A Critical Analysis of Surveillance Law and Privacy Rights in a Time of Changing Technology: A Comparative Case Study of the United States and Germany

By Alexandra Tsakopoulos

CEU eTD Collection

M.A. Long Thesis
Central European University
1051 Budapest, Nador utca 9
Hungary

Executive Summary

Surveillance law may be defined as the law that governs the interception of transmissions and communications of individuals.[1] As technology rapidly develops, surveillance law becomes increasingly pertinent. This thesis focuses on the adaptation of surveillance law to include technological advances, in particular, the Internet. It addresses two jurisdictions, namely: the United States and Germany. To provide context for further analysis, it examines the histories of each respective country, looking at governmental involvement in the development of the radio. This thesis then analyzes each government's current approach to the Internet. Finally, it details both American and German surveillance law, and examines the breadth of privacy rights in each jurisdiction. This thesis seeks to determine which approach provides the most effective safeguards in protecting personal privacy, and how.

Upon analyzing the above information, this thesis concludes that German law provides the most effective safeguards in protecting the personal privacy of its citizens. It is through Germany's groundbreaking laws of surveillance and the Internet that there is greater protection of this privacy. The United States is currently addressing issues such as privacy, technology and surveillance in court, and would be wise to follow Germany's example.

This thesis discusses two jurisdictions, which simply grazes the surface of worldwide surveillance law. In addition, as technology changes by the nanosecond, the findings herein will most likely be outdated soon. Despite these limitations, this thesis emphasizes that upon examining the policy of these jurisdictions, we may learn about achieving a proper balance between a government's need to implement surveillance methods and an individual right to privacy.

[1] NCSL National Conference of State Legislatures: Electronic Surveillance Laws. Accessed 23 March, 2011.
http://www.ncsl.org/default.aspx?tabid=13492

CEU eTD Collection

CEU eTD Collection

TABLE OF CONTENTS

CEU eTD Collection

CEU eTD Collection

I. Introduction

The word *surveillance* often conjures up images of a watchful eye. The term itself means: "close watch kept over someone or something,"[2] and is manifested in a range of ways, from video cameras to wiretapping to panopticism. And over time, as methods of communication have developed from whispering amongst the eaves to the advent of the telephone and the proliferation of the Internet, a new concept of surveillance has emerged: electronic surveillance. According to Black's law dictionary, electronic surveillance is defined as a method that: "employs sophisticated electronic equipment to intercept private conversations or observe conduct that is meant to be private."[3] This includes high-tech apparatuses such as "small radio transmitters or 'bugs' to listen in on telephone or in-person conversations."[4]

Today, it is not just the methods of surveillance that are electronic, but also the platforms for communication as a whole. *Email*, formally known as 'electronic mail', is our modern method of communication. It is described as "a means or system for transmitting messages electronically (as between computers on a network),"[5] and is used by over 1.88 billion people worldwide.[6] With the advent of the Internet, most communication has shifted to the realm of computers; nearly 107 trillion emails were sent via the Internet in the year 2010.[7]

CEU eTD Collection

[2] Merriam-Webster Dictionary: Surveillance. Accessed 24 March 2011 http://www.merriam-webster.com/dictionary/surveillance
[3] Black's Law Dictionary: Electronic Surveillance
[4] *Ibid*
[5] Merriam-Webster Dictionary: Surveillance. Accessed 24 March 2011 http://www.merriam-webster.com/dictionary/email
[6] Royal Pingdom: Internet 2010 in numbers. Accessed 24 March 2011 at 2:40 pm http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/
[7] *Ibid*

With all of this written information bouncing between computers and networks, concerns of privacy and safety of information rise to the fore. Where does the information go? Can others tap into email conversations? And how is ones privacy ensured? As such, much has been speculated about safety. As a remedy, these methods of electronic surveillance often have strict judicial guidelines. As Black's definition acknowledges: "Many of these sophisticated forms of surveillance require a search warrant because they violate a person's reasonable expectation of privacy. This area of law is in a constant state of flux as courts interpret the use of new technologies."[8]

In a seminal article published in the Harvard Law Review in 1890, Justice Louis Brandeis and Justice Samuel Warren of the United States discuss an evolving legal system. They detail the reality of ever-changing norms: "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society."[9] Justice Brandeis and Justice Warren recognize that the law must change in order to fit a growing society; that the law needs to develop. They illustrate changes of the time: "[…] in very early times, the law gave a remedy only for physical interference with life and property […] Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened […] to comprise […] the intangible, as well as tangible."[10] Over a century later, this approach still holds true. With ever-changing technological platforms, concepts of law and privacy have evolved alongside one another.

The rise of the Internet and new mediums of communication raises questions, such as: are technological advances regulated and codified to ensure protection, and if so, how? Are laws outmoded and thus unable to apply to new technology? What is a government's role in

CEU eTD Collection

[8] Black's Law Dictionary: Electronic Surveillance
[9] Samuel D Warren & Louis D. Brandeis, The Right of Privacy, 4 Harv. L. Rev. 193 (1890)
[10] *Ibid*

assuring this protection of privacy, and does it breach this protection under potentially outdated surveillance law? This thesis seeks to answer these questions in respect to each jurisdiction, and to compare and analyze the results in order to continue the search for an adequate balance between governmental surveillance mechanisms and the protection of personal privacy.

CEU eTD Collection

II. Literature Review

Much research has been done on the topics of surveillance law, changing technologies and a right to privacy, including different combinations of the three. Bringing together this trio nicely, the Markle Foundation has funded numerous works on the subject matter. The Markle Foundation is an organization that: "focuses on how best to mobilize information and technology to advance national security while protecting civil liberties."[11] Founded in 1927, the foundation has an impressive history of action. In its archives it boasts a wide variety of public policy research papers, along with information on past initiatives. It focuses on the "intersection of policy and information technology,"[12] and addresses topics such as Internet governance. This source allows access to a wide range of position papers. For example, the third report from the Markle Foundation Task Force on National Security in the Information Age includes a chapter called *Mobilizing Information to Prevent Terrorism while Protecting Civil Liberties.* This article proposes a mechanism of sharing between national, statewide and local governmental bodies, along with private industry, in order to help strike a balance between privacy rights and national security.[13] It states: "The President should ensure that we protect privacy and civil liberties as we achieve security. Security and liberty are dual core obligations and goals, not competing rivals."[14] This is an estimable sentiment.

CEU eTD Collection

[11] The Markle Foundation: Advancing Health and National Security in a Connected World. Accessed 9 November 2011
http://www.markle.org/our-story
[12] *Ibid*
[13] Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment. Third Report of the Markle Foundation Task Force, Page 18
[14] Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment. Third Report of the Markle Foundation Task Force, Page 26

However, the proposal seems to overreach in its estimates of feasibility. It calls on the President to: "issue guidelines that rigorously protect privacy and civil liberties […]."[15] While this is a commendable goal, its proposal for implementation seems impractical. The report lists *trust* as a crucial component to implementing the mechanism for information sharing: "The public must trust that information sharing is effective, appropriate, and legal. Lack of public confidence that systems are functioning within clearly established guidelines can lead to the termination of essential government initiatives."[16] This seems credible. But much of the proposed information sharing mechanisms will be private: "The details of operations and the practical application of rules, will of course need to be secret […]."[17] While the goals of the Markle Foundation's proposal seem desirable, the secretive nature of its processes may raise questions. This concealment may lead to too much governmental control, and thus a potential for abuse. And the public will likely be wary of handing over power and trust to clandestine operations. Thus, the proposal may not be feasible.

The Stanford Technology Law Review also provides relevant research. A piece by Paul Ohm entitled *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*[18] deconstructs the Fourth Amendment and analyzes its application over time. It provides a detailed look into the evolution of what the government determines as "property" and "possession." Ohm recognizes a tendency towards a "physical property-centric model of dispossession."[19] This analysis raises questions addressed in this thesis: Is current U.S. law, such as the Fourth Amendment, adequate when applied to new technology?

CEU eTD Collection

[15] *Ibid* page 11
[16] *Ibid* page 24
[17] *Ibid* page 22
[18] Paul Ohm. *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*. 2008 STAN. TECH. L. REV. 2 Accessed April 2011 http://stlr.stanford.edu/pdf/ohm-olmsteadian-seizure-clause.pdf
[19] Paul Ohm. *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*. Paragraph 14. 2008 STAN. TECH. L. REV. 2 Accessed April 2011 http://stlr.stanford.edu/pdf/ohm-olmsteadian-seizure-clause.pdf

Ohm argues no; that the property-based interpretation of the Fourth Amendment still, in part, prevails. The findings in this thesis are similar. However, in the conclusion of his piece, Ohm touches on the uncertainty of the law with regards changing technology, and the shift back towards the property-based analysis of the Fourth Amendment: "Awesome technologies have arisen in the meantime that none of the justices in 1967, much less in 1928, could have foreseen. Modern surveillance technologies can duplicate without revelation. Courts might hold that these tools neither search nor seize […]."[20] While at the time of Ohm's article, there may have been a shift back towards the tangible, property-centric interpretation of the Fourth Amendment, in recent developments this is not the case. Contrary to Ohm's predictions, several of the latest judgments have revealed a move towards a more intangible approach. This will be discussed further in the body of this thesis.

Alisdair A. Gillespie has written an article that is particularly linked to this thesis. Entitled *Regulation of Internet Surveillance*, the article was published in the European Human Rights Law Review. The article asks similar questions as this thesis but on a much smaller scale, as it is markedly shorter. It differs in that the article addresses and assesses specific forms of online communication, delving into details of web postings, applications and software. However, it is linked to this thesis in that it explores the confines of surveillance law: "technological advances mean that it is now possible to monitor persons in ways that would not necessarily be included within traditional understandings of surveillance."[21] As in this thesis, the article recognizes the discrepancy between surveillance law and new technology. Additionally, it attempts to situate web-surveillance within the already established regulatory framework. Gillespie concludes that online surveillance needs parameters, as: "The regulation of surveillance exists to ensure that the state only interferes

[20] *Ibid* Paragraph 7
[21] Alisdair Gillespie. Regulation of Internet Surveillance. Section: Defining Surveillance. European Human Rights Law Review, Issue 4 2009. Pg 552-565

CEU eTD Collection

with a person's private life when necessary."[22] While the article's conclusion is similar to that of this thesis, the means of achieving it are different. Gillespie suggests that: "The modern telecommunications era has meant that the boundary between a person's offline and online lives is blurred at best, and it is important that the law recognises the right to personal integrity online, and it is incumbent on law enforcement agencies and the relevant inspecting commissioners to ensure that this is followed through in practice."[23] Gillespie calls for law enforcement to take action in the application of surveillance law, to ensure that rights are protected. This thesis, however, argues that the law itself must be updated, and it is not only up to law enforcement agencies and inspecting commissioners, but lawmakers and the judiciary as well.

