Spring 2018

Privacy in America: The Traditions, Changing Views, and Response

Emmet J. O'Connell
Bard College, eo2431@bard.edu

Privacy in America: The Traditions, Changing Views, and Response

Senior Project Submitted to
The Division of
The Division of Multidisciplinary Studies
Of Bard College.

by

Emmet O'Connell

Annandale-on-Hudson, New York
May 2018

Acknowledgements

Thank you to my Advisor, Myra Armstead, who has been an incredible source of support. Thank you for taking the time to give me invaluable feedback and advice throughout this whole process, it will forever be appreciated.

Timand Bates, thank you for all these years of support. You gave me the confidence and encouragement to make this project happen, and of course to graduate.

Thank you Jacey for giving me helpful advice and encouragement to get this project done. Thanks for being by my side every step of the way.

Thank you to my brother Rob, who has been a significant influence in my senior project. You helped me develop my ideas and were a tremendous resource.

Thank you mom and dad for your endless love and support throughout this journey and my educational experience. None of this would have been possible without you.

Table of Contents

Introduction……..……1
Chapter 1…….5
Chapter 2…..……..19
Chapter 3…..……..35
Conclusion...……..56
Bibliography…..……..……..58

Introduction

As senior year approached and I started to think about my project, one concern kept crossing my mind. I really wanted my project to be meaningful. I did not want to have to think of it as just another assignment. I knew that if I was not fully invested in my work, it would be an unbearable experience and I would get nothing out of it. This project was going to take up a full academic year of my life. How could I stay focused and not lose interest? I soon realized I would really need to connect with my work. In order to have a more meaningful connection to my work, I realized it would be best if my topic could bring in more aspects of my life than just academics. I also wanted my project to have some significance to me once I leave Bard.

The more I thought about ideas for a topic, I began to make observations about my life, both personally and academically. Everything in my life up until now, both personally and academically, has been pushing me towards one common goal--getting a job once I graduate college. This got me thinking that my topic should help me achieve this goal. As long as I can remember, I always had this idea in my head that going to work meant waking up early, putting on nice clothes, like a shirt and a tie, grabbing coffee, and a newspaper going into an office. This became a reality for me when I received my first internship following my freshman year at Bard. My older brother, Rob, was nice enough to find me a position within the insurance company he was working for, Ace Group, where he had once interned a few years back.

This internship was my first introduction to the business world as well as the insurance industry. I was eager to prove myself at every opportunity and gave it my complete effort. I not only learned a tremendous amount of information about the insurance industry, I formed many valuable relationships with co-workers. My hard work paid off as I was invited back for more

internships. Throughout my four years at Bard, I had three summer and one winter internships with Chubb (previously Ace Group). It was an unforgettable experience, each one being better than the last. Before my internship experience, I had very little knowledge of the insurance industry and no real appreciation for it at all. Now with the knowledge I have, I have come to appreciate the industry way more and believe it would be a great place to begin a career given the opportunity.

Given my internship experience, I plan on pursuing a career in the insurance industry upon graduation. I wanted my project to help me in the pursuit of this career choice in some way--whether that be helping find a job once I finish college or helping me move up along my career path. I hoped to incorporate insurance into my project topic in a way that would be interesting and informational. I thought about what I had learned in my internships and one topic that really resonated with me was cyber insurance.

Cyber insurance is the newest market for insurers and is rapidly growing. I remember one of my first days as an intern, I had not been given a computer yet so my manager gave me an insurance magazine to pass some time. I read article after article about cyber insurance. It was the hottest topic and had the most potential for growth. Funny enough, my brother had just recently begun underwriting cyber policies. It seemed pretty clear that cyber insurance would be a great topic for my project. Not only is it new, interesting and rapidly growing, but I also have a great source for information through my brother. Now the final challenge would be finding a way to connect this topic to my major, American Studies.

American Studies has given me the opportunity to focus my studies on some of my interests. I see myself as a fairly analytical person, and American Studies has allowed me to use these skills to better understand the United States and American culture. My interests that I have

been able to focus on in American Studies are history and pop culture. I have always found that history has been one of my stronger subjects. I like getting caught up in facts as well as imagining stories in my head. One of my favorite topics is learning about the Civil War. In high school, I was even a member of the History Club. Through this club, I was able to visit Gettysburg several times and take tours of the battle fields. I really enjoyed those experiences, especially sitting there imagining what it would be like to be there in the summer of 1863. Pop culture is another interest of mine that I have not had much time to study. Although I may not participate in the every new trend, I am usually aware of them. My interest around pop culture comes from trying to understand these trends. In thinking about how to bring together cyber insurance and American Studies, I wanted to have aspects of both history and pop culture.

