Supreme Court agreed with Sony. They reversed the Court of Appeals that had held that Sony was liable for contributory infringement of copyrights. The court indicated that there was a significant likelihood that free television programs and other recordable events could be recorded that would allow consumers to time shift their watching habits and that this was not a violation of copyright law. The
Sonly Betamax case is what opened the door for home recording of music, videos and other media.

New acts in 1992 and 1997 addressed the problem related to the new digital environment. The 1997 act became known as the NET act, and increased potential fines to as much as $100,000 with penalties as much as one year in prison. The last act passed by Congress is known as the Digital Millennium Copyright Act (DMCA). This 1998 act raises the stakes significantly. First-time offenders can be fined as much as $500,000 and imprisoned for five years or both. For repeat offenders the maximum penalty is $1 million and maximum time in prison up to 10 years, or both (DMCA). The Digital Millennium Copyright Act was Congress’ attempt to catch up with the new digital environment. The act also incorporates and implements the World Intellectual Property Organization (WIPO) Copyright Treaty and Performances and Phonograms Treaty. This all-pervasive act, dealt with not only recording industry concerns, but also the burgeoning computer industry. By the passage of this act, many were aware that we were living in an entirely new age of computers and computer technology. Notwithstanding this awareness, Congress never did fully grasp, as probably most people did not, how ubiquitous computer based technology would become in our everyday lives. The Digital Millennium Copyright Act (DMCA) was quite broad at the time of its passage. It did not take long for the problems associated with digital media, and the brave new digital world to outpace the confines of the act. Notwithstanding the warp speed that new inventions were permeating society, The DMCA did accomplish some noteworthy goals. One of the most important provisions of the DMCA are the safe harbor provisions for online service providers. The safe harbor provision allows online service providers to not be held liable
for allegedly infringing material provided that they follow certain guidelines. If they operate within these guidelines, and either promptly remove or block access to allegedly infringing material in a timely fashion when they've received notification of infringement claim from a copyright holder, they will avoid liability as a company (DMCA).

Ironically, this provision of the DMCA codifies what ultimately case law begin to conclude before the law was passed. The Internet turned copyright law on its head. Prior to Internet law, copyright law placed the onus of compliance with copyright provisions on the infringer. The law had positive proscriptions indicating that certain behavior was illegal or improper under copyright law. It was left up to the potential infringer to avoid such conduct. A number of cases, primarily led by Google’s parent company, Alphabet, Incorporated, led the fight to allow Internet service providers to provide Internet content irrespective of potential copyright violations. The notion that someone, or their agent, holding a copyright have the responsibility to notify Internet Service Providers (ISPs) of infringing conduct is a new development in copyright law. The DMCA sets the new paradigm into statutory law. To the extent that the DMCA picks up where the Electronic Communications Privacy Act of 1986 left off, we now have some degree of consistency in how electronic communications are construed. The missing link and remaining connections relate to how digital privacy should be affected by these changes.

5.2.3 Patent Law History

The first patent act was passed in 1790. This act allowed patents for “any art, manufacture, engine, machine or device,” (1790 Patent Act). According to one scholar, the American Patent Act of 1790 was “the first statutory enactment by any country
obligating any form of examination to determine whether a patent should be granted,” (Walterscheld, American Patent Law and Admin., 1997). Walterscheld goes on to indicate that the idea of absolute novelty was a uniquely American idea. England as well as the Italian City States did not insist on absolute novelty, only newness to the particular area where the practice was being introduced. The 1790 act required actual novelty, (Walterscheld, American Patent Law and Admin., 1997) Just a few years later in 1793 the act was amended to include “composition of matter, “as well as to impose a registration system akin to the British system in lieu of examination, (Walterscheld, and 1793 Act). Patent law statutory history is quite short as compared to copyright law statutory history. The 1952 statute amended the 1793 act and laid out what would become the scheme for patent protection since that time. Under the 1952 act, eligibility for a patent requires four things. Utility, novelty, non-obviousness, and sufficiency of disclosure, (1952 Act). The vast majority of activity regarding patent law has been within the court system. One of the major topics of historical disagreement has been what has been called “the Jeffersonian story of patent law.” According to advocates of this school of thought, patent law grants a special monopoly privilege to a few not justifiable under concepts of natural philosophy. The idea behind this notion is that Congress passed the Sherman act making monopolies illegal, yet somehow or another people with a patent are able to have a monopoly. This concept had been buttressed by statements from Supreme Court justices in their opinions which seemed to support this notion. Other scholars tend to disagree with that theoretical paradigm and postulate that patents are nothing more than property rights, (Mossoff, Cornell Law Rev., 2007)
The America Invents Act (Leahy-Smith Act) presented wholesale changes to the US Patent system by changing from a first to invent to a first to file system in harmony with the rest of the world, (Leahy-Smith Act, 2011).