It must be noted that the process of surveillance has many benefits, and may be adequately justifiable. Stanford University addresses this point: "For some cases in the clash between privacy and advancing technologies, it is possible to make a compelling argument for overriding the privacy intrusions. Drug and alcohol tests for airline pilots on the job seem completely justifiable in the name of public safety, for example."[24] Further, there are circumstances, such as insider trading and terrorism, which may affect a great number of people, and may be deemed reasonable reasons to conduct surveillance. However, there needs to be a balance between personal privacy and national security: "With the development of new and more sophisticated technology, recent work on privacy is examining the ways in which respect for privacy can be balanced with justifiable uses of emerging technology."[25]

CEU eTD Collection

[22] Alisdair Gillespie. Regulation of Internet Surveillance. Section: Conclusion. European Human Rights Law Review, Issue 4 2009. Pg 552-565
[23] *Ibid*
[24] Stanford Encyclopedia of Philosophy, Entry on "Privacy". First published Tue May 14, 2002; substantive revision Mon Sep 18, 2006. Accessed September 2011. http://plato.stanford.edu/entries/privacy/
[25] *Ibid*

This issue will be addressed below, as both the United States and Germany have circumstances in which surveillance is deemed justifiable.

This thesis refers to surveillance law as "adequate" or "inadequate." This body of work values robust civil rights protection. What constitutes adequacy in this thesis is a strong respect for a right to privacy, one that is respected even with the governmental need for surveillance law.

As the Internet is constantly changing, many questions remain unaddressed or have yet to be updated. Though there is much literature on changes in surveillance law, it is generally not current. For example, Juri Stratford, a government specialist at UC Davis, writes about policy changes and regulation in a briefing entitled "Internet Surveillance: Recent U.S. Developments." However, this piece dates back to 2003, which can be considered dated from our current standpoint. Much has changed in American policy since then. Because of its timeliness, this thesis will provide a fresh standpoint on surveillance law and new technology.

This swift process of aging is a perennial problem of technology and regulation. And the aging process will affect this thesis as well; technology changes so rapidly that this account will not be current for long. After these findings herein, much will continue to change. For example, in the United States, the Supreme Court is currently reviewing the application of the Fourth Amendment to new technology in the appeal case *United States v. Jones*. This will make a profound difference in the field of surveillance law. As cited by the New York Times, law professor Susan Freiwald highlights the importance of the case: "The Jones case requires the Supreme Court to decide whether modern technology has turned law enforcement into Big Brother, able to monitor and record every move we make […]."[26] As

CEU eTD Collection

[26] Adam Liptak, *Court Case Asks if Big Brother is Spelled GPS*. The New York Times Online, 10 September 2011. Accessed October 2011. http://www.nytimes.com/2011/09/11/us/11gps.html?_r=2&hp

such, there are changes occurring every day, and this thesis may be dated even before it is completed.

Nevertheless, this thesis will provide valuable insight into the policies of several governments and their attempts to codify surveillance methods to adapt to changes in technology. This thesis will give a historical snapshot of governmental policy. In addition, it may be useful, as other, less developed jurisdictions will one day cope with similar issues of providing adequate legal frameworks for new technology.

In addition, this thesis adopts a distinctive approach to the topic. Technological terms tend to prevent those without specialized computer proficiency from engaging in relevant debates. Here, this is not the case. This paper will be approached from a unique perspective, one that will allow accessibility to those without a particular computer-based understanding. Written without using technical vocabulary in the field of computer science, this thesis will be understandable to the everyday reader.

This thesis focuses on the approaches different governments take to the codification of surveillance law in a changing electronic environment. Chapter I sets forth a brief history of government regulation of media technologies in each country. Firstly, each government's history with the radio is presented as a comparative form of new technology. By looking at approaches of the past, insight may be gained into current governmental relations to changing technology. Next, the history of each government's relationship to the rise of the Internet is presented and explored. The focus then shifts to the specificities of surveillance law. In Chapter II, each government's approach to surveillance law is detailed. This is presented in order to evaluate the laws currently in place. Chapter III introduces the topic of privacy. It seeks to limit the scope of this topic to privacy as a right, looking directly to informational privacy. Then, the right to privacy is evaluated and compared in the respective jurisdictions. Chapter IV allows for a comprehensive comparison of the adequacy of the laws in place in

CEU eTD Collection

America and Germany, with respect to protecting the right to privacy. This thesis also aims to offer insight into striking a proper balance between surveillance law and privacy rights, highlighting positives of and downsides to American and German law. Needs are highlighted, and a recommendation is made to allow for adequate protection of privacy.

There are other models, viewpoints, and judgments when analyzing the adequacy of surveillance law. Various sources may find that robust protection, such as laws enacted in order to guard against access to indecent materials by minors, is too extreme, and that these laws may hinder other rights, such as free speech.[27] And some sources may find that, in times of war, national security outweighs a right to privacy. It is clear that there are different opinions as to the balancing of rights. This thesis takes a distinct view, one that will be detailed below.

While other methods of analyzing surveillance law may be important in understanding the complexity of the law, this thesis provides a narrow scope and comparative structure where much insight may be gleaned. This thesis studies the history of regulation, analyzes past and present laws, and determines the breadth of privacy rights in two jurisdictions, culminating in a reasoned opinion on the adequacy of current legal structures and propositions for the future.

CEU eTD Collection

Chapter I: Governmental Regulation

This chapter explores the history of governmental involvement in technology in the United States and Germany, looking particularly at the advent of the radio, in order to scrutinize different approaches to the regulation of technology. Looking at the complex connection between governments and technology sets the stage for deeper analysis of

[27] *Reno v. ACLU*, Brief for the Appellees. October 1996, Supreme Court of the United States. Accessed October 2011 http://epic.org/free_speech/cda/lawsuit/sup_ct_brief.html

governmental use of technology for surveillance. This chapter also examines both governments' position to the Internet, and seeks to highlight various complexities that arise with these different relationships.

a. The United States

i. History of Governmental Regulation of the Radio

Governmental influence on the development of technology in the United States has a history; it spans across different media during the nascent, and even later stages of various communications. One may find interesting parallels in efforts taken to create protected and secure media technologies, such as in the development of the radio. In the early 20th century, the United States Navy, as well as other agencies such as Department of Agriculture, helped to popularize the use of radio technology through the implementation of wireless radio contact.[28] Though radio use was widely adopted amongst government agencies, it remained de-centralized. President Theodore Roosevelt established an ad hoc panel in order to create a forum to discuss the government's role in the growth of radio.[29] A main purpose of the board was to encourage the centralization of radio control for governmental agencies, allowing for easier communication and oversight.[30] Subsequently, in 1911, the ad hoc board apportioned the majority of regulatory control of the radio to the U.S. Navy.[31]

In the meantime, an unregulated system allowed for the proliferation and public popularity of the radio. While governmental agencies used radio for naval communications and the like, many people saw the radio as a pseudo telegraph and adopted it as a means for

CEU eTD Collection

[28] White, Thomas. United States Early Radio History. Early Government Regulation: http://earlyradiohistory.us/sec007.htm
[29] *Ibid*
[30] White, Thomas. United States Early Radio History. Early Government Regulation: 1904 Roosevelt Board. Accessed 30 November, 2010. http://earlyradiohistory.us/sec023.htm
[31] *Ibid*

cheap, wireless communication in communities.[32] Along with the new method came concerns of discretion, as access to the wireless radio network was not guarded, and "anyone with a suitable receiver could 'listen in' to wireless."[33] However, this individual communications network with scant privacy protection morphed into a system that allowed multiple listeners to tune into specialized programs for the purpose of entertainment.[34] By the early 1920s, radio's popularity swelled: "[it] was becoming a widespread craze across the country as hundreds of stations squeezed on the air using the then available handful of frequencies." [35]

As the number of commercial stations and laymen listeners rose, the government adopted a more stringent approach in its regulation of the radio. In the early1920s, "[…] there was almost no government regulation—only a license for the asking and no enforcement power."[36] But in 1929, the President shifted power away from the U.S. Navy and created a distinct government body to regulate and monitor the media: the Federal Radio Commission (FRC). The FRC "was tasked with clearing up the interference on the air, and within a year or two had largely succeeded."[37] And subsequently, in 1934, Congress created the Federal Communications Commission (FCC) to replace the FRC.[38] The FCC remains a U.S governmental agency to this day, monitoring, among other media, the radio.