I went back and forth with my brother talking about ways in which I could bring cyber insurance into my project. A few ideas that really stuck with me were privacy and technological innovation. American Culture seems to uniquely embrace both these interests, which is fascinating because they are increasingly antagonistic ideas. I have always considered privacy to be a core American belief. At the same time, I have also noticed that new technologies are exposing people to new threats to privacy. This is intriguing because Americans seem to be at the forefront of embracing technological innovation. This dynamic is playing an important role in the development of the cyber insurance market.

The more I thought about the conversations with my brother, I realized that this idea of privacy was a great starting point. I had some knowledge of privacy, but not much. As stated earlier, I did consider it to be a core American value. However, I did not have a complete understanding of the idea. In wanting to understand American privacy more, I saw this as a great opportunity to use my interest in history to form a better understand by looking to the past to

study the early ideas and traditions. I also saw the opportunity to use an interest in pop culture to focus on American trends that are fueling the acceptance of technological innovation by ordinary Americans. I wanted to end my project by looking at cyber insurance as a response to privacy concerns. I wanted to know if this response was actually in line with American privacy views.

In the first chapter, I explore the history of privacy in America. I outline the traditions and views of privacy in American history and culture. I was able to get a better understand of American views on privacy and where the roots for these views come from. Once I was able to understand some of the history surrounding privacy views, I could see how they align with privacy views in America today. The next chapter is where I explore the changing views of privacy in the twenty-first century. In this chapter, I used my interest in pop culture to further my understanding of these privacy views. I did this by looking at social media, one of the most popular uses of the internet and technology among Americans. I used social media as a basis for the dynamic views of privacy, which are also discussed in this chapter. Finally, in the last chapter, I looked at cyber insurance. I had a basic understand of it but wanted go really into depth. I discuss exactly what it is, the history behind it, how it works, where it's going and more.

From this investigation, I conclude that although cyber insurance is a response to privacy concern, it is not a solution. A solution would be one that does better to protect individual citizens not just organizations. I was able to see that Americans are concerned with their individual personal information being used without their consent or knowledge. Cyber insurance protect organizations that collect personal information, but is not a direct response to the concerns of American citizens.

Chapter One:

History of Privacy in America

European Tradition

The roots of American privacy can be traced back to England. The crime of eavesdropping first appeared in England and made its way across the Atlantic to the Colonies. American colonies soon adopted eavesdropping laws as part of the common laws. As early as 1361, England had put laws into place to protect against eavesdropping and peeping toms. The Justice of the Peace 1361 provided legislation against eavesdropping.[1] The leading legal authority for England and American Colonies at the time was Sir William Blackstone, who in a way created the offense in his famous compendium of English law. In the eighteenth century, he wrote,

> Eavesdropping, or such as listen under walls or windows, of the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance, and presentable at the court-leet or are indictable at the sessions, and punishable by fine and finding sureties for their good behavior.[2]

Early in the nineteenth century, American courts began to apply this section of the criminal common laws. Eavesdropping and privacy were dealt with at local levels of the judicial system. The number of cases reported that dealt with eavesdropping was very small. There were also many struggles early on regarding the application of this law in courts. There was

---

[1] David J. Seipp, *The Right to Privacy in American History* (Harvard University, 1981), [5], accessed February 2018, http://pirp.harvard.edu/pubs_pdf/seipp/seipp-p78-3.pdf.

[2] Seipp, *The Right*, [4]. Quoting Sir William Blackstone, *Commentaries on the Laws of England*, ed. William Draper Lewis (Philadelphia,1922).

debate in courts on whether the English laws applied in America. A Pennsylvania Court in the early nineteenth century gave its reason behind prosecuting an eavesdropper: "Every man's house is his castle, where no man has a right to intrude for any purpose whatever. No man has a right to pry into your secrecy in your own house. There are very few families where even the truth would not be very unpleasant to be told all over the country."[3]

This is a very early and interesting example of privacy values in America because of the comparison of the house to a castle. In drawing a connection back to Europe where only rulers and the aristocracy had castles, the court is asserting the importance of ordinary American citizens and their abodes. The home was sacred for the colonists. Just as the noble's castle was a fort built to withstand attacks, they wanted the home to be a safe place. Another point being made was to not have gossip spreading around. Gossip was a privacy concern in the early nineteenth century. However, this concern seemed to be only American. It was not something that was found its way to the colonies from Europe. This might have been a reflection of the Biblical consciousness and religiosity of many early settlers in British North America since the Bible contains many injunctions against gossip[4]. In the Colonies people were concerned with other people's affairs, but not as much so in England. A British visitor to America in the early part of the nineteenth century said, "In England, every one appears to find full employment in his own concerns;-here it would seem that the people are restless until they know every person's business."[5] This observation makes it seem as if American people want to know everything about each other. It goes on to say that American people did like to know what their neighbors were up to. However, it also seemed as if the gossip was relatively