5.2.4 Alternative Theories Pertaining to the Origins of Intellectual Property Law

There are a number of theoretical articles about the origins of intellectual property law. One author discusses these origins as “Origin Myth” or “Origin Stories.” (Silbey, Geo. Mason L. Rev., 2008). The author discusses such myths as what he calls the “creation myth” and indicates that our notions of property rights in the Intellectual Property area are deeply rooted in those theories from childhood. Other scholars trace our patent system to the Statute of Monopolies passed in England in 1623. This statute codified what had been the practice for quite some time in England, namely the practice of granting to merchants what are called limited term monopoly rights for either new inventions or importers of new trade, (Walterscheid, Pat. And Trademark Office, 1997). Walterscheid indicates that the custom of granting limited term monopoly privileges actually dates back to the Italian City states of the fourteenth and fifteenth century. Although I cannot specifically address the earliest adoption of patent type protections, it is my theory that there is an even earlier example of copyright protection than some of the earliest theories I have seen proposed. This origin is contained in Exodus 20:4 which reads, “Thou shall not make unto thee any graven image, or any likeness of any thing that is in heaven above, or that is in the earth beneath, or that is in the water under the earth.” (Exodus 20:4 KJV) While many scholars would indicate that this is only a prohibition against idolatry, a closer analysis would indicate that while it is clearly a prohibition
against idolatry, there is also the prohibition of a “graven image.” This prohibition of creating a “graven image” would arguably be the first “Copyright Act.” This prohibition against graven images is clearly due in part to the claim made in Genesis 20:11 that “For in six days the lord made heaven and earth, the sea, and all that in them is, and rested the seventh day:” In short, this “copyright” prohibition says “I made it all, it’s mine, and you shall not copy it by any graven image or likeness thereof.” Most biblical scholars would indicate that the book of Exodus, also known by the Jewish nation as the part of the Torah and by later Christians as part of the Pentateuch, was written by the biblical character Moses sometime around the 5th Century B.C. Although the date is certainly in dispute, the general timeframe of the authorship of the book is pretty well agreed upon. Whenever the book of Exodus was written, it appears to be before any other works claiming to espouse copyright or any other intellectual property right.

Parenthetically, the right to privacy also has deep roots. As mentioned earlier, Harvard Law Review recognized the existence of that right back in 1890. If we go back to the Declaration of Independence, the document memorializes the idea of “Life, Liberty, and the Pursuit of Happiness.” One thing is certain—without privacy there can be no liberty! Liberty demands that a person has the right to live their life how they choose without interference. The idea that a government or business or anyone else can compromise your privacy without consequences is farcical. To many, liberty is a God-given right. If it is inalienable, then privacy is equally important to protect and assert the right to liberty.
5.2.5 Other Theories of Law

Much has been written about which theoretical paradigm is at play when discussing Intellectual Property Law. I attempt to avoid the traditional arguments and to go in a different direction. We can start this analysis by looking at the theories of Donald Black regarding the nature, purpose and effect of law. Donald Black asserts in his book “The Behavior of Law” that “law is governmental social control,” (Black, 1976). The more social control you have in any particular area, the less need for laws to regulate behavior. Many people are controlled by their personal relationships. Whether these relationships revolve around church attendance, social networks, or family relationships, there are some informal controls that help to assure that individuals behave in compliance with social norms. In the absence of these informal social controls, formal laws and rules are necessary. Black sees this relationship as inverse. The more social control the less law needed. Where there is very little social control, more law is needed, (Black, 1976).

Donald Black further looks at concepts of stratification as helping to explain the relationship between law and individuals. He defines stratification as inequality of wealth. He states in his book that law varies directly with stratification. More stratification, the greater need for law. Less stratification, a lesser need for law, (Black, 1976).

Black further postulates that “people with less wealth have less law.” That is to say, according to Black, people that can afford lawyers and can afford to influence politicians have endless points of law on their side. The poor on the other hand, have laws that are stacked against them. Because they cannot influence the political process the laws that are passed are antithetical to their best interest” (Black, 1976).
Donald Black goes on to demonstrate that law is directional. Upward law versus downward law. Downward law is quite penal in its approach and effect. Donald Black continues his analysis by looking at culture. Less culture, more law. More culture, less law. According to Black, this relationship is curvilinear. What this means is that laws less likely at the extremes where there is little or no cultural diversity. These outliers do not necessarily have the same issues as the case is in the middle (Black, 1976).

In general terms, if we take what Donald Black says in his book as true, then the poor are subjected to more laws than the rich, resulting in the loss of liberty and privacy. The impact of these laws have a far greater detriment to individuals towards the lower end of social stratification. Individuals with greater wealth would be far more insulated from laws and the impact these laws would have in their lives. Further, access to the legal system would be greater for those who have more resources than those that do not.

Another author, G. William Domhoff, has written a number of books dealing with corporate and class dominance. One of his books “Who Rules America,” looks at how power and influence have a lasting and major impact on society, (Domhoff, 2010).

The book specifically deals with what Domhoff and other social scientists call “The Power Elite.” The power elite are made of members of society that by virtue of their money, influence, connections and friendships, they dominate the functions and operations of government and industry, (Domhoff, 2010). By virtue of this inordinate amount of power, this group has an outsized influence on laws, rules and regulations in American society. The power elite typically attend some of the same Ivy League institutions and are socially connected. Domhoff and other social scientists refer to the “policy planning network.” This group of individuals by virtue of their status as the
power elite also have inordinate control over foundations, think tanks, policy discussion groups, and the business Roundtable, (Domhoff, 2010). The book “Who Rules America” is just one book that supports these theories. The idea of the power elite and the idea of policy planning networks is well-established in social sciences literature. The Domhoff book is in its seventh edition, and has been available continuously in the United States and some edition or another for the past 50 plus years.