---

[32] The Radio and Television Museum. Gallery 1: Wireless Beginnings. Accessed 29 November 2010
http://radiohistory.org/?page_id=28
[33] *Ibid*
[34] *Ibid*
[35] *Ibid*
[36] The Radio and Television Museum Gallery 2: Birth of Broadcasting. Accessed 29 November 2010
http://radiohistory.org/?page_id=27
[37] White, Thomas. United States Early Radio History. Early Government Regulation: 1904 Roosevelt Board. Accessed 30 November, 2010.
http://earlyradiohistory.us/sec023.htm
[38] The Radio and Television Museum Gallery 3: Radio Comes of Age. Accessed 29 November 2010
http://radiohistory.org/?page_id=29

CEU eTD Collection

ii. America's Approach to the Internet

Similar to the radio, the Internet began as a military project. As defined by the Supreme Court of the United States, the Internet is "an international network of interconnected computers."[39] This network began as a military program in 1969 entitled 'ARPANET,' an acronym for: the Advanced Research Projects Agency Network.[40] ARPANET was created in the context of the Cold War and sought to allow military-operated computers, as well as "universities conducting defense-related research, to communicate with one another by redundant channels even if some portions of the network were damaged in a war."[41] To completely destroy communication systems and obliterate the necessity of contact would be detrimental to a nation at war. ARPANET provided the opportunity for decentralized methods of communication in order to assure, in threatened times, that at least some contact could be conducted. Renowned communications professor Wolfgang Kleinwächter describes the advent of the Internet as creating something of a paperless plutonium, namely: "the desire to create a mechanism that is nearly impossible to destroy."[42]

Though similar to other media in its military beginning, the development of the Internet is and has been unique. In the Supreme Court case of *Janet Reno v. ACLU* (1997), the first United States Supreme Court case to consider the regulation of content on the Internet, the Court found the Internet to be starkly different from media such as the radio for three substantial reasons. Firstly, the Internet itself is not deemed to be as "invasive" as other

CEU eTD Collection

[39] Janet Reno, Attorney General of the United States, et l. v. American Civil Liberties Union et al. 521 US 844, 138 L Ed 2d 874, 117 S Ct 2329 [No. 96-511]. Pg 884
[40] *Ibid*
[41] *Ibid*
[42] Professor Wolfgang Kleinwaechter. *Challenges of Internet Governance: New multistakeholder models for global policy development*. Lecture, Attended 26 October, 2010.

media such as television or radio.[43] On the radio, a listener may turn on the apparatus and be confronted instantaneously with something he or she does not intend to be exposed. But with the Internet, one must take a more proactive approach to receive the content contained within; it " […] requires a series of affirmative steps more deliberate and directed than merely turning a dial."[44] As such, the Internet is considered intrinsically less invasive than other media outlets.

In addition, unlike radio and television, the Internet is not considered to be a "scarce expressive commodity," [45] as it is widely available to any and all users. Regarding the radio, there are a limited number of frequencies available for use. In addition, one must acquire a broadcasting license from the FCC in order to have and use a station. Contrastingly, the Internet allows for voices to be heard through an unprecedented amount of user access with no license requirement and very few prerequisites. In the 1990s, the Supreme Court of the United States supported this claim, stating that " [the Internet] provides relatively unlimited, low-cost capacity for communication of all kinds. […] Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox."[46] And it has grown beyond what many had predicted. In the 1990s, the Supreme Court cited a governmental estimation: the number of Internet users would grow to 200 million by the year 1999.[47] This statistic has climbed dramatically. Close to a decade later, the Internet now has over 1 billion users worldwide.[48] To assess the magnitude of these

CEU eTD Collection

[43] Janet Reno, Attorney General of the United States, et al. v. American Civil Liberties Union et al. 521 US 844, 138 L Ed 2d 874, 117 S Ct 2329 [No. 96-511]. Pg 887
[44] *Ibid*
[45] *Ibid*
[46] Janet Reno, Attorney General of the United States, et al. v. American Civil Liberties Union et al. 521 US 844, 138 L Ed 2d 874, 117 S Ct 2329 [No. 96-511]. Pg 897
[47] *Ibid*
[48] Internet World Statistics: *Usage and Population Statistics.* Accessed November 2010 http://www.internetworldstats.com/stats.htm

numbers, one may consider that 1 billion seconds is nearly 32 years.[49] With the broadest usership imaginable, reaching worldwide from Azerbaijan to Antarctica, this media is different from the rest.

And finally, the Supreme Court distinguished the Internet from other media because it is not subject to any federal regulation.[50] Though it began as largely bonded with the government, the Internet is now divorced from direct federal drive and is primarily powered by individuals. In the *Reno v. ACLU* decision, the Court emphasized the importance of this separation. The Court looked to precedent, finding that regulation of the Internet has not existed: "Neither before nor after the enactment of the [Communications Decency Act] have the vast democratic forums of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry."[51] In addition, by citing Judge Dalzell, the Supreme Court found that not only has government regulation not existed, but the Internet should be protected from it: "the Internet – as the most participatory form of mass speech yet developed, is entitled to the highest protection from governmental intrusion."[52] As of November 2011, the Internet is not strictly regulated in the United States.

b. Germany

i. History of Governmental Regulation of the Radio

In the midst of the Second World War, Germany's regulatory control of the radio was draconian. Many restrictions were placed on what particular airwaves could be accessed by

CEU eTD Collection

[49] Wikipedia: One Billion, number. Accessed 27 November 2010 http://en.wikipedia.org/wiki/1000000000_(number)
[50] Janet Reno, Attorney General of the United States, et l. v. American Civil Liberties Union et al. 521 US 844, 138 L Ed 2d 874, 117 S Ct 2329 [No. 96-511]. Pg 876
[51] *Ibid* Pg 895-896
[52] *Ibid* Pg 892

the public.[53] In particular, the German government issued a list of frequencies to which citizens were allowed to listen; there were dire consequences for disobeying this: "Listening to unauthorized Radio stations was a criminal offence […] and [could result in] capital punishment."[54] Further, foreign radio was banned, and radio programs that encouraged support of the Nazi regime were promoted. This is evidenced in a propaganda poster of the 1940s that states (in translation): "All Germany hears the Führer on the People's Receiver."[55] In addition, in order to promote the ideals of the Nazi regime, the government created its own radio receiver of a lesser cost to encourage a wider audience.[56] The German government amassed a strong grip on the radio.

But this shifted after the war. The political changes of the country influenced the progression of its media.[57] While the East German government retained much control over the media, a more liberal West Germany allowed for more open airwaves. The Museum of Broadcast Communications emphasizes this discrepancy: "Throughout most of the developments in West Germany, television broadcasting in the German Democratic Republic (East Germany) remained under government control and served as a propaganda instrument for socialistic ideals."[58] For example, the program *Aktuelle Kamera* (Current Camera) was under the limited aegis of the government.[59] And "Der Schwarze Kanal (The Black Channel)

[53] Radio Mentor: Hoerverbot 1941. *List of Authorized Broadcasting Stations.* Accessed 13 October, 2011
http://aobauer.home.xs4all.nl/hoerverbot_1941.htm
[54] Radio Mentor: Diese Sender des Mittel- und Langwellenbereiches dürfen in Deutschland abgehört werden. Accessed 13 October 2011
http://aobauer.home.xs4all.nl/hoerverbot_1941.htm
[55] German Propaganda Archive: the German Federal Archives. Accessed 13 October 2011
http://www.calvin.edu/academic/cas/gpa/posters2.htm
[56] *Ibid*
[57] Radio Mentor: Diese Sender des Mittel- und Langwellenbereiches dürfen in Deutschland abgehört werden. Accessed 13 October 2011
http://aobauer.home.xs4all.nl/hoerverbot_1941.htm
[58] The Museum of Broadcast Communications – GERMANY. Accessed 18 November 2011
http://www.museum.tv/eotvsection.php?entrycode=germany
[59] *Ibid*

CEU eTD Collection

[…] reacted directly to West German news coverage with propaganda material."[60] The difference between East and West German broadcasting was growing.

However, the differences in broadcasting material between East and West Germany began to diminish. After the unification of East and West Germany, the German Democratic Republic and the Federal Republic, governmental control of the radio became decentralized and organized on a state level: "After years of strong polarisation from the 1950s to the 1970s, media policy is now again based on a broad consensus between the Länder."[61] This was implemented in order to thwart attempts at widespread manipulation. The decentralization of broadcasting systems allowed for more diversity in opinion: "Radio and television are administered in a decentralized fashion as prescribed in the Basic Law. The intent behind the pattern of regional decentralization is to prevent the exploitation of the media by a strong national government, as had happened under the Nazi dictatorship."[62] This regulation remains on the state level. In particular, state media authorities are responsible for: "licensing and controlling as well as structuring and promoting commercial radio and television in Germany."[63]

While most regulation is conducted within the state, the states must cooperate on a national level as well: "For a great number of issues relating to broadcasting, [there are] rules applicable across Germany as a whole […] The 14 state media authorities therefore cooperate in different decision-taking councils and commissions coordinating and aligning matters on a national level."[64] The Interstate Treaty on Broadcasting and Telemedia outlines this German

CEU eTD Collection

[60] *Ibid*
[61] European Journalism Centre – Media Landscape, Germany. 5.3 Regulatory Authority. Accessed 13 October 2011 http://www.ejc.net/media_landscape/article/germany/
[62] *Ibid*
[63] Die Midienanstalten. Accessed October 12, 2011 http://www.die-medienanstalten.de/home.html
[64] Die Midienanstalten. Accessed October 12, 2011 http://www.die-medienanstalten.de/home.html

law. Specifically, to illustrate interstate cooperation, the Treaty demands that: "It is for the state media authorities to cooperate more closely in the interest of equal treatment of commercial broadcasters and the improved implementation of decisions."[65] Germany has a strong system of state and nationwide regulation in place.

ii. Germany's Approach to the Internet

Germany spearheaded a legal approach to Internet regulation with a wide-reaching law, entitled Federal Law to Regulate the Conditions for Information and Communications Services (IuKDG). In 1997, Germany passed this first so called "'cyberlaw', holding Internet service providers (ISPs) partially responsible for providing […] public access to sites containing illegal content, such as pornography and hate speech."[66] As cited by the German Minister of Technology at the time, Juergen Ruettgers, the law was initially put into place to protect children from sordid material.[67] Article 6 of the law, the Amendment of the Law on the Dissemination of Writings Harmful to Minors, adds the phrase: "Audio and video storage mechanisms, data storage mechanisms, pictures and other representations are equivalent to writings,"[68] thus creating a law on the dissemination of *audio, video, data* etc. that is harmful to minors. Further, German authorities held that it was unlawful "to offer youth endangering material that glorifies violence, promotes racial hatred or bends morals."[69] This is particularly

[65] Interstate Treaty on Broadcasting and Telemedia (Interstate Broadcasting Treaty) 1 April 2010. Preamble
[66] Westfall, Joseph. Internet Blocking. Santa Clara University, Markulla Center for Applied Ethics. Accessed October 2010 http://www.scu.edu/ethics/publications/submitted/westfall/blocking.html
[67] The Los Angeles Times: *Germany Passes Internet Law Limiting Content*. From the Associated Press. 5 July, 1997. Accessed October 2011 http://articles.latimes.com/1997/jul/05/business/fi-9816
[68] Federal Law to Regulate the Conditions for Information and Communications Services (IuKDG), Article 6. Final Draft, December 20, 1996 Translation by Christopher Kuner, Esq.
[69] Edmund L. Andrews. *Germany's Efforts to Police Web are Upsetting Business*. The New York Times, Published 6 June, 1997. Accessed October 2010.