[3] Seipp, *The Right*, [4]. Quoting Commonwealth V. Lovett, 4 Clark 5 (Pa., 1831).
[4] Seipp, *The Right*, [5-6].
[5] Seipp, *The Right*, [5] Quoting.Charles William Janson, The Stranger in America, 1793-1806, 1807 (Rpt. New York, 1935), p.20.

local. Most people wanted to know about what was going on within the area they lived. Gossip in the early nineteenth century was usually kept local and non-harmful, and therefore never really had any criminal side effects[6].

Bill of Rights

American right to privacy is written directly into the Bill of Rights, in the Third, Fourth and Fifth Amendments. As discussed earlier, there had previously been laws of privacy before, but they protected against eavesdropping and gossiping. These Amendments give Americans protection from privacy intrusions of the government. The basis for these ideas of privacy came from pre-revolutionary war ideas, which at this time the main issue with privacy was the intrusion of the government. Prior to and during the Revolution the British government was doing many things that invaded the colonists' privacy. Each amendment protects Americans privacy from governmental intrusions that were specifically done by the British.

The largest way the British imposed themselves into the privacy of the colonists was with the writs of assistance and general warrants. These two tactics were used by the British government while revolutionary tensions were high. They imposed on people's homes which was, as discussed earlier, a sacred place for colonists, as well as Europeans. The writs of assistance authorized "sweeping searches and seizures without any evidentiary basis", allowing homes to basically be invaded based purely on suspicion. General warrants "resulted in 'ransacking' and seizure of the personal papers of political dissenters, authors, and printers of seditious libel", again complete invasion of privacy with no evidence needed. The Quartering Act of 1765, was also an invasion of colonist's privacy, which required people to give food,

[6] Seipp, *The Right*, [2-6].

shelter, and water to British troops.[7] As a result, each of these intrusions are protected by the Bill of Rights.[8]

The distrust in the Government by the newly independent colonists was forged into the Bill of Rights. The Third Amendment attacks the Quartering Act directly and protects the privacy of the home: "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[9] This amendment prevents the government from requiring anyone to host a soldier in the house if they do not wish to do so. The Fourth Amendment attacks searches and seizures that were unreasonably done by the British Government:

> 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.[10]

The Fourth Amendment puts limitations on the government's powers when it comes to searching and seizure of an individual, by preventing any "unreasonable searches and seizures." In order to conduct a search, a Government Official needs a judicial approval that gives them a warrant to search that is supported by probable cause. The Fifth Amendment protects an individual from being compelled to testify about incriminating information. The

---

[7] The Editors of Encyclopedia Britannica, ed., "Quartering Act," Encyclopedia Britannica, last modified July 12, 2016, accessed April 2018, https://www.britannica.com/event/Quartering-Act.

[8] Daniel J. Solove, "A Brief History of Information Privacy Law," *Proskauer On Privacy*, 2006, [4-5], https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2076&context=faculty_publications.

[9] U.S. Constitution. Amendment. III.

[10] U.S. Constitution. Amendment. IV.

government cannot force a person to give any information that may incriminate the individual.[11]

Postal Service and Privacy Ideas

Early colonial America did not have a reliable or official mailing system. Prior to 1710, there was no official postal service in the British colonies.[12] It wasn't until the British government got involved and took over the unofficial system already in place, that the system was institutionalized. Before that, letters were either given to a trusted friend, a paid messenger, or given directly to a ship's officer. The letters given to a ship's officer were to be received at port once the ship had gotten in. In the colonies, if the mail onboard a ship was unclaimed it would go to a tavern or a coffee shop to be picked up there. People started to leave the letters in a public space along with other letters hoping they would make it to the respected destination. The leaving of letters in public spaces soon began to influence the way people would send letters. There would be a rise in the lack of trust between the senders of letters and a ship's officers. Colonists no longer wanted to leave letters they were sending directly with the ship[13].