The ideas that are postulated are not considered to be fringe ideas or out of the mainstream social science thought. The idea of the power elite is a well-accepted mainline social science paradigm. Many scholars trace conflict theory back to the writings of Karl Marx. While it is true that Marx proposed a conflict theory paradigm, today's scholars that subscribe to conflict theory are a long way from anything that could remotely be called socialist theory. The immediate question we have to deal with is how do conflict theories impact intellectual property law? Is there a relationship? Do these theories help to explain why the law may be the way it is? I intend to demonstrate that these theories underlie the very basis of why law is passed and how it became law. If we go back to the first Copyright Act of 1897 that imposed criminal sanctions, it is clear that the only individuals that were directly affected by the criminal portions of the act were typically transient and without financial means. This is certainly not a coincidence. The law specifically singled out “public performances” as being worthy of special attention. This era was before the abundance of recorded musical and video media, so the idea of copyright violations involving electronic duplication of protected works was limited to those of financial means. The large commercial studios had the capability to duplicate and distribute protected works. These studios were ultimately dominated by a few large
companies such as Walt Disney, 20th Century Fox and Warner Brothers. Why single out public performances? Although the argument can be made that a movie or musical production would be a public performance, the record does not indicate that this is what the law had in mind. It is clear from the language of the act, as well as enforcement mechanisms used for the next few decades that the idea of public performances related to live performances by actors and musicians. From the very origins of copyright criminal law, a class of individuals were singled out that generally were not members of the elite power structure in society.

It is clear from the early literature that the idea of infringing on someone's intellectual property rights was considered theft. The ECPA also considers taking someone’s private digital property theft. A look at Black's Law dictionary definition of theft would indicate that theft is a “felonious taking and removing of another's personal property with the intent of depriving the true owner of it.” (Black’s). A theoretical problem immediately arises when concepts of theft are applied to intellectual property law violations. For example, in the case of a musical composition, how does the public performance of that composition deprive the true owner of the composition? While there may be an infringement, there does not appear to be a deprivation. Both parties can mutually have access to the musical performance and musical score simultaneously. The infringers use of the musical composition does not deprive the true owners right to also play and use the composition. This lack of deprivation makes intellectual property theft, at least in the case of copyright, different from other types of theft where the true owner is fully deprived of the use of their property. Thus the term infringement. To whatever extent Congress decided that infringement is the same as theft, the dissimilarities became
unimportant. Because Congress has the right to proscribe and forbid certain behaviors, theoretical notions of theft do not necessarily have to deter Congress from acting. It obviously did not. Notwithstanding the differences between theft of personal property versus infringement of intellectual property, Congress saw fit, only in the case of copyright, to criminalize the latter.

The real question that arises from this fact pattern is why did Congress decide to criminalize public performances versus other violations of intellectual property law? When looking at the theoretical paradigms that come to play, as mentioned earlier, by theories regarding the power elite, and theories about the “haves and the have-nots,” it becomes more clear that the statutes criminalizing intellectual property law copyright infringement were specifically designed to accomplish the very thing it appears they were intended to accomplish. Vis-à-vis to impose a harsh criminal penalty on performers and actors for their public performances. Some scholars attempt to trace this theoretical shift from civil penalties only to criminal penalties to the fact that intellectual property continued to grow in value as opposed to real and personal property. This certainly would be quite true for the latter part of the 20th century. The real question to answer, is whether that was actually true in 1897. In 1897, as mentioned before, only a few wealthy individuals had the capability to actually record and disseminate protected intellectual property works. These wealthy individuals controlled the fledgling film, book publishing, and music industry. Why would Congress pass an act that largely ignores the potentially bigger problem of mass infringement, versus the relatively minor problem of public performance infringement?
I am not suggesting that Congress needed a crystal ball to foresee into the future the rapid growth and development of media production companies. Enough evidence existed in 1897 for Congress to understand the difference between protecting the interests of large corporate and financial behemoths, versus protecting the interests of generally, most commonly, smalltime local performers. It is not too much to infer that Congress was neither naïve nor misinformed as to who the act would apply to primarily. This is further made clear by the adoption of the 1909 act which broadens the impact of the criminal sanctions to cover aiding and abetting, (1909 Act). In making the decision to differentiate which types of copyright violations would be subject to criminal penalty, Congress showed a clear preference for protecting one type of rights over others. Congress always has the right to pass whatever laws it deems appropriate, even if these laws disproportionately affect the poor.

5.2.6 The Absence of Criminal Sanctions for Patent Violations

While the history of criminal sanctions can be traced from its misdemeanor origins for copyright law to ever increasing fines and longer sentences for copyright violators, the absence of any corresponding criminal penalty or sanction for patent law violations is quite stark. When we consider the fact that the first misdemeanor criminal sanction for copyright violations was passed in 1897, why is it that nearly 120 years later, no criminal sanctions have been passed regarding patent violations? The idea of criminal sanctions for patent violations are not completely novel. The European Union considered such sanctions when they recently updated their intellectual property laws. Ultimately, they decided not to impose cruel sanctions for patent violations. When looking at the
impact to society for patent violations versus copyright violations, many argue that copyright violations have a larger impact. It may be true that more people are involved in copyright violations. That is not the same as saying that the impact is larger for copyright violations. Most recently in the news, many should be aware of what have been termed as the “smart phone patent wars.”

The major lawsuits in these wars have been between Apple Computer Incorporated and Samsung Electronics Company, Limited. These multimillion dollar battles involve billions of dollars in profits and fees. Apple has claimed that Samsung has violated its patents that makes it iPhones unique. On the other hand, Samsung has made the same claim about its smartphones. In this battle fought on multiple continents, Apple has won in some courts and Samsung has won in other courts. One thing is certain; there are billions of dollars at stake in the litigation. It seems obvious on its face that someone at one or both of these companies must assume some responsibility for the intentional violation of patent protections. It is inconceivable that corporate executives at Apple or corporate executives at Samsung are totally unaware of any infringing activities by their companies. After the millions of dollars spent in litigation, numerous depositions, interrogatories and discovery requests, can we logically presume that everyone at either of both companies just innocently, and unknowingly infringed on the others patent rights? This is next to impossible to fathom. Engineers, technologists, and other employees have to have some awareness where they got the ideas or technology that forms the basis for these lawsuits. With this much evidence in existence, how hard would it be to mount some sort of criminal investigation that held some of the parties criminally liable for their behavior? Theories that purport to write off the possibility of patent
criminal liability based on the difficulty of prosecution are misguided. If given the statutory authority to proceed with criminal prosecutions, there are some industrious prosecutors that would quickly build solid criminal cases going after some of the worst and most flagrant offenders.