CEU eTD Collection

relevant to Germany's past. According to the law, punishable sites include those that depict "swastikas and other celebrations of Hitler's Third Reich. Such symbols have been outlawed [in Germany] since the end of World War II."[70] And the ambit of the law itself is comparatively wide reaching. Juergen Ruettgers highlighted the applicability of this protection: "That applies even to a network that knows no national borders […] The Internet is not outside the reach of the law.'"[71] [72]

A comparison to American law in the late 1990s highlights the broad reach of the German law. In 1996, the United States Congress attempted to suppress sexually explicit material on the Internet by proposing the Communications Decency Act (CDA). The CDA intended to: "prohibit Internet users from using the Internet to communicate material that, under contemporary community standards, would be deemed patently offensive to minors under the age of eighteen."[73] However, this was deemed unconstitutional by the Supreme Court, in that it treaded on the rights of the First Amendment. In the aforementioned case, the American Civil Liberties Union (ACLU) held that the CDA would be restrictive of First

---

http://www.nytimes.com/1997/06/06/business/germany-s-efforts-to-police-web-are-upsetting-business.html?scp=3&sq=germany+cyber+law&st=nyt

[70] Edmund L. Andrews. *Germany's Efforts to Police Web are Upsetting Business.* The New York Times, Published 6 June, 1997. Accessed October 2010. http://www.nytimes.com/1997/06/06/business/germany-s-efforts-to-police-web-are-upsetting-business.html?scp=3&sq=germany+cyber+law&st=nyt

[71] The Los Angeles Times: *Germany Passes Internet Law Limiting Content.* From the Associated Press. 5 July, 1997. Accessed 23 October 2010 http://articles.latimes.com/1997/jul/05/business/fi-9816

[72] The law has been put on hold during the writing of this thesis. The law had been enacted by Parliament, but remanded by the newly elected coalition government in order to further scrutinize the matter. According to a site dedicated to civil rights in Europe, after an extended trial period, "the new consensus seems to be that the law will be withdrawn through a new act of the Parliament." – 6 April 2011. Accessed September 2011 http://www.edri.org/edrigram/number9.7/germany-internet-blocking-law

[73] The United States Court of Appeals for the Third Circuit. Decision, February 2000, on the COPA. Accessed October 2011 http://www.efa.org.au/Issues/Censor/cens3.html#usa

CEU eTD Collection

Amendment Rights.[74] The ACLU stated that: "Not only does this ban unconstitutionally restrict the First Amendment rights of minors and those who communicate with them about important issues, but, because of the nature of the online medium, it essentially bans 'indecent' or 'patently offensive' speech entirely, thus impermissibly reducing the adult population to 'only what is fit for children.'"[75]

In a follow up attempt to protect children from offensive material, Congress proposed the Child Online Protection Act (COPA). Scholar Steven Merlis describes it as: "a law with the same objectives as the CDA, but with narrower construction designed to meet the constitutional concerns raised by the Supreme Court in its rejection of the CDA."[76] COPA sought to prohibit individuals from: "knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, mak[ing] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors."[77] However, the Supreme Court also struck this down. Merlis highlights the importance of First Amendment rights (in particular freedom of speech and of the press) in this particular instance: "Clearly, the Court made a point that the First Amendment will not be sacrificed even in the face of legislation designed to benefit

CEU eTD Collection

[74] Supreme Court of the United States. *Janet Reno v. American Civil Liberties Union*. Brief for the Appellees. October 1996. Accessed October 2011 http://epic.org/free_speech/cda/lawsuit/sup_ct_brief.html
[75] Supreme Court of the United States. *Janet Reno v. American Civil Liberties Union*. Brief for the Appellees. October 1996. Accessed October 2011 http://epic.org/free_speech/cda/lawsuit/sup_ct_brief.html
[76] Steven E. Merlis. Preserving Internet Expression While Protecting Our Children: Solutions Following *Ashcroft v. ACLU*. 4 Nw. J. Tech. & Intell. Prop. 117. Accessed 15 November 2011 http://www.law.northwestern.edu/journals/njtip/v4/n1/6
[77] USA Court of Appeals for the Third Circuit decision February 2000 on the COPA

America's children."[78] In America, unlike in Germany, the regulation of the Internet cannot be justified, even when considering offensive material and the nation's youth.

c. Third Party Sources: Public Opinion of Internet Regulation

Looking past the two jurisdictions, many members of the Internet community ardently support the separation between the Internet and the State. The Cyberspace Declaration of Independence boldly stakes this non-regulatory status, emphasizing that: "Governments of the Industrial world […] are not welcome. "[79] The Declaration continues, furthering and amplifying this anti-regulatory rhetoric:

> In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. […] We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.[80]

In addition, the Internet Corporation for Assigned Names and Numbers (ICANN) expresses a somewhat gentler preference for independent, supranational governance. Within ICANN, important Internet decisions are strictly made not by a concentrated government, but by people all over the world: "[ICANN] is where Internet policy is born, formed, and decided. ICANN's meetings are an integral part of the multi-stakeholder model as they provide an arena for global collaboration on important issues […] They are a testament to the bottom-up, consensus driven model that Internet Governance is based on - overseen by the world, for the

CEU eTD Collection

[78] Steven E. Merlis. Preserving Internet Expression While Protecting Our Children: Solutions Following Ashcroft v. ACLU. 4 Nw. J. Tech. & Intell. Prop. 117. Accessed 15 November 2011
http://www.law.northwestern.edu/journals/njtip/v4/n1/6
[79] Professor Wolfgang Kleinwaechter. Challenges of Internet Governance: New multistakeholder models for global policy development. Lecture, Attended 26 October, 2010.
[80] John Perry Barlow. *A Declaration of the Independence of Cyberspace*. February 8, 1996. Accessed: November 30, 2010.
http://editions-hache.com/essais/pdf/barlow1.pdf

world."[81] As indicated, many people all over the world strongly disagree with governmental efforts to control certain aspects of national Internet access. It seems, however, that some regulation must be implemented in order to promote and protect civil rights. Through complete deregulation on a national level, there is room for abuse.

Summary of Chapter I:

Chapter I gives a brief summary of the history of governmental regulation in two jurisdictions with regards to both the radio and the Internet. In America, the government had strong ties to the creation of the radio. This seems completely contradictory to its approach to the Internet, where, as of November 2011, it remains unregulated. This is because the Internet is deemed to be a very different mode of communication than the radio.

In Germany, the government also had strong ties to the nascent stages of the radio. And because of its unique history during WWII, Germany now has strict laws in place to assure that the medium cannot be monopolized by one view. As regards the Internet, Germany has spearheaded regulatory laws in order to assure its civility. In Germany, unlike in the United States, Internet content is partially regulated, specifically in relation to shielding minors from inappropriate material. In Germany, the regulation of the Internet can be justified when deemed to be protecting the nation's youth.

Finally, a public, supra-national opinion is presented in order to highlight a differing view. Various third parties vehemently oppose any national regulation of the Internet. Though the sources call upon the United States as an inhibitor of Internet freedom, their view of de-regulation lines up with much of American policy towards the Internet (or lack thereof). The third party view highlights a movement towards deregulation. It indicates a desire for independence, not the involvement of respective governments. But by supporting little to no

[81] ICANN – Internet Corporation for Assigned Names and Numbers. Last modified 13-Aug-2010. Accessed November 30, 2010. http://www.icann.org/

CEU eTD Collection

governmental regulation of the Internet, there will consequently be little to no ensured protection of certain human rights.

These developments set a foundation for further exploration into specific, national surveillance law. They highlight America's hesitancy toward Internet regulation, and Germany's more involved approach. Below we will examine how these relationships are translated into surveillance law.

Chapter II: Existing Surveillance Law

This chapter builds upon the relations established in the previous chapter. It will give an overview of current legislation that stipulates governmental monitoring of personal communications, specifically for use in criminal proceedings. It begins by outlining the bounds of the Fourth Amendment of the United States Constitution in case law. It then moves to American national legislation, giving a brief introduction to two acts that stipulate U.S. surveillance law. For Germany, an analysis of the Code of Criminal Procedure is presented, and a recent decision by the German Constitutional Court is introduced. This chapter explores the questions of: what protections do citizens have from being monitored by the government? And to what extent, and under what circumstances can each government legally monitor the email communications of its citizens?

CEU eTD Collection

a. The United States

In the United States, citizens are protected from unwarranted governmental surveillance through the Fourth Amendment of the United States Constitution in combination with assorted legislation enacted over many years. The Fourth Amendment of the United States Constitution protects against *unreasonable search and seizure*. It reads:

> 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.[82]

The Fourth amendment has been interpreted and thus refined in connection with emerging technologies, such as wiretapping. It was originally conceived of as solely applicable to physical violations, and did not protect citizens from intangible intrusions. In the 1928 Supreme Court case of *Olmstead v. US*, police investigated a lead by installing wiretaps in public places, such as on the street.[83] In its review, the court deemed there to be no violation of this wiretap, as no concrete, physical trespass had occurred: "The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[84] The wiretap was not deemed to be search or seizure, and thus deemed constitutional, purely because it did not constitute a *physical* intrusion.

Over time, the Fourth Amendment has morphed. In his dissent of Olmstead, Justice Brandeis argued that the Constitution is not static, and that it must adapt to changing technological, social and economic conditions.[85] And, forty years later, this view took hold. In the 1967 case of *Katz v. United States*, the Supreme Court widened its scope to include an intangible view of property: "The Fourth Amendment governs not only the seizure of tangible items but extends as well to the recording of oral statements overheard without any technical trespass under […] local property law."[86] Further, lower courts have affirmed this intangible view of property. The Seventh Circuit court case of *LeClair v. Hart* illustrates this;

CEU eTD Collection

[82] Fourth Amendment of the United States Constitution
[83] *Olmstead v. United States,* 277 U.S. 438 (1928) at 464
[84] *Ibid*
[85] *Ibid*
[86] *Katz v. United States,* 389 U.S. 347 (1967).

the court found that there was indeed a "seizure" when IRS agents dictated financial documents verbatim into a recording device.[87] This view extends the protection of the Fourth Amendment to broader modes of communication.