This tradition also worked its way into mail that was to be sent within the colonies. The sending and receiving of mail from public spaces served as a basis for the unofficial mail system for the colonies. However, there was some faults in this system regarding privacy. Letters being sent were no longer in the hands of trusted friend or a paid messenger, but in the possession of a complete stranger. The unofficial postal service was a non-regulated,

---

[11] Seipp, *The Right*, [4-5].
[12] Seipp, *The Right*, [7].
[13] Seipp, *The Right*, [7-9].

unorganized system with no authority that colonists had to trust. This lead to letters easily being read by unintended people. Gossipers would ransack mail bags in order to find news worth spreading. This happened quite frequently due to the fact that there was very limited news coming to the colonies. Business rivals also took part in prying into people's mail to get a leg up on their competition. Colonists soon petitioned to have an official mail service, which started in Boston. The British took control of an official postal service in 1710 and immediately regulated it.[14]

The British government imposed the Postal Act of 1710, shortly after taking control of the system. This act reiterated a Proclamation of 1663 which stated: "No person or persons shall presume wittingly, willingly, or knowingly, to open, detain or delay, or cause, procure, permit, or suffer to be opened, detained or delayed, any letter or letters, packet or packets."[15] The Act basically outlawed all official tampering with letters. This did not halt the use of unofficial sending of letters however. There would still be problems with official tampering of the mail prior to independence and for a few years following it. As revolutionary tensions grew toward the end of the colonial period Benjamin Franklin realized that his personal letters were being opened either in Boston or it is more likely by postal officials in London. Patriots in Boston started to take notice of the abuses and tampering of the mail service. These revolutionaries began to petition for a new postal system as early as 1774. These people wanted a "New American Postal Service" that would protect the privacy of the people's letters.

It wouldn't be until Independence that Americans would begin creating their own laws on privacy of the mail. In 1792, under the constitution the United States Post Office was able to

---

[14] Seipp, *The Right*, [7-12].

[15] Seipp, *The Right*, [8] : "9 Anne. cap. X 40."

have a law that penalized anyone for opening, delaying or destroying another person's mail. The law was similar to one passed by the Continental Congress in 1782.[16] This was the earliest seen regulations put into place for the United States postal service. However many historians will argue it effectiveness. There was still instances of people's mail be tampered with during delivery. It was difficult to get the mail through the postal service without it being read. Even George Washington and Thomas Jefferson struggled with their letters being opened by the postal service during their presidencies. The lack of trust in the postal service and its officers lead to many people sending their mail by the way of private messengers and friends. As time went on, the regulations put into place became more effective and created a better sense of security within the postal service. There were regulations being put into place, but it wasn't until the post-Civil War era when tensions around secession died down that the United States Post Office could operate without any major threats to interference.[17]

The idea of being able to mail something across the world and not having it looked at before arriving at its desired destination is something that everyone is used to today, but this wasn't always the case. In fact, this was an idea that Ralph Waldo Emerson was fascinated with. Emerson found fascination in the sanctity of the mail stating "To think that a bit of paper, containing our most secret thoughts and protected only by a seal, should travel safely from one end of the world to the other, without anyone whose hands it had passed through had having meddled with it."[18] Today we don't think that our letters would be read if we mailed them, but this was definitely a possibility late into the nineteenth century. Emerson's fascination with this

---

[16] Solove, "A Brief," [6].

[17] Seipp, *The Right*, [7-15].

[18] Ralph Waldo Emerson, quoted in Frederick A. Currier, Postal Communication, Past and Present (Fitchburg,Mass 1894) p.4 see also Emerson "Civilization," in Works (Riverside edition) v.7, [26]

idea of safely delivery mail is something that many people take for granted today. It seems almost necessary and part of American ideals today.[19]

Census

The idea of a census was nothing new by the time of post Revolution America. In fact, the Romans used a census and there are even mentions of it in the Bible. The United States first established a periodical national census in it federal constitution of 1787. The goals of the census were politically driven. Americans wanted better representation, which would be based on population and the census could help determine how much representation each state would have. Suspicion around a census was not a new idea either, this was something that also made its way into the colonies from Europe. The backing for this suspicion is that people feared that something ominous would come from numbering citizens.[20]

The first census in America was faced with some backlash from the people. The main fear of the people was that the census would begin to ask more question and the government would demand more information from them. The first census wasn't met with too much backlash, but it was later when more questions actually where added that problems began to arise. A particular incident was from the 1799 census, which asked questions on the number and size of windows, in order to help house taxes. There were even accounts of protest in Northeastern Pennsylvania due to these new questions. This incident points out the location that had the most problems with the census, which was nearly always rural areas. People in cities did not seem to mind the additional questions as much as those people from rural areas.[21]

---

[19] Seipp, *The Right*, [6-7].
[20] Solove, "A Brief," [6].
[21] Seipp, *The Right*, [16-21].