In the last 10 years or so, the United States has embarked upon a relative paradigm shift in how corporations are treated. The Supreme Court has on a number of occasions indicated that corporations are in fact people. They've indicated that corporations have rights, duties and obligations stemming from their citizenship as people. In one such case Citizens United v. Federal Election Commission, 558 US 310 (2010), the Supreme Court held that companies and unions could spend as much as they like in elections to defeat political candidates. The decision essentially recognized First Amendment free speech rights for corporations. The Supreme Court as well as lower courts have begun to impose corporate criminal liability on not only corporations but also individually on corporate officers. This new theoretical paradigm posits that those who run corporations must personally be liable for the behavior of those corporations to assure that these businesses fulfill all of its obligations to stakeholders. Although the idea of corporate criminal liability is not entirely new, its imposition to officers and directors has evolved in recent times, (Dodd-Frank, 2002). After a number of corporate scandals, as well is corporate failures, the United States passed what became known as the Dodd-Frank Act. This act specifically provides that officers and directors of a corporation are charged with the responsibility of knowing what is happening in those businesses. Failure to understand what's going on, when you are in a position of leadership, is not an excuse for avoiding criminal liability. The Dodd-Frank Act specifically imposes liability on
these officers and directors who are in a position to know what the business is doing, or failing to do (Dubber, Nev. Crim. L. Rev., 2013).

Why is their duplicity in liability for corporate officers and directors when it comes to patent infringement but clear liability when it comes to other kinds of corporate misconduct? On the one hand, Dodd-Frank imposes civil and criminal liability to these officers and directors that violate financial, disclosure, and/or ethical rules and regulations. Patent infringement is like the 800-pound gorilla in the room. The fact that Apple and Samsung are involved in over 50 lawsuits with each other regarding patent infringement gives us some sense as to how important these issues are and the real scope of potential violations. Most analysts would indicate that the potential loss to business for patent infringement approaches billions of dollars. Although the estimates are all over the board, they are all in the billions. That being said, it is difficult to justify why a college student that downloads ten songs without permission is subject to criminal prosecution, but an executive of a major corporation can supervise the theft of billions of dollars in protected patent property, and face no criminal sanctions whatsoever. Under the ECPA, persons that steal satellite TV or cable signals are criminally prosecuted for their electronic theft/ How could this possibly be fair? Many have tried to argue that the reason why there are no criminal sanctions in patent law is because it will be difficult to prove criminal liability. There certainly may be some truth as to the complexity of patent law, but as demonstrated earlier, that is not an excuse for not having protections and sanctions in place for obvious violators.

Let us take a look at the patent process to make some reasoned judgments as to whether or not criminal liability can be imposed for infringers. In a successful patent
prosecution (the term prosecution is used to refer to obtaining a patent) certain things must occur. First, the inventor must describe the invention in writing. Second, the application must" enable any person skilled in the art to which it pertains… To make and use" an invention. Third, a claim has to be clear and concise. Fourth, the inventor must" set forth the best mode contemplated by the inventor of carrying out his invention."

(Mendez, Buff. Intel Prop., 2008). If the Patent Office, and courts that review patent decisions, can engage in this deep level of analysis, why should we be concerned that other specially trained lawyers and paralegals cannot navigate successfully any potential pitfalls with successful criminal prosecution?

United States patent law as currently configured prohibits" whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefore, infringes the patent." (35 USC)

Many argue that prosecuting patent infringers would be too difficult. The reasons given are that the criminal courts are not qualified to deal with these patent issues. This argument suggests that patent issues are so complex that judges would not be able to understand what's going on. If that is true then there should not be any civil violations for patent infringement. Just like civil judges have to learn the particulars of patent law, so criminal law judges would have to learn new things. Certainly, a successful defense to patent infringement would be the invalidation of the patent. It is quite clear that prosecutors would have to use reasonable judgment in which patent infringers they go after. This level of discretion is not new to prosecutors. Exercising discretion as to whom they should prosecute is part and parcel of what prosecutors do every day. Why would
making that assessment in a patent case be any different than the assessment that
prosecutors make in any case? In a case that is a close call, prosecutors would certainly
have the discretion not to bring criminal charges. They have that discretion now. What
about the clear and obvious violations? Once again, I go to the analogy of a college
student that downloads 10 copies of protected music illegally. The student is prosecuted
for and convicted of criminal copyright infringement.

On the same campus, a professor in one of the university discovery parks,
intentionally steals protected patented information and ideas from another company. The
professor understands fully that these inventions are patented. With full intention of
wrongdoing, the professor infringes on the patent and improperly incorporates the
patented invention into a product for his own startup company. The way the law stands
right now, the student goes to prison, while the professor goes home to dinner! How
could that possibly be fair?

Complexity is not in and of itself a sufficient grounds to allow this disparity to
continue to access. Another reason given for why patents should not be part of criminal
law violations is because some say it is not possible for law enforcement officers to
determine whether or not a patent violation has occurred. (United States Code: Title 35 -
Patents, Part II).