This trend towards an intangible interpretation of the Fourth amendment has an impact on the protection of communications from unreasonable search and seizure. A question remains: does the Fourth Amendment now stretch to cover email and electronic communication? In December of 2010, a Federal Court ruled that email is indeed within the scope of the Fourth Amendment. In the Sixth Circuit Court of Appeals case of *United States v. Warshak et al.,* the court found that:

> Given the fundamental similarities between email and traditional forms of communication [like postal mail and telephone calls], it would defy common sense to afford emails lesser Fourth Amendment protection … It follows that email requires strong protection under the Fourth Amendment; otherwise the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve.[88]

However, this ruling conflicts directly with a federal law. This ruling does not necessarily protect citizens from government surveillance of intangible messages in cyberspace.

The Fourth Amendment is applied in tandem with national legislation in order to create guidelines for government surveillance of individuals. The government cannot commit unreasonable search and seizure. However, several national Acts enumerate the specificities of conditions under which authorities may legally conduct surveillance in the United States. The Omnibus Crime Control and Safe Streets Act of 1968 outlines the specificities of legal wiretapping. Also known as the "Wiretap Act", the Act covers federal and state wiretaps, and outlines regulations for obtaining wiretap orders. Title III of the Act:

> prohibits the unauthorized, nonconsensual interception of "wire, oral, or electronic communications" by government agencies as well as private parties,

[87] *LeClair v. Hart* 800 F.2d 692 (7th Cir. 1986)
[88] U*nited States v. Warshak, et al.* Decided 14 December, 2010

CEU eTD Collection

> establishes procedures for obtaining warrants to authorize wiretapping by government officials, and
> regulates the disclosure and use of authorized intercepted communications by investigative and law enforcement officers.[89]

The law criminalizes private wiretaps, and creates conditions for determining when a warrant is required.

The Omnibus Crime Control and Safe Streets Act of 1968 was amended in order to create the Electronic Communications Privacy Act (ECPA). The ECPA of 1986 illustrates the most updated federal surveillance law as of 2011. The ECPA was amended in 1986 in order to include not just "oral" and "wire" communications, but also electronic communications. § 2516 of Title 18, Part I, Chapter 119 enumerates circumstances for legal wiretaps. Entitled 'Authorization for Interception of Wire, Oral or Electronic Communications,' the subsection allows for specified authorities to "authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation."[90] However, there are specific circumstances when a judicial application may be surpassed:

> An exception to the requirement that government obtain a warrant before intercepting covered communications is provided where: any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State...[91]

Additionally, the circumstances under which wiretapping is allowed are emergency situations that involve: "immediate danger of death or serious physical injury to any person,

CEU eTD Collection

[89] U.S. Department of Justice, Office of Justice Programs. *Justice Information Sharing: Federal Statutes.* Accessed 18 November 2011 http://it.ojp.gov/default.aspx?area=privacy&page=1284
[90] Electronic Communications Privacy Act. TITLE 18 > PART I > CHAPTER 119 > § 2516 Authorization for Interception of Wire, Oral or Electronic Communications
[91] *Ibid*

conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime."[92]

The Stored Communications Act (SCA) is also a part of the Electronic Communications Privacy Act (ECPA). The SCA allows for "a 'governmental entity' to compel a service provider to disclose the contents of [electronic] communications in certain circumstances."[93] Specifically, the SCA gives the government three ways to get permission to obtain information in electronic storage: " (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order […]."[94] Though the Fourth Amendment has moved towards protecting against the unreasonable search and seizure of electronic communications, federal law still allows for loose regulatory practices to occur. The ECPA is the most updated federal surveillance law as of 2011, and will be analyzed further in the coming chapters.

b. Germany

Current surveillance law in Germany is governed by the Code of Criminal Procedure (Strafprozeßordnung).[95] Section 100 of the German Code of Criminal Procedure outlines specific conditions regarding the interception of telecommunications, as well as guidelines to submit a judicial order for this interception. Further, it details acceptable measures implemented without the knowledge of the person concerned, the circumstances for reporting, and the details on the use of personal data.[96] Specifically, the law is broad. Section 100c allows for the application to new technology, in that it does not specify a particular means of surveillance. It reads: "other special technical means intended for the purposes of

CEU eTD Collection

[92] Electronic Communications Privacy Act. TITLE 18 > PART I > CHAPTER 119 > § 2516 Authorization for Interception of Wire, Oral or Electronic Communications
[93] Stored Communications Act, 18 U.S.C. §§ 2701 et seq.,
[94] Stored Communications Act, 18 U.S.C. §§ 2701 et seq.,
[95] German Code of Criminal Procedure, (Strafprozeßordnung, StPO), translated by the Federal Ministry of Justice.
[96] *Ibid*

surveillance may be used to establish the facts of the case or to determine the whereabouts of the perpetrator provided the investigation concerns a criminal offense of considerable importance."[97] This allows for new technology to be used to surveil alleged perpetrators.

Although it allows for the use of new technology in the surveillance of its citizens, the German Constitutional Court has instituted a groundbreaking right with regards privacy and telecommunications. The newspaper *Süddeutsche Zeitung* writes: "The constitutional court has created a new right for the second time in the history of postwar Germany. […] The new one […] allows some online surveillance by the government, but only under strict conditions.[98] In February of 2008, the German Constitutional Court struck down a law that would allow: "not just access to the hard disk but also ongoing surveillance of data, such as e-mail, as well as remote tracking of keyboard entries or online phone calls."[99] By turning down the law, the Constitutional Court protected many against violations of the right to privacy.[100] Despite the broad protection, there remain limitations. In cases deemed to be of "'paramount importance' -- that is, in cases of life or death, or a threat to the state -- authorities would be permitted to use such software, with a court's permission."[101] The act of the Court, however, has been deemed groundbreaking. German newspaper *Der Spiegel* has summarized the impact of the Court's actions: "This verdict […] has not only pointed the way for an upcoming federal law. It has done nothing less than establish a new 'fundamental

CEU eTD Collection

[97] German Code of Criminal Procedure, (Strafprozeßordnung, StPO), translated by the Federal Ministry of Justice.
[98] *Germany's New Right to Online Privacy.* Der Spiegel. Published 8 February 2008. Accessed September 2011 http://www.spiegel.de/international/germany/0,1518,538378,00.html
[99] State Spyware: German Court Permits Restricted Online Surveillance. Der Spiegel. Published 27 February 2008. Accessed September 2011 http://www.spiegel.de/international/germany/0,1518,538094,00.html
[100] *Ibid*
[101] *Ibid*

right' for the 21st century."[102] Germany has arguably the world's most updated surveillance laws, including strong protection for the technological communications of its citizens.

Summary of Chapter II:

This chapter introduces existing surveillance law in both jurisdictions. It looks to determine what protection citizens have against unreasonable intrusion by government surveillance mechanisms. In the United States the Fourth Amendment has served as protection from unreasonable search and seizure. Additionally, a recent trend towards recognizing intangible property as applicable in the search and seizure clause may include email and other electronic communications under the ambit of the amendment. However, contrary court rulings and federal laws further confuse and contradict the protection of the Fourth Amendment. The Omnibus Crime Control Act and the addition of the ECPA regulate the means by which the government can surveil its citizens. But there are exceptions to these laws; in emergency situations, the law may be surpassed.

The German Code of Criminal Procedure is briefly presented, and its specificities for legal wiretapping mentioned. Most notable is Germany's groundbreaking law protecting personal, technological communications. This law is was among the first of its kind, and while it does have an exception clause, it offers a large penumbra of protection. It is starkly different from the United States law in that, as a written law, it specifically protects personal, technological communications from unreasonable interference. While the United States has recent case law moving towards the protection of email communications, there is no written law to protect them. The German law has been updated along with technological innovation.

CEU eTD Collection

[102] *Germany's New Right to Online Privacy.* Der Spiegel. Published 8 February 2008. Accessed September 2011 http://www.spiegel.de/international/germany/0,1518,538378,00.html

This indicates a drastic difference between the adequacy of American and German law; German law is just that, a law, and is strikingly more current.

Chapter III: Evaluating Privacy

This chapter seeks to narrow the scope of this thesis by defining privacy as a right, and not a concept. A codified right to privacy will then be analyzed within each jurisdiction. And finally, it will be determined in each jurisdiction if this right to privacy is inviolable, or balanced with national security.

a. Privacy as a Right

Privacy may be understood in several ways. Firstly, the term may be approached as a concept. Scholars Solovon and Swartz hold that: "Privacy as a concept involves what privacy entails and how it is to be valued."[103] To illustrate, Alan Westin, one of the foremost scholars on privacy, attempts to define the term: "[privacy is] the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[104] However, privacy may also be conceived of as a right. Solovon and Swartz elaborate, quoting Hyman Gross: "the law does not determine what privacy is, but only what situations of privacy will be afforded legal protection."[105] Thus, conceiving of privacy as a right is determining the extent of its legal protections.[106] This includes concrete legal provisions that create or impact a level of protection for individuals. For example, privacy rights may have a Constitutional basis; some specific legal provisions

[103] Daniel J. Solove, Marc Rotenberg, Paul M. Schwartz. *Privacy, Information and Technology.* Aspen Elective, 2nd Edition, page 34
[104] Alan Westin, Privacy and Freedom. The Bodley Head Ltd. April 1970.
[105] Daniel J. Solove, Marc Rotenberg, Paul M. Schwartz. *Privacy, Information and Technology.* Aspen Elective, 2nd Edition, page 34
[106] *Ibid* pg 39

CEU eTD Collection

may explicitly protect privacy. Other protections can be inferred from case law. In this thesis, Privacy will be examined not as a concept but as a right, as it is explicitly understood through national and case law.