It was unclear if the backlash was due to ideas of individual privacy or privacy from the government. As the nineteenth century wore on, the economic questions of the census began to ask question that sought more information, for example occupation, agricultural and slave holdings, raw materials owned, wages, kinds of machinery held and much more. These questions created many problems, and sometimes were not even answered by some people. The refusal to answer the economic question also seemed to come from the rural areas of southern states. In 1850, a promise of confidentiality came out, which stated that no personal information would be published. Any information that might be published would be connected to a greater part of facts and it would be impossible to single one person out. The census opened many people's eyes to the need for the need for privacy that would need to come from high up in the government.[22]

Although, there is something to be said about American privacy from the census and the postal service there were no laws put into place for privacy. The advances in the postal service and the census were very small, but pushed the people and the government's thinking in the right direction regarding privacy. Industrialization and urbanization that came following the Civil War, would have profound effects on American life and how information was handled. Changes in life and economics changed the way people's expectations of privacy. People began to protest against government and big business on the behalf of Americans right to privacy. The rights to privacy come from those specifically given in the Bill of Rights.[23]

---

[22] Seipp, *The Right*, [22-25].
[23] Seipp, *The Right*, [6].

Privacy Today

The American feelings toward privacy has evolved out of these early views and needs of the first American citizens. The framework for privacy has been constructed since the time of Independence. At that time, no would be able to tell how much things in America would change, especially with regards to technology. We are at a time now were the potential capabilities of technology are limitless, specifically in the case of monitoring and surveillance. These two action have direct drawbacks on privacy. Ralph Waldo Emerson wrote, "I become a transparent eye-ball" in one of his famous essays "Nature". In today's society, where we there is constant surveillance, this image has taken on a much scarier meaning. New technology has allowed for the transparent eyeballs to have their own place in society. Transparent eyeballs follow us everywhere we go, they are present in the cameras that are perched in and around buildings, on the corner of intersections, and on everyone's cellphones and laptop computers, which are constantly watching us. This is concerning for many people because our actions can be constantly monitored, however the Fourth Amendment does offer some needed protection.

As discussed earlier, the Fourth Amendment specifically gives privacy rights to American citizens. The language in the amendment is such that we are given rights based upon past actions that wrongfully invaded privacy of others. The Fourth Amendment clearly goes against any form of "unreasonable searches or seizures," and promises the American people the right "To be secure in their persons, houses, papers and effects." In recent years, there has more pressure, in courtroom, on the specificity of rights given by the amendment. Judges and lawyers have scrutinized the language written in the Fourth Amendment, working to establish just how much privacy we are actually granted. In 2014, two cases reached the Supreme Court that dealt with the specific rights given by the Fourth Amendment. These cases asked whether or not the

Fourth Amendment allows police the right to seize a cellphone from a suspect. In both cases, police officers went through cell phones of had been confiscated upon arrest. The issue was whether or not these officers needed a warrant to access the information on the cell phones. This is an issue that has become more prominent within the last couple years. It was ruled that the searching of the cell phones were unlawful and that in order to search any mobile phone a warrant is required[24]. American lives are becoming more visible to the transparent eyeballs of the future, which has created controversy that will only continue and the Fourth Amendment is right at the center of the controversy[25].

Privacy in America today has some of the same aspects of the first ideas that came with first settlers from Europe. These ideas of not having others eavesdrop or pry into one's private life, a regulation of the government, and the sanctity of a person's home. These fundamental ideas can still be seen in the concept of American privacy today, just adapted to the changes that have occurred, especially with the respect to technology. Technology has done wonders for society, but at the same time has created some drawbacks when it comes to privacy. Today, it has become so much easier to know private details about people, even someone you may have never met. That is a scary thought for many people. Technology has provided civilians with better capabilities of monitoring others than the US government had for multiple decades. It is hard to imagine the capabilities of today's US government.

The government is still the top concern when it comes to American ideas of privacy. As we have seen, the government has always been a topic of concern when it comes to our privacy,

---

[24] *SUPREME COURT OF THE UNITED STATES*, report no. 13-132, October 2013, https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

[25] Ted Widmer, "How Privacy became an American Value," BostonGlobe.com, last modified May 18, 2014, accessed February 2018, https://www.bostonglobe.com/ideas/2014/05/17/how-privacy-became-american-value/fVrcUTX0h2M39HcjOtBbIN/story.html.

long before invention the internet. The internet is just one example of technology being used as a medium to restrict privacy. The internet allows for many people to communicate across the globe. It provides a great service, but also some dangers. We can never really be sure who is on the other side of the screen, as well as, who has access to what, and who can read what. As an example I will use email, you can email anyone from anywhere as long as you know their email address. This is great invention for communication, however there are some privacy concerns. Private messages between two individuals, theoretically, should be between just those two individuals or anyone they may share it with. However, we can never really know who has access to it. Is it possible a hacker is going through your email? Is it possible the government is going through your email? Is it possible your neighbor is going through your email? Yes, all are possibilities, maybe unlikely possibilities, but possibilities nonetheless. This type of privacy invasion is just like the idea of eavesdropping that came with the settlers from England, only now there are more opportunities for our privacy to be invaded. One of the scariest aspects of these new privacy concerns, is that we could have no idea that any of them are happening. Private email conversations could be read by anyone who has the capability of getting into your server, whether that is by hacking into it, or simply negligence.