Other reasons given are that patent litigation is expensive, and that a significant
portion of patents are revoked in the course of patent litigation. (United States Code: Title
35 - Patents, Part II). Once again, simply because prosecutors face a difficult job, should
not be an excuse for corporate criminals, and other violators, to violate the law of patents,
and to use another person’s invention intentionally, potentially making millions or
billions of dollars in the process, without any criminal liability whatsoever. Complicated trials for criminal behavior have become a part and parcel of the American landscape. Once again, complicated trials have become commonplace in the era of Dodd-Frank. In many ways we have to look at another theory for criminal justice and criminology to really see what’s going on. Edward Sutherland postulated way back in the 1960s a new concept of criminal liability. He coined the term “white-collar crime”.

Edward Sutherland used this phrase to refer to criminals that may be educated, and are almost always financially well-off, and can wreak havoc in society by stealing from and misusing corporate assets with impunity, (Friedrichs, 2004). It is still a common occurrence in the United States for someone that might be guilty of stealing a few hundred dollars’ worth of goods from the local grocery store to be sentenced to more time in prison then a corporate executive that may have stolen millions of dollars including retirees’ life savings. There is no question that the imbalance has improved over the last 20 years. Notwithstanding the improvement, it is still common that white-collar criminals are treated with kid gloves as compared to the street criminal that likewise did no physical harm to the victim.

The only real explanation that gets to the very heart of why people with power, money, prestige, and connections can avoid criminal liability has to do with a conflict perspective. Although there are different theories as to why these white-collar criminals are able to steal millions of dollars’ worth of patented material, none of the theories adds up without looking at the conflict perspective, and power perspectives.

Only when you analyze how laws are passed and the influence of political action committees as well as lobbyists in the political process can you reach a conclusion that a
person guilty of knowingly and intentionally stealing millions of dollars does not face
criminal prosecution but an individual guilty of stealing a few dollars can go to prison for
quite some time. Theories that have been postulated so far, including a conflict
perspective, the power elite, and policy planning networks helps to account and explain
this anomaly. The fact that there have been numerous successful prosecutions in other
areas of IP law undercuts any notion that criminal prosecution in the area of patent law
would be too difficult.

Some examples of other areas of IP law where criminal law violations have been
successfully launched include the Economic Espionage Act of 1996. This act imposes
criminal and civil penalties for the theft of trade secrets. The law was originally passed
because of a high level of concern that foreign companies were attacking American
businesses with electronic theft of important information, (Am. Crim. L. Rev.). The act
defines trade secret as information that has “derived independent economic value, actual
or potential, from not being generally known to, and not being readily ascertainable
through proper means by the public.” (Am. Crim. L. Rev.) The act further imposes the
requirement that the owner has to take reasonable steps to keep the information private.
(Am. Crim. L. Rev.) The Economic Espionage act also requires that the “theft of trade
secrets benefits a foreign government, instrumentality, or agent.” (Am. Crim. L. Rev.).

Prior to adoption of the Economic Espionage Act of 1996, another act existed that
also deals with trade secrets. The “Trade Secrets Act” (TSA) deals with the unauthorized
disclosure of government information by employees.

The idea that Patent Violations are immune from criminal prosecution is
inconsistent with the entire notion of protection of individual and corporate privacy,
property and intellectual property rights. The entire movement in the area of rights protection seeks to find ways to buttress protection of rights. (Am. Crim. L. Rev.).

5.2.7 The Relationship between the Protection of Electronic Communication and Protection of Digital or Electronic Intellectual Property Rights

Today, courts disagree on what the constitutional protections may be relative to electronic communications and surveillance as well as how to protect electronic intellectual property rights or digital privacy rights. United States Circuit Courts have split on whether their decisions should expand digital privacy rights or limit digital privacy rights. Both of these scenarios pose a question implicating how fourth amendment protections will be analyzed and implemented. What is clear to even a casual observer is that if digital privacy rights are at risk in general, than digital privacy rights coupled with valuable intellectual property rights are also at risk. In order to ascertain the efficacy of legal protections today, it is necessary to compare the protections in existence today with protections in the past.

This analysis will gauge the status of protection afforded electronic communications today with the protection levels of electronic and non-electronic communications in bygone decades. If the protection levels are the same, and courts are enforcing modern-day electronic communications protections in the same manner that non-electronic communications were protected in the past, than the case law history from the past can help to inform us as to what we can expect in the future. If not, then this new electronic frontier has ushered in a new era that creates a disjunctive from some of the
common law precedents of the past. 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 we can see that the
law has lagged behind the advancements in communications technology leaving
electronic communication rights, associated data security rights, electronic intellectual
property rights and most notably, digital privacy rights vulnerable and unprotected.

5.3 Conclusion

Many proposals have been made as to how best to protect Americans
constitutional privacy rights. The root of the problem stems from a basic reality. The
founding fathers never really contemplated digital privacy rights per se. They certainly
understood in the fourth amendment that citizens should be “secure in their persons,
houses, papers, and effects.” Looking at the history of how the United States Supreme
Court found that privacy was a right that emanated from the penumbras of rights as
contained in the Bill of Rights, indicates that we have a judicially mandated concept that
is subject to interpretation and change. A recent look at the make-up of the Supreme
Court demonstrates how this right, particularly of digital privacy, still exists at the whim
of the courts.