This right to privacy is often not absolute. Privacy may be conceived of as a balance between an individual's right to privacy and a society's legitimate need for information to adequately maintain public safety.[107] A basic principle of democracy is that the public has a right to know what the government is doing. But at the same time, from a law enforcement perspective, effective information sharing is crucial. Scholar Richard Posner enumerates this tension between personal privacy and public safety: "The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy."[108] But Posner finds that:

> Privacy is the terrorist's best friend, and the terrorist's privacy has been enhanced by the same technological developments that have both made data mining feasible and elicited vast quantities of personal information from innocents: the internet, with its anonymity, and the secure encryption of digitized data which, when combined with that anonymity, make the internet a powerful tool of conspiracy.[109]

This thesis will now address several questions: Is it possible to address and balance privacy with other national interests, such as protection from terrorism? How do America and Germany attempt to do so?

b. An American Right to Privacy

In the United States, a right to privacy emerged through Constitutional interpretation; there is no distinct, written right to privacy in the Constitution. The elusive conception of

[107] It must be noted that public safety is just one of a society's legitimate needs. Along with public safety, health and morals may be included, as well as the economic well being of the nation. It is a much broader concept that will be analyzed in this thesis through the narrower scope of national security/public safety.
[108] Richard Posner, Not a Suicide Act: The Constitution in a Time of National Emergency. New York: Oxford University Press, 2006. Page 143.
[109] *Ibid*

CEU eTD Collection

privacy emerged in the 1965 case of Griswold v. Connecticut, wherein the Supreme Court found that "zones of privacy" exist under various Constitutional guarantees.[110] Further, the term *privacy* reappeared in the case of Katz v. United States, where the Supreme Court found that, "a person has a constitutionally protected reasonable expectation of privacy."[111] In the Katz case, the Court found this under the Fourth Amendment protection from unreasonable search and seizure.

In America, this expectation of privacy is not absolute. Courts must take into consideration the interests of security. In order to reconcile security and privacy, courts use a standard of reasonableness: the reasonableness of the government to respect the liberty of that individual, as well as the reasonableness of an individual to their community, to respect the obligation to be a good citizen.[112] In U.S. jurisprudence, to be deemed *reasonable*, a search should be: "as limited in its intrusiveness as it is consistent with satisfaction of the need that justifies it."[113] For example, the threat of terrorism and the fear of further destruction may be considered a reasonable justification for more intrusive investigative techniques.[114]

In the United States, the protection of national security often trumps claims to personal privacy in times of war. Looking to history, in the case of *Korematsu v. United States* (1944), which evaluated the constitutionality of Japanese internment camps, the Supreme Court held that the need to protect the nation overruled Korematsu's individual rights. They found that an infringement on rights may be justified, as: "we are at war with the Japanese Empire […] [and] military authorities feared an invasion of our West Coast and felt

CEU eTD Collection

[110] *Griswold v. Connecticut* (No. 496) 151 Conn. 544, 200 A.2d 479, reversed.
[111] *Katz v. United States*, 389 U.S. 347 (1967)
[112] Miller Center of Public Affairs, National Discussion and Debate Series. Privacy vs. National Security. Accessed 14 May 2011 http://millercenter.org/public/debates/privacy
[113] *United States v. Davis*, 482 F.2d 893, 910 (9th Cir.1973)
[114] Sara Kornblatt. *Are Emerging Technologies in Airport Screening Reasonable Under the Fourth Amendment?* Loyola of Los Angeles Law Review, 2007.

constrained to take proper security measures."[115] Consequently, the internment of 110,000 Japanese Americans was substantiated on grounds of national security.[116]

In 2011, as a nation at war, the United States faces a threat of terrorism and may feel again "constrained to take proper security measures."[117] As the Fourth Amendment is applied in the context of the War on Terror, the interest lies not in prosecution, but in preemption; for example the prevention of chemical and biological weapons that pose a threat to millions of U.S. citizens. Many scholars hold that to prevent a potentially catastrophic outcome, such as nuclear terrorism, there needs to be a preemptive approach.[118] And many believe this preemptive approach may be reached through the surveillance of citizens.

c. A German Right to Privacy

In Germany, a right to privacy is found in Article 10 of the Basic Law. It is noteworthy because, unlike the U.S Constitution, it states the term *privacy* explicitly: "(1) The privacy of correspondence, posts and telecommunications shall be inviolable." It does, however, set limitations. The law is not entirely inviolable:

> (2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

Despite its limitations clause, the law is wide reaching. It addresses technological innovation: "In a series of important decisions, the German Constitutional Court has interpreted Article

[115] *Korematsu v. United States* 323 U.S. 214
[116] Bharath Krishnamurthy, Markkula Center for Applied Ethics, Santa Clara University. *Privacy vs. Security in the Aftermath of the September 11 Terrorist Attacks*. Published November 2001. Accessed July 2011 http://www.scu.edu/ethics/publications/briefings/privacy.html
[117] *Ibid*
[118] Miller Center of Public Affairs, National Discussion and Debate Series. Privacy vs. National Security. Accessed 14 May 2011 http://millercenter.org/public/debates/privacy

CEU eTD Collection

10 as protecting not only telecommunications content but also telecommunications proceedings. The Constitutional Court has been squarely involved in judicial review of measures that affect telecommunications privacy."[119]

Unlike the United States, Germany subscribes to a concept of privacy in a broader, supranational context, that of the Council of Europe. As a member of the Council of Europe, Germany is partied to the Convention for the Protection of Human Rights and Fundamental Freedoms (also known as the European Convention on Human Rights [ECHR]). As a State Partied to the ECHR, Germany may be held accountable for the content within, which includes an article on privacy. Article 8 of the ECHR states that:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This details a right to respect of ones private life. However, it must be noted that when dealing with national security, among other national concerns, ones privacy is again not absolute.

The European Court of Human Rights (ECtHR), the judicial body established by the ECHR, has developed a three-pronged standard to be met when determining rights violations with exception clauses, such as Article 8. The approach is three-fold: "The first standard requires that any interference with the Convention right must be "in accordance with the law" or "prescribed by law."[120] Second, such interference must pursue any of the legitimate aims that are exhaustively laid down in the second paragraphs of Articles 8-11. Third, a measure of

CEU eTD Collection

[119] Paul M. Schwartz. *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*. August 2003. Accessed July 2011 http://www.paulschwartz.net/pdf/hastings-03.pdf

[120] Yutaka Arai-Takahashi, The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR. Pg 11.

interference must be considered "necessary in a democratic society."[121] These criteria create distinct circumstances under which a government can interfere with its citizen's privacy.

When determining whether a violation has occurred, the judicial scrutiny does not stop with these three standards. As stated above, the first prong holds that an interference of a right must be "in accordance with the law." This may be further dissected. In order to be in accordance with the law, this requires that the national law must be accessible to its citizens. And further, in addition to being accessible, the law must be communicated in a way "as to enable the citizens to foresee with precision the exact scope and meaning of the provision."[122] Citizens must be able to understand the law clearly. In summary, in order for an interference to be deemed in accordance with the law, it must be *accessible* to its citizens and adequately *foreseeable* in scope and meaning. Thus, Germany is subscribed to a more stringent privacy law than the United States.

Summary of Chapter III:

This chapter establishes the concept of privacy dealt with in this thesis: a *right* to privacy. It attempts to define this aspect of privacy. Next it analyzes this concept with regards each jurisdiction in order to determine how the United States and Germany protect this right. In America, it is revealed that there is no distinct written right to privacy in the Constitution; rather, it is through judicial interpretation that this right has emerged. This right has evolved without distinct and clear legal bounds, and its application may be hazy. It is established that in America, national security often trumps a right to personal privacy. In Germany, on the other hand, the right to privacy is explicitly outlined in the Basic Law. And thus, privacy jurisprudence in Germany is strong and defined. In Germany, there must also be a balance between national interests and a right to privacy, but these interests must be qualified by

[121] *Ibid*
[122] *Ibid*

CEU eTD Collection

standards such as those of the ECHR. These differences between the United States and Germany lay the groundwork for the next chapter in that they directly affect how surveillance law may be evaluated.

Chapter IV: Analysis of Surveillance Law and Implications on Personal Privacy

This chapter seeks to answer the questions for each jurisdiction: Are surveillance laws suitable to apply to the Internet? Do they violate a right to privacy? It seeks to compare each nation's approach, and determine which view is more suitable for protecting privacy rights in a time of changing technology.

a. Is American Law Adequate?

Justice Scalia of the United States Supreme Court has found that new technology impacts privacy. He has stated that: "it would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[123] Do the effects on privacy, as acknowledged by Scalia, warrant changes to the law?

Judge Nicholas G. Garaufis of the Federal Disctrict Court in Brooklyn finds that U.S. law has steps to take in order to cover new technology. He recently stated that: "the courts must begin to address whether revolutionary changes in technology require changes to existing Fourth Amendment doctrine."[124] Judge Garaufis continued: "Their answer will bring Fourth Amendment law into the digital age, addressing how its 18th-century prohibition of

[123] Supreme Court to Rule on GPS Surveillance, Addressing 'Big Brother' Claims – NYTimes.com. Accessed 24 October 2011 http://www.nytimes.com/2011/09/11/us/11gps.html?_r=1&hp
[124] *Ibid*

CEU eTD Collection

'unreasonable searches and seizures' applies to a world in which people's movements are continuously recorded by devices in their cars, pockets and purses, by toll plazas and by transit systems."[125] This clearly indicates a preference for the adaptation of the law to changing technological times. The case of *Lopez v. the United States* also highlights a need for a change to the interpretation of the Fourth Amendment:

> There is a right of liberty of communications as of possessions, and the right can only be secure if its limitations are defined within a framework of principle. The Fourth Amendment does not forbid all searches, but it defines the limits and conditions of permissible searches; the compelled disclosure of private communications by electronic means ought equally to be subject to legal regulation.[126]

This also indicates a strong desire for the adaptation of the law to accommodate new technology in order to provide adequate protection to its citizens.

The applicability of the Fourth Amendment to technological communications remains uncertain. Standards have been interpreted inconsistently by courts. This is evidenced in contradictory rulings: "A district court in Oregon recently opined that email is not covered by the constitutional protections, while the Ninth Circuit has held precisely the opposite. Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion."[127] This creates uncertainty for those interacting with the technology, including internet users, service providers and even law enforcement agencies. How can we know, as citizens, if our online communications are protected from unwarranted intrusion?