The basis for many Americans feelings towards privacy in today's society is how secure anything they do online is, and whether or not they can do anything private online without worrying if it is private or not. The first concern for an individual would be doing everything on their side to keep their information private. The way of going about this would be protecting against others getting access to private materials. This would be by having a strong password and not letting others know the password, not keeping private information open for others to walk by and get into, and other things along those lines of not being negligent. This would protect

someone from accessing information from the individual's side. The next step is to protect against a hack or a breach. This can be done by having the correct software to deal with hacks as well as carefully monitoring what you access and download. This is a little harder to do, but still doable. There is again room for negligence that one should be aware of, knowing which sites to browse, links to click, and downloads that are safe. Phishing emails are always good to be aware of, and can usually be spotted because they look off.

In 2013 there were many reports on Edward Snowden and the revelations on government surveillance, this would open the eyes of many Americans about the issues of privacy, and specifically online privacy. As stories began to develop and new details emerged, so did the debates on privacy. In the years to follow, the public would also become aware of the major security breaches of large health insurance companies, financial institutions and large retailers. These events have had a big impact on the way people view privacy. There are some people who find these developments troubling and restrictive towards our right, and want limits put into place for our protection. While on the other side, there are other who believe these issues do not affect them. Many of these later people, feel that innocent people should have nothing to hide and that monitoring can have many benefits for social safety and security.

In June of 2013, Edward Snowden, a government contractor, leaked information about the National Security Agency (NSA). Snowden's leaks informed people of the NSA's surveillance of Americans' online and phone communications. As stated earlier, this helped start a public interest and debate on privacy issues. One specific topic was whether government surveillance served a useful purpose in an anti-terrorism effort or was just a strict violation of our privacy rights. A 2014 survey by Pew Research Center, had equally divided results on whether Americans believe that Snowden's leaks harmed or served public interest. Government intrusion

has always been a concern for Americans with regards to privacy. This Snowden case is a specific example of government intrusion. It can be said that the government should be allowed to continue such surveillance because it is being used to protect us. On the other hand, it is also believed that this gives too much power to the government, and this could lead to further and more extensive intrusions on our privacy. The government believes they can do these things because it could help stop terrorism. Many Americans don't believe this is an adequate excuse for monitoring citizens. In fact, 65% of American adults believe that there are not proper limits on internet and telephone data that the government collects[26].The majority of Americans don't believe that there is enough limitations on the government in regards to privacy. The public usually agrees that it is acceptable for the government to monitor others for our safety, but this includes foreign citizens, foreign leaders, and American leaders. Majority of people believe individuals who search specific words such as "explosives" and "automatic weapons" or frequently visit anti-American websites should be monitored. However, most people would agree that it is unacceptable for the government to monitor communications between citizens.[27] Obviously, this frustration with government intrusion on Americans privacy is still a major issue.

[26] Lee Rainie, "The state of privacy in post-Snowden America," Pew Research Center, last modified September 21, 2016, accessed February 2018, http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.
[27] Rainie, "The state," Pew Research Center.

Chapter Two:

Privacy as a Dynamic Idea in American Culture Today

Currently, historical understandings of privacy in America are changing. On the one hand, valuing privacy is well established in American Culture. Legal decisions and cultural commentary from the past established that Americans see it as important to protect their privacy from a) government intrusion and b) intrusions coming from other citizens whether in the form of libel, slander, disclosure of personal information, and/or negative statements that compromise their reputations. Courts have even confirmed this.

However, we are at a point in history where we are constantly sharing information. Technology is allowing us to connect in ways that we may not be prepared for. These innovations give new opportunities to share information and ideas as well as new ways of interacting with others. Considering the constant innovation, how persistent are these ideas of privacy in the contemporary period?