Presently there are only eight members sitting on the Supreme Court, after the
death of Justice Antonin Scalia. Most recently, in a case before the court, regarding
funding of public unions, the court split with a four to four tie. It is pretty clear from that
situation that we are at a stage in our history when the Supreme Court could become
more conservative or more liberal. Who is to say that the earlier rulings, even finding that there is a right to privacy, are sacrosanct. There is a political battle going on in Washington DC as I write the final chapter of this dissertation where the Republican-controlled Senate refuses to act upon the Supreme Court justice nomination of President Obama. I obviously do not have a crystal ball, and cannot predict how this impasse will be played out. If the Senate GOP leadership continues to insist that they will not hold any hearings whatsoever on the presidential nominee, this seat could be made vacant until after the 2016 elections. If that is the case, the direction of the Supreme Court will be seriously impacted by whomever wins the 2016 election. If a conservative wins, we can expect that the court will end up with a conservative nominee and ultimately a conservative justice. If a liberal wins, we can expect that the court most likely will end up with a more liberal nominee and ultimately more liberal justice.

Although it is not always clear how conservatives or liberals may view privacy rights, American’s digital privacy rights should not be contingent upon who is nominated and confirmed to the Supreme Court. There was no way in the constitutional convention of the late 1700s that our founding fathers could have foreseen the radical transformation of our society. Electricity, indoor plumbing, automobiles, airplanes, radio, televisions, telephones, cellular phones, and a whole host of inventions had not even been dreamed of by that time. From time to time, the American people have recognized that the Constitution needed updating to reflect the changes to modern society. It is ironic that the most recent amendment to the Constitution became effective on May 7, 1992. This amendment was submitted by Congress to the states for ratification way back in 1789. The amendment is quite simple and states, “no law, bearing the compensation for the
services of the Senators and Representatives, shall take effect, until an election of representatives shall have intervened.” (United States Constitution, Amendment 27, 1992).

When this amendment was first submitted to the states for ratification the idea of privacy rights didn’t even exist. By the time it was ratified in 1992, the need for privacy rights, particularly digital privacy right was quite apparent.

Today, in 2016, Americans expectations of digital privacy have significant and important dimensions. Violations of digital privacy rights, as demonstrated in Chapter 4, not only emanates from the government, but even to a greater extent from big business. Additionally, individuals, can violate a person’s digital privacy rights, and wreck-havoc in a victim’s life. Some of the examples, as mentioned, include sportscaster Erin Andrews and how her life was drastically changed by an invasion of her privacy by a private individual. In this electronic age, privacy rights, and particularly digital privacy rights are far more important than simply being secure against unlawful searches and seizures and the body of law developed to protect physical property.

When the fourth amendment indicates that, “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized,” it was language for a different time and era as it relates to digital privacy rights. It was brilliant language, no doubt, but antiquated language that was addressed at physical searches, and not at all aimed at electronic and digital privacy. The idea of probable cause being necessary before the government can enter your house or
business, go through your papers and effects, is certainly a valuable protection. Unfortunately, it is not enough to protect digital privacy rights. Digital privacy rights, are far more important to our security as a people than the traditional notions of unreasonable searches and seizures. Probable cause is one of the lowest standards recognized in law. Although it is certainly greater than articulable suspicion, not by much. As indicated in earlier chapters, the United States Supreme Court articulated what probable cause means in the case of Brinegar v. United States (338 U.S. 160). The court implemented the two-pronged test in Aguilar v Texas, (378 U.S. 108) in 1964 and abandoned that test in 1983 in favor of a “totality of Circumstances” test in the case of Illinois v Gates (462 U.S. 213). This new totality of circumstances test rejected the stronger two-pronged test. In a dissenting opinion, Justices Brennan and Marshall indicate that the new test allows for dishonest and unreliable testimony to support a probable cause affidavit that will severely impact the rights of those that have not committed a crime.

In short, the privacy rights, particularly digital privacy rights, of Americans are hinged upon whether or not justices that authored the decision in Illinois v Gates, sits on the Supreme Court, or whether or not justices that are sensitive to digital privacy rights have control of the Supreme Court. The reality that existed in 1983 still exists today. Americans’ digital privacy rights can literally be expanded or contracted depending on the ideological perspective of the five justices who make up the majority of the court. Digital privacy rights, in 2016, need far more protection than happenstance. Americans need protections not only from the government but also from private actors. The judicially created concept of privacy is insufficient to protect these important digital privacy rights in our complex technological society as articulated today.
This study proposes three separate solutions to this problem. The first solution: Judicial Fiat, or adoption of a Clear and Convincing standard for digital privacy rights, by court rulings. This is a possible but quite unlikely solution. In an era where many justices have shown a reluctance towards judicial activism it is quite unlikely for the court on its own to change course that radically midstream. It certainly is possible, but highly unlikely. The second solution to the problem of digital privacy rights for American citizens is to seek, and successfully implement a constitutional amendment that unequivocally protects Americans digital privacy rights. Any such amendment, would need to abandon, the easily manipulated idea of probable cause.

A more robust standard should exist for violation of an individual’s digital privacy rights. I propose that a higher judicial standard known as “clear and convincing evidence,” should apply to this new constitutional amendment. It is important, to limit the abundance of litigation that would result from a new constitutional amendment to articulate a standard that is already well known. There is a significant body of law around the clear and convincing evidence standard. Because this body of law already exists, the amount of litigation resulting from the new constitutional amendment would be limited. As indicated in an earlier chapter, as recently as 2011 the United States Supreme Court unanimously upheld the concept of clear and convincing evidence. The case was a patent law case. In Microsoft Corp. v. i4i Limited Partnership. The court held that in all patent infringement cases, and accused infringer must prove that the patent is invalid by clear and convincing evidence. This is an interesting ruling because it essentially says that a business that owns a patent has a substantial court protected constitutionally protected right to that property, and that anyone who wants to invalidate that protected right, must
do so with clear and convincing evidence. Why should the digital privacy rights of everyday citizens, businesses, and other entities, be afforded any less protection? A digital privacy amendment will assure that the rights of everyday citizens to be protected in their electronic security, should be at least as great as a corporation’s right to be protected from patent infringers.