Through both judicial and popular opinion, it may be determined that American surveillance law is inadequate. And not just by the hazy bounds of applicability of the Fourth Amendment. The ECPA is also starkly outdated. While it does include the addition of

CEU eTD Collection

[125] *Ibid*
[126] *Lopez v. United States*, 373 U. S. 427 (1963)
[127] Digital Due Process: About the Issue. Accessed 23 October 2011. http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163

"electronic communications" to its scope,[128] this is not enough. Digital Due Process (DDP), 'a diverse coalition of privacy advocates, major companies and think tanks,' that includes support from Microsoft among many other large companies, rightly calls the ECPA into question because of the changing technological times:

> The Electronic Communications Privacy Act (ECPA) was a forward-looking statute when enacted in 1986. It specified standards for law enforcement access to electronic communications and associated data, affording important privacy protections to subscribers of emerging wireless and Internet technologies. Technology has advanced dramatically since 1986, and ECPA has been outpaced.[129]

The DDP coalition is correct. The ECPA is starkly outdated. The ECPA is inadequate in that it includes conflicting information. Specifically, the ECPA lists inconsistent guidelines outlining governmental access to personal email and stored documents:

A single email is subject to multiple different legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient to the time it is stored with the email service provider […] [In addition,] a document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but the ECPA says that the same document stored with a service provider may not be subject to the warrant requirement.[130]

Due to these discrepancies, the ECPA is inconsistent and hence unclear. Consequently, as the DDP coalition aptly summarizes: "the vast amount of personal information generated by today's digital communication services may no longer be adequately protected."[131]

b. Is German Law Adequate?

CEU eTD Collection

[128] U.S. Department of Justice. Office of Justice Programs. Justice Information Sharing. Accessed 20 November 2011 http://it.ojp.gov/default.aspx?area=privacy&page=1284
[129] Digital Due Process: About the Issue. Accessed 23 October 2011. http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163
[130] Digital Due Process: About the Issue. Accessed 23 October 2011. http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163
[131] *Ibid*

As of November 2011, German surveillance law may be deemed adequate. Firstly, the law is inclusive, as found in the ECtHR case of Uzun v. Germany. The law covers future developments of new technology, thus making it foreseeable to German citizens. Germany came into direct contact with this standard of 'foreseeability' in the ECtHR case of Uzun v. Germany (Application no 35623/05). And the German law held up to this standard. In this case, an applicant claimed violation of Article 8 of the ECHR due to the observation of his whereabouts by the authorities via a Global Positioning System (GPS). The applicant claimed that there was a violation of Article 8 in part because the use of GPS technology for surveillance was not foreseeable in German law. The applicant stated that the Code of Criminal Procedure of Germany had not meant to "cover measures of surveillance unknown at the time of its adoption."[132] He continued that the Code of Criminal Procedure was "not sufficiently clear, and having regard to possible technical developments in the future, its content was not foreseeable for the persons possibly concerned."[133] In its judgment, the ECtHR found that the interference by the German government into the applicant's private life was foreseeable, and thus in accordance with the law. This was because the relevant German legislation was broad enough to include future technological developments: it allowed for the implementation of "technical means […] to detect the perpetrator's whereabouts."[134] By using the broad language of 'technical means,' the law is clearly inclusive of new technology. Thus, the ECtHR found the law to be sufficiently clear.[135]

Secondly, the law has stretched to cover new technology. In February of 2008, the German Constitutional Court published a momentous ruling concerning the constitutionality

CEU eTD Collection

[132] *Uzun v. Germany* Judgment, Fifth Section. (Application no. 35623/05) Strasbourg, 2 September 2010 paragraph 54
[133] *Ibid*
[134] *Ibid* paragraph 68
[135] *Ibid*

of government agencies in their attempts to conduct clandestine online searches of computers.[136] The Court held that: (in translation)

> "From the relevance of the use of information-technological systems for the expression of personality (Persönlichkeitsentfaltung) and from the dangers for personality that are connected to this use follows a need for protection that is significant for basic rights. The individual is depending upon the state respecting the justifiable expectations for the integrity and confidentiality of such systems with a view to the unrestricted expression of personality.[137]

Scholars highlight the significance of this ruling: "The decision constitutes a new 'basic right to the confidentiality and integrity of information-technological systems' as derived from the German Constitution."[138] Further, some have cited the establishment of this new law as a profound new right: "It has done nothing less than establish a new 'fundamental right' for the 21st century [...] Now that the court has spoken, lawmakers and police have some idea of where a person's 'private sphere' starts and ends -- even if the suspect is surfing a wireless connection, outdoors, on a laptop."[139] By creating more specific bounds of the private sphere and becoming consistent and clear, the German law may be deemed sufficient.

Summary of Chapter IV:

This chapter looked at the adequacy of surveillance law in America and Germany with respect to new technology. Does surveillance law cover electronic communications? Does it respect a right to privacy?

CEU eTD Collection

[136] *Germany's New Right to Online Privacy.* Der Spiegel. Published 8 February 2008. Accessed September 2011 http://www.spiegel.de/international/germany/0,1518,538378,00.html
[137] Das Bundesverfassungsgericht BVerfG, 1 BvR 370/07 vom 27.2.2008. Margin number 181
[138] *Germany's New Right to Online Privacy.* Der Spiegel. Published 8 February 2008. Accessed September 2011 http://www.spiegel.de/international/germany/0,1518,538378,00.html
[139] *Ibid*

In America, the bounds of the Fourth Amendment are still unclear. While a court recently ruled that the Fourth Amendment should apply to email communications, national law dictates otherwise. In addition, while the ECPA does refer to electronic communication, it has many downfalls. Specifically, it is inconsistent in its applicability nationwide, and it has variable requirements for intercepting communications. Thus, it does not ensure adequate protection; it cannot be said to sufficiently protect the right to privacy.

In Germany, the law specifically covers electronic communications. The European Court of Human Rights deemed the German law to be adequately foreseeable, and clear enough to be understood by its citizens. Further, Germany effectively respects the right to privacy, as it has created a new Basic Right with regards personal privacy of technological communications. Thus, German law adequately addresses the protection of privacy.

Chapter V: Recommendations: Striking a Proper Balance

This chapter lays out several recommendations for each nation in order to achieve an adequate balance between surveillance law and privacy rights.

a. The United States:

The United States must define the bounds of the Fourth Amendment to cover email communications. Without this coverage, a right to privacy may not be respected. Though in recent case law the United States has taken steps toward the recognition of email communications as protected by the Fourth Amendment, the protection remains inconsistent. It must be made sufficiently foreseeable and clear. This can be done through a Supreme Court ruling. Currently, the United States Supreme Court is addressing the bounds of the Fourth Amendment in the case of *United States v. Jones*. While the case deals with the high

CEU eTD Collection

tech surveillance of a person's public and perceptible movements, it still addresses the tension between new technology and the Fourth amendment. In preliminary hearings of the case, Justice Samuel A. Alito Jr. stated these tensions:

> The heart of the problem that's presented by this case is that in the pre-computer, pre-Internet age, much of the privacy – I would say most of the privacy – that people enjoyed was not the result of legal protections or constitutional protections. It was the result simply of the difficulty of traveling around and gathering up information. But with computers, it's now so simple to amass an enormous amount of information about people […] So, how do we deal with this? Do we just say, well, nothing is changed […] there is no search or seizure when [information] is obtained, because there isn't a reasonable expectation of privacy? But isn't there a real change in this regard?[140]

Justice Alito recognizes the change technology has induced, and the need for wider protection. Thus, in order to create more robust protection of personal privacy, the Supreme Court should use this case in order to create a wider ambit of the Fourth Amendment in order to apply to new technology, such as email communications.

The ECPA needs to be amended. It is inconsistent; there is a need for nationwide standards of surveillance. Information must be communicated clearly, and needs to be available to the public so they understand their rights and the exceptions of these rights. In order to protect privacy, the United States may even consider the determination of a right of cyber privacy, as Germany has, thus addressing the latest in technological advances.

It must be considered that the United States is a nation at war. During times of war, concerns of national security override personal privacy interests in the United States, as illustrated above in the case of *Korematsu*. Perhaps as the War on Terror continues, no direct right to cyber privacy will be enacted. Yet the current war is indistinct, as it seems a war against terrorism will never cease. Consequently, restrictions on privacy could become the status quo. But despite being a nation at war, the United States should update its surveillance

[140] United States Supreme Court, *United States v. Antoine Jones*. 8 November 2011. Oral Transcript. Accessed 25 November 2011 http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf

CEU eTD Collection

law and the applicability of the Fourth Amendment. With advancements in technology, privacy may be further ensured, while national security concerns may still be addressed.

b. Germany:

Germany is a trailblazer of privacy rights. Germany has enacted the first "cyberlaw," and has created what some call a "new fundamental right of the 21st century."[141] It has been proactive in addressing concerns of the applicability of surveillance law in times of changing technology. For this, Germany may be lauded.

Germany must continue questioning and altering its laws in order to maintain this forward thinking. It must often evaluate whether it strikes an adequate balance between privacy rights and surveillance law, taking into consideration advancements in technology. In addition, Germany must always question its position, as to not be too stringent in its regulatory laws. But it deserves much respect, and the United States can look to Germany as a model for its strong privacy protection.

Summary of Chapter V:

After the analysis conducted in the earlier portion of this thesis, Chapter V proposed recommendations for further action. It outlines specific steps the United States should take to assure adequate protection of personal privacy, such as the clarification of the ECPA and the broadened scope of the Fourth Amendment. It suggests that Germany continue analyzing its laws with regards new technology. It finds that Germany may serve as an example for the United States.

CEU eTD Collection

[141] Spiegel Online International: Germany's New Right to Online Privacy. 2/28/2008. Accessed 9 November 2011 http://www.spiegel.de/international/germany/0,1518,538378,00.html

III. Conclusion

The inquiry into existing surveillance policies of the United States reveals serious deficiencies of the law. This thesis suggests that the United States update its policies regarding surveillance law in order to create consistency in its applicability and clarity in its purpose. The findings in this thesis differ, as it is opined that Germany has effective mechanisms in place for protecting personal privacy. With its laws tailored to protect the privacy of technological communications, Germany has created a defense against unwarranted intrusion. It is suggested that Germany serve as an example to the United States and other countries in need of updating surveillance law to accommodate new technology, thus providing adequate protection of personal privacy.

While some inadequacies of surveillance law have been pointed out, further research must be done. The results herein are valid, as they give a historical snapshot of the development of governmental surveillance law and policy. However, there are limitations to this research. The law is constantly in flux. During the writing of this thesis, cases have been heard and laws have been enforced. In order to remain updated, there is a need for further research. Additionally, the need for further research will probably never cease because technology is ever changing. But the results of this research remain useful, as they provide insight into specific laws and policies, and may help to shape surveillance law and procedure in the future.

CEU eTD Collection

IV. Bibliography

1. Andrews, Edmund L. *Germany's Efforts to Police Web are Upsetting Business*. The New York Times, Published 6 June, 1997. Accessed October 2010. http://www.nytimes.com/1997/06/06/business/germany-s-efforts-to-police-web-are-upsetting-business.html?scp=3&sq=germany+cyber+law&st=nyt

2. Arai-Takahashi, Yutaka. *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*. Intersentia nv, 2002

3. Barlow, John Perry. A Declaration of the Independence of Cyberspace. February 8, 1996. Accessed: November 30, 2010. http://editions-hache.com/essais/pdf/barlow1.pdf

4. Black's Law Dictionary, 9th edition. West Group, 2009.

5. Das Bundesverfassungsgericht (BVerfG), 1 BvR 370/07 vom 27.2.2008. Margin number 181

6. Die Midienanstalten. State Media Authorities in the Federal Republic of Germany - ALM GbR. Published 2011. Accessed October 12, 2011 http://www.die-medienanstalten.de/home.html

7. Digital Due Process: *About the Issue*. Accessed 23 October 2011. http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163

8. Electronic Communications Privacy Act. TITLE 18 > PART I > CHAPTER 119 > § 2516 Authorization for Interception of Wire, Oral or Electronic Communications

9. European Journalism Centre – Media Landscape, Germany. 5.3 Regulatory Authority. Accessed 13 October 2011 http://www.ejc.net/media_landscape/article/germany/

10. Federal Law to Regulate the Conditions for Information and Communications Services (IuKDG), Article 6. Final Draft, December 20, 1996. Translation by Christopher Kuner, Esq.

11. German Code of Criminal Procedure, (Strafprozeßordnung, StPO), translated by the Federal Ministry of Justice.

12. German Propaganda Archive: the German Federal Archives. Accessed 13 October 2011 http://www.calvin.edu/academic/cas/gpa/posters2.htm

13. *Germany's New Right to Online Privacy.* Der Spiegel. Published 8 February 2008. Accessed September 2011 http://www.spiegel.de/international/germany/0,1518,538378,00.html

14. *Germany Passes Internet Law Limiting Content*. The Los Angeles Times. From the Associated Press. 5 July, 1997. Accessed October 2011

CEU eTD Collection

http://articles.latimes.com/1997/jul/05/business/fi-9816

15. Gillespie, Alisdair A. Regulation of Internet Surveillance. European Human Rights Law Review, Issue 4 2009. Pg 552-565. Edited by Jonathan Cooper

16. *Griswold v. Connecticut* (No. 496) 151 Conn. 544, 200 A.2d 479, reversed.

17. Internet Corporation for Assigned Names and Numbers (ICANN). Last modified 13-Aug-2010. Accessed November 30, 2010
http://www.icann.org/

18. Internet World Statistics: *Usage and Population Statistics.* Accessed November 2010
http://www.internetworldstats.com/stats.htm

19. Interstate Treaty on Broadcasting and Telemedia (Interstate Broadcasting Treaty) 1 April 2010. Preamble

20. *Janet Reno, Attorney General of the United States, et l. v. American Civil Liberties Union et al.* 521 US 844, 138 L Ed 2d 874, 117 S Ct 2329 [No. 96-511].

21. *Katz v. United States,* 389 U.S. 347 (1967).

22. Kleinwaechter, Wolfgang. *Challenges of Internet Governance: New multistakeholder models for global policy development.* Lecture, attended 26 October, 2010.

23. *Korematsu v. United States* 323 U.S. 214

24. Kornblatt, Sara. *Are Emerging Technologies in Airport Screening Reasonable Under the Fourth Amendment?* Loyola of Los Angeles Law Review, 2007.

25. Krishnamurthy, Bharath. *Privacy vs. Security in the Aftermath of the September 11 Terrorist Attacks*. . Markkula Center for Applied Ethics, Santa Clara University. Published November 2001. Accessed July 2011
http://www.scu.edu/ethics/publications/briefings/privacy.html

26. *LeClair v. Hart.* 800 F.2d 692 (7th Cir. 1986)

27. Liptak, Adam. *Court Case Asks if Big Brother is Spelled GPS*. The New York Times Online, 10 September 2011. Accessed October 2011.
http://www.nytimes.com/2011/09/11/us/11gps.html?_r=2&hp

28. *Lopez v. United States,* 373 U. S. 427 (1963)

29. The Markle Foundation: *Advancing Health and National Security in a Connected World.* Accessed 9 November 2011
http://www.markle.org/our-story

30. The Markle Foundation: *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*. Third Report of the Markle Foundation Task Force

CEU eTD Collection

31. Merlis, Steven E. Preserving Internet Expression While Protecting Our Children: Solutions Following *Ashcroft v. ACLU*. 4 Nw. J. Tech. & Intell. Prop. 117. Accessed 15 November 2011
http://www.law.northwestern.edu/journals/njtip/v4/n1/6

32. Merriam-Webster Dictionary: Surveillance. Accessed 24 March 2011
http://www.merriam-webster.com/dictionary/surveillance

33. Miller Center of Public Affairs, National Discussion and Debate Series. *Privacy vs. National Security*. Accessed 14 May 2011
http://millercenter.org/public/debates/privacy

34. The Museum of Broadcast Communications – GERMANY. Accessed 18 November 2011
http://www.museum.tv/eotvsection.php?entrycode=germany

35. National Conference of State Legislatures: Electronic Surveillance Laws. Accessed 23 March 2011.
http://www.ncsl.org/default.aspx?tabid=13492

36. Ohm, Paul. *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*. 2008 STAN. TECH. L. REV. 2 Accessed: April 2011
http://stlr.stanford.edu/pdf/ohm-olmsteadian-seizure-clause.pdf

37. *Olmstead v. United States*, 277 U.S. 438 (1928) at 464

38. Posner, Richard. *Not a Suicide Act: The Constitution in a Time of National Emergency*. New York: Oxford University Press, 2006.

39. Radio Mentor: Diese Sender des Mittel- und Langwellenbereiches dürfen in Deutschland abgehört werden. Accessed 13 October 2011
http://aobauer.home.xs4all.nl/hoerverbot_1941.htm

40. Radio Mentor: Hoerverbot 1941. *List of Authorized Broadcasting Stations.* Accessed 13 October, 2011
http://aobauer.home.xs4all.nl/hoerverbot_1941.htm

41. The Radio and Television Museum. Gallery 1: *Wireless Beginnings.* Accessed 29 November 2010
http://radiohistory.org/?page_id=28.

42. The Radio and Television Museum Gallery 2: *Birth of Broadcasting*. Accessed 29 November 2010.
http://radiohistory.org/?page_id=27

43. The Radio and Television Museum Gallery 3: *Radio Comes of Age*. Accessed 29 November 2010
http://radiohistory.org/?page_id=29.

44. Royal Pingdom: Internet 2010 in numbers. Accessed 24 March 2011

CEU eTD Collection

http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/

45. Schwartz, Paul M. *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*. August 2003. Accessed July 2011 http://www.paulschwartz.net/pdf/hastings-03.pdf

46. Solove, Daniel J., Marc Rotenberg, Paul M. Schwartz. *Privacy, Information and Technology.* Aspen Elective, 2nd Edition.

47. Stanford Encyclopedia of Philosophy, Entry on "Privacy". First published Tue May 14, 2002; substantive revision Mon Sep 18, 2006. Accessed September 2011. http://plato.stanford.edu/entries/privacy/

48. *State Spyware: German Court Permits Restricted Online Surveillance*. Der Spiegel. Published 27 February 2008. Accessed September 2011 http://www.spiegel.de/international/germany/0,1518,538094,00.html

49. Stored Communications Act, 18 U.S.C. §§ 2701 et seq.

50. Supreme Court of the United States. *Janet Reno v. American Civil Liberties Union.* Brief for the Appellees. October 1996. Accessed October 2011 http://epic.org/free_speech/cda/lawsuit/sup_ct_brief.html

51. *Supreme Court to Rule on GPS Surveillance, Addressing 'Big Brother' Claims –* NYTimes.com. The New York Times. Accessed 24 October 2011 http://www.nytimes.com/2011/09/11/us/11gps.html?_r=1&hp

52. The United States Constitution, Amendment Four.

53. The United States Court of Appeals for the Third Circuit. Decision, February 2000, on the COPA. Accessed October 2011 http://www.efa.org.au/Issues/Censor/cens3.html#usa

54. U.S. Department of Justice, Office of Justice Programs. *Justice Information Sharing: Federal Statutes.* Accessed 18 November 2011 http://it.ojp.gov/default.aspx?area=privacy&page=1284

55. United States Supreme Court, *United States v. Antoine Jones*. 8 November 2011. Oral Transcript. Accessed 25 November 2011 http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf

56. *United States v. Davis*, 482 F.2d 893, 910 (9th Cir.1973)

57. U*nited States v. Warshak, et al.* Nos. 08-3997/4085/4087/4212/4429 Decided 14 December, 2010

58. *Uzun v. Germany* Judgment, Fifth Section. (Application no. 35623/05) Strasbourg, 2 September 2010

CEU eTD Collection

59. Warren, Samuel D & Louis D. Brandeis, The Right of Privacy, 4 Harv. L. Rev. 193 (1890)

60. Westfall, Joseph. Internet Blocking. Markulla Center for Applied Ethics, Santa Clara University. Accessed October 2010
http://www.scu.edu/ethics/publications/submitted/westfall/blocking.html

61. Westin, Alan. *Privacy and Freedom*. The Bodley Head Ltd. April 1970.

62. White, Thomas. *United States Early Radio History*. Early Government Regulation: 1904 Roosevelt Board. Accessed 30 November, 2010.
http://earlyradiohistory.us/sec023.htm

63. Wikipedia: One Billion, number. Accessed 27 November 2010
http://en.wikipedia.org/wiki/1000000000_(number)

CEU eTD Collection