Privacy is becoming more and more dynamic in the twenty-first century and this may be due to the fact that social organization has changed and continues to change. Privacy has become dynamic because our lives are constantly changing with the development of new technologies. Looking back into our history served a purpose by finding where our beliefs and traditions for privacy courts come from as Americans. Courts have confirmed our beliefs and proved that is one of our rights as citizens. However, new technologies and new forms of social organization have created constant changes to the way people view privacy. New technologies make interactions between people more convenient but much less personal. This has also changed the way we interact in our social networks, which are now almost exclusively online. These factors

play an important role on how Americans view privacy and what concerns they have toward their privacy. As technology continues to develop and become more innovative our social networking and interactions will also continue to change, as a result, privacy will only become more dynamic.

In *Bowling Alone:The Collapse and Revival of American Community*, Robert Putnam describes declining social engagement throughout the twentieth century. Putnam explains how memberships in social clubs and organizations significantly decreased throughout the twentieth century. The Roanoke, Virginia chapter of the National Association for Advancement of Colored People (NAACP) is one example. The number of memberships decreased from about 2,500 to a few hundred throughout the 1990s. Similarly, the Veterans of Foreign Wars (VFW) Post 2378 in Berwyn, Illinois had so few memberships in 1999 that it struggled to pay taxes. Putnam gives more examples including a Boston area High School that in 1999 had brand new marching band uniforms sit in storage because so few students joined.[28] The first sections of the book describe the civic engagement trends that have led to a diminishing social capital throughout the twentieth century.

> ...the broad picture is one of declining membership in community organizations. During the last third of the twentieth century formal membership in organizations in general has edged downward by perhaps 10-20 percent. Most important active involvement in clubs and other voluntary associations has collapsed at an astonishing rate, more than halving most indexes of participation within barely a few decades.[29]

The memberships in organizations throughout the last part of the twentieth century began to drop, which Putnam believes negatively affected social capital. Fewer memberships means less

---

[28] Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community* (New York: Simon & Schuster, 2000), [15].
[29] Putnam, *Bowling Alone*, [63].

community engagement, as if the population is becoming more isolated, which leads to a lower social capital[30].

The declining membership of social organizations described was not due to the fact that old members are leaving. Rather, there were no new members being added; these organizations are not being revitalized with new participants. The 1960s signaled a potential threshold for involvement in these community groups. The postwar baby boom resulted in a young population of Americans who might positively affect community involvement. The potential for civic engagement in America had greatly increased. Surprisingly, that was not the case as it actually declined by the end of the century.[31]

Putnam describes this change in character of American society of decreasing civic engagement in terms of social capital. The idea behind social capital is that social networks have value[32]. Putnam clarifies social capital in this way:

> Whereas physical capital refers to physical objects and human capital refers to properties of individuals, social capital refers to connections among individuals-social networks and the norms of reciprocity and trustworthiness that arise from them. In the sense social capital is closely related to what some have called "civic virtue." The difference is that "social capital" calls attention to the fact that civic virtue is most powerful when embedded in a dense network of reciprocal social relations. A society of many virtuous but isolated individuals is not necessarily rich in social capital.[33]

In other words, a society benefits from its collective social capital the more that individuals coming together on a regular basis in their communities. The more individuals connect in order to take part in community life, the higher the social capital. Engagement of individuals helps a community because the interactions allow for the exchange of ideas and things for mutual

---

[30] Putnam, *Bowling Alone*, [63]
[31] Putnam, *Bowling Alone* [65]
[32] Putnam, *Bowling Alone* [65]
[33] Putnam, *Bowling Alone* [19]

benefit. These interactions also foster trust between community members. Putnam infers that "social capital is a cause, not merely an effect, of contemporary social circumstance."[34]

Putnam shows that Americans are not happy with their social isolation. He states that "Americans today feel vaguely and uncomfortably disconnected," and that "we wish we lived in a more in a more civil, more trustworthy, more collectively caring community."[35] By lamenting the growth of isolation, Putnam's book is somewhat of a critique of privatistic behavior by individuals and a call for renewed social connections. In other words, too much privacy and the protection of it can be a bad thing.

The second part of the book identifies technology as the reason for the diminishing social capital in America throughout the last third of the twentieth century--specifically the appearance of television after World War II and its total embrace by Americans. (But as will be discussed later, technology could also be presented as a way of reconnecting socially.) People who have TV as their "primary form of entertainment" engage less in the community in all aspect because most of their free time is taken up by sitting around watching television. He explains, "TV dependence is associated not merely with less involvement in community life, but with less social communication in all its forms- written, oral, or electronic."[36] People who are more dependent on TV are way less likely to interact in their communities than those who are not as dependent on the TV for entertainment. In fact, Putnam figures that those individuals dependent on TV for entertainment only volunteer on average of 4 times per year compared to 9 times a year for individuals who are not dependent on TV.[37]

---

[34] Putnam, *Bowling Alone*, [294].
[35] Putnam, *Bowling Alone*, [402].
[36] Putnam, *Bowling Alone*, [231].
[37] Putnam, *Bowling Alone*, [231-234].