A proposed digital privacy amendment would read as follows:

The right to digital privacy shall be vigorously protected. Anyone or any entity that collects personal data must protect the data from misuse. Personal data shall not be sold or disseminated without permission of the individual or entity affected. Governments (federal or state) may not access personal electronic data, without a warrant issued by a competent court. For a court to issue a warrant allowing access to electronic data, the party seeking the warrant shall demonstrate by “clear and convincing evidence” that the party whose information is sought has committed or is committing a crime. In circumstances where a government entity (state or federal) seeks to compel a service provider to disclose a user’s private communications or documents, in any form, a warrant shall be obtained based on “clear and convincing evidence.” Any government entity (state or federal) that seeks to track the location of any mobile communication device or obtain transactional data, by means of any communications technology, shall first obtain a warrant issued upon “clear and convincing evidence” of the commission of a crime by the individual whose information is sought. Individuals, business entities and other organizations are also prohibited from violating digital privacy rights of any individual or entity. Violations of the provisions of this amendment shall result in severe penalties as established by Congress. It shall also be a felony to intentionally violate this
amendment. Congress may enact other criminal and civil sanctions to effectuate the goals of this amendment.

This solution would certainly solve much of the problem. Raising the standard to “Clear and Convincing” evidence would establish a very high bar to government encroachment of digital privacy rights. Assuring that businesses and individuals face certain punishment by the loss of finances or the loss of liberty would serve as a strong deterrent to violation of digital privacy rights. The problem with the solution of course is the extreme difficulty in which it takes to amend the Constitution. As mentioned earlier the 27th amendment took 203 years to be ratified by the states. The equal rights amendment, as simple and straightforward as it was, has never been ratified although it came close. However much time it takes to pass such an amendment would be worth the effort.

Another solution to the problem of digital privacy rights in America, is the most practical solution. Congress could, with the president’s approval, simply pass statutory language almost identical to the digital privacy amendment language above. Obviously, a statutory scheme should include a much more robust indication of penalties for violations and potential fines. A statutory scheme would be more comprehensive. But the salient feature, would be the adoption of a “clear and convincing” standard for the issuance of warrants, and/or the access of private data. Many would argue that such a standard would hamper law enforcement. This is doubtful in that law enforcement has always shown a resilient capability to find and prosecute criminals. Although the United States makes up approximately 4% of the world’s population, we incarcerate 25% of the world’s prisoners. The argument that says that law enforcement would be hampered has no
support in the evidentiary record. More importantly, fragile digital privacy rights of American citizens would be adequately protected.

One of the things anyone you meet at any prison or jail will tell you, is that the loss of privacy is a horrendous loss. When incarcerated, you do not have the ability to keep others from watching you, tracking you, and even searching you. The space that you live in is open and subject to inspection and unlimited searches and seizures.

Without privacy there can be no liberty, liberty and privacy are intricately tied together. Digital privacy is the most important type of privacy because conceivable much more is at stake. Digital privacy also 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 an important right to simply not be bothered. Without digital privacy this right cannot exist. Digital privacy must be protected for liberty to thrive.
LIST OF REFERENCES
LIST OF REFERENCES


Markus D. Dubber, the Comparative History and Theory of Corporate Criminal Liability, 16 New Crim. L. Rev 203 (2013).


Other Sources

1 Cong. Ch. 15, May 31, 1790, 1 Stat. 124)

Act of January 6, 1897, 54 Cong. Ch. 4, January 6, 1897, 29 Stat. 481

Copyright Act of 1909, §28, 35 Stat. 1075


Digital Millennium Copyright Act, 17 U.S.C.A §1204


35 U.S.C. §101-112

Leahy-Smith America Invents Act (2011), Pub L. No. 112-29, 125 Stat. 284


35 U.S.C. §27A

Digitaldueprocess.com

Info.whistleblower.org


www.westlaw.com

https://www.lexisnexis.com

Harvard Law Review, 4, 5, 1890, pp. 193-220


Retrieved from https://www.law.cornell.edu/wex/fourth_amendment.

Aguilar v. Tex., 378 U.S. 108 (U.S. 1964)


U.S. Const. art. 1, § 8, cl. 6.)
VITA

FREDERICK GREENE

PERSONAL DATA

Address:
ENMU 2001, 1500 S Ave K
Portales, NM 88130
Office 575-562-2033
frederick.greene@enmu.edu
professorfredgreene@gmail.com

EDUCATION

2016  Doctor of Philosophy (Ph.D.) in Technology*
      Purdue Polytechnic Institute at Purdue University
      West Lafayette, Indiana 47907
      Department of Technology Leadership & Innovation
      Major Focus: Organizational Leadership, Innovation and Entrepreneurship.
      Cognate completed at Purdue Krannert School of Management. Cognate Areas:
      Sustainability Leadership and Management. Dissertation: “Protecting Privacy
      Rights of American Citizens.” Degree conferred expected August 6, 2016

2014  Master of Laws (LL.M.) in Intellectual Property Law
      Indiana University School of Law—Indianapolis, Indiana 46202
      Research Focus: Historical Anomalies between Patents and Copyrights.
      Degree conferred: December 22, 2014

1987  Juris Doctor
      University of Notre Dame Law School
      Notre Dame, Indiana 45665.

1986  Conccannon Program of International Law (Summer Semester),
      Completed classes in various areas of International Law.
1984  **Bachelor of Science in Business Administration**  
*Kentucky State University*, Frankfort, Kentucky 40601.