The second and "single most important cause of our current plight is a pervasive and continuing generational decline in almost all forms of civic engagement."[38] Younger generations are not as willing as older ones to engage in community efforts. This goes also goes along with the first factor, because younger generations have more attachment to the television.

The final two factors that have led to a declining social capital are pressures on time and money as well as mobility along with mobility and sprawl. Americans are always trying to use their time the best they can, and most people would rather spend time making money rather than volunteering in community engagement[39]. Putnam agrees with Walter Lippmann and quotes him saying "we have changed our environment more quickly than we know how to change ourselves."[40] American's environments are constantly changing and it happens so rapidly that they are not always aware and cannot adapt to these changes. Not being aware of these changes hinders social capital because individuals are not conscious of how important their role in the community actual is.

In the third part of the *Bowling Alone*, Putnam describes the negative consequences that a diminishing social capital has and builds the case for Americans to weigh the cost of excessive privacy and private living. Specifically, he discusses how the decrease in social capital affects children's welfare, safety and productivity of neighborhoods, health, democracy, economic prosperity and education. Not enough social engagement is bad for all these aspect of the community and may prevent prosperity.[41]

---

[38] Putnam, *Bowling Alone*, [404].

[39] James A. Montanye, "Bowling Alone (Book Review)," *Independent Review* 5, no. 3 (Winter 2001): http://web.b.ebscohost.com/ehost/detail/detail?vid=3&sid=4210404c-1558-44b9-bb15-a21255be7619%40sessionmgr103&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=4097410&db=aph.

[40] Putnam, *Bowling Alone*, [402].

[41] Putnam, *Bowling Alone*, [404].

However, in an almost prophetic way, Putnam argues that too much social capital is also not healthy for a community either. He warns that "A single-minded pursuit of social capital might unacceptably infringe on freedom and justice."[42] Overly aggressive social capital could turn out to be a bad thing and go against ideas of personal liberty. It can be argued that this concern reflects the historical fear that American have against governmental interference with privacy.

The final section of the book, Putnam recaps the social movements that defined the Gilded Age and the Progressive Era. These were important eras of American history that helped create a strong and abundant stock of social capital, which would later dissipate throughout the last quarter of the twentieth century. As Putnam puts is, "...my message is that we desperately need an era of civic inventiveness to create a renewed set of institutions and channels for a reinvigorated civic life that will fit the way we have come to live."[43] Social capital may have started to dissipate, but a push toward more community engagement in new modern ways can get us closer to where we want, where Putnam believes we should be.

I believe that Putnam's observations are very important for understanding Americans' dynamic views of privacy. The reduction of engagement in communities means that people are either isolating themselves or finding new ways to interact and socialize. My theory is that internet changed the way people interact so much, that it has changed the idea of the community. It is no longer just the physical community but also a digital community. Although people are not engaging as much in their physical community, there is more and more engagement in the digital community.

---

[42] Putnam, *Bowling Alone*, [404].
[43] Putnam, *Bowling Alone*, [401].

It is important to analyze the reason social network sites have become so popular to better understand why people continue to share personal information online. I will do this by looking at the most popular online social network, Facebook. A case study determined two primary needs that have attributed to motivating Facebook users. These are a need to belong and a need for self-presentation.[44] There are many factors that contribute to the need to belong and the need for self-presentation that are demographics, culture and personality traits such as introversion, extraversion, narcissism, shyness, self-esteem and self-worth. These factors lead to members being broken into two groups, individualistic members and collectivistic members. Collectivistic members pursue the need to belong, that contributes to these members having more frequent interactions and close circle of "friends" online. Individualistic members pursue the need for self-presentation, which is responsible for members feeling the need to share more private information.[45]

The need to belong and the need for self-presentation can also been seen as factors that Putnam would argue lead to the increased social engagement during the first third of the twentieth century. These needs were met by individuals going out and getting more involved in their community. As times changed, Americans were no longer engaging in their communities. However, these needs were still present in society, individuals just need new ways to fulfill them. The internet is the perfect platform to fulfill these needs, and social network sites were able to facilitate virtual communities for individuals to interact. As individuals try and fulfill their needs to belong and for self-presentation, they also feel the need to share more private information. The increased sharing of private information is contributing to changing views of privacy.

---

[44] Ashwini Nadkarni and Stefan G. Hofmann, "Why do People use Facebook?