**EMPLOYMENT**

2013-PRESENT  
**Associate Professor of Business Law and Management**  
Eastern New Mexico University, College of Business  
Portales, New Mexico 88130

Responsible for teaching Business Law I and II, Comparative Law, International Law, Leadership and Organizational Change, Law and Ethics for MBA Students, Research Methods for MBA Students. Also engaged in advisement, service and research. Utilized Face to Face and online delivery.

**Professional Online Course Delivery:**  
Proficient and experienced at Online course delivery including all aspects of Blackboard, Mediasite, Collaborate, Wimba, and various other online video and content delivery methods and practices.

December, 2015  
**Guest Lecturer and Visiting Scholar**  
Programa De Pos-Graduacao.  
Unisul University, Florianopolis, Brazil.  
Team taught a one week class on Business Ethics at university in Brazil, Second week engaged as a visiting scholar with faculty.

2011-2013  
**Graduate Teaching Assistant/ Lecture Instructor**  
Purdue University College of Technology, West Lafayette, IN  
Responsible for teaching two large lectures each semester of OLS 252 Human Relations in Organization (185-220 Students in each section).

2002-2013  
**Associate/Assistant Professor of Sociology & Criminal Justice**  
Saint Joseph’s College, Department of Sociology,  
Rensselaer, Indiana 47978  
Responsible for teaching, student advising, and college service.  
Promoted to Associate Professor and granted Tenure by the Board of Trustees on February 9, 2007 effective 8/20/2007.

2005-2006

Chair, Saint Joseph’s College Faculty Assembly
Elected position as chief administrator of faculty governing body. Responsibilities include faculty committee assignments, determination of all business to go before the assembly, act as liaison between the administration and faculty, and to function as the chief administrative officer of the Faculty Assembly.

2001-2002

Assistant Professor of Management.
Wilberforce University, Business and Economics Division, Wilberforce, Ohio 45384-1001.
Introduction to Business, Business Law, Business Policy and Administration, and Quantitative Business Methods.

1997-2000

Assistant Dean for Student Affairs & Director of the Academic Excellence Program
The University of Mississippi
School of Law. University, Mississippi 38677
Directed the Office of Student Affairs and counseled students concerning housing, financial aid, admissions and law school success. Supervised and advised all law school organizations. Counseled students on academic probation and developed individual plans for success.

Member of the Admissions Committee responsible for identifying, and recruiting qualified non-traditional, and minority students.
Designed and implemented outreach programs for high school students statewide. Successfully operated recruitment programs statewide.

Responsible for implementing and coordinating diversity related matters and developed policies and procedures for Americans With Disabilities Act (ADA) compliance. Responsible for planning and coordinating Law School Commencement and Law School participation in University Programs.

Directed the Academic Excellence Program and designed creative and successful programs to address the needs of first year law students to assure their academic success, including orientation for all first year students. Instructed weekly classes, and supervised ten Teaching Assistants, training them how to effectively teach law students.
1988-1997

**Managing Partner and Attorney at Law,**
Greene & Associates, P.C.
Lansing, Michigan 48917
Managed law firm, supervised Attorneys, Paralegals, and other support staff, and practiced law throughout Michigan, and on a case-by-case basis in Indiana, Ohio, and Wisconsin.
Experienced lead litigator for firm. Also counseled, advised, and represented clients in civil rights litigation, labor law issues, family law matters, and criminal law matters in state and federal court. Actively engaged in court appearances and conducted complex and extensive trials on a regular basis.

1989-1996

**Adjunct Professor,**
Lansing Community College,
Lansing, Michigan 48933.

**SCHOLARSHIP**

**Vanquishing Our Golden Calves.** Yom HaShoah Ceremony Holocaust Days of Remembrance Cannon Air Force Base, Clovis, New Mexico (April 16, 2015)

**Reaching For the Stars: How Graduate School Expands Opportunities**
Eastern New Mexico University Campus-Wide Presentation (February 17, 2015)

**America Today: Situational Awareness 50 Years Later***
Grand Finale Black History Month Program at Eastern New Mexico University. (February, 2014) *Voted Program of the Year Award.*

**Is Academic Electronic Communications at Risk?** New Mexico Technology in Education Conference (NMTIE), Albuquerque, NM (November, 2013)

**Cyberspace Safety and Technology Transfer.** VACCINE Agency, Department of Homeland Security. HS-STEM Luncheon, Purdue University. (November, 2011)

**Preparing Your Child for College: Things You Need to Know.**
Science Bound Program Luncheon for Parents, Purdue University. (2008)

**Remembering the Past, While Building For the Future.** Black Heritage Month Luncheon, Columbus Air Force Base, Columbus, Mississippi. (February 18, 1998).


COMMITTEE SERVICE


PROFESSIONAL AFFILIATIONS

The State Bar of Michigan, 1988-Present
Licensed Life Insurance Agent, Indiana and Ohio, 2003-2010
(Life, Casualty and Variable Products)
United States District Court, Eastern and Western District of Michigan, 1988-Present
United States Court of Appeals for the Sixth Circuit, 1992-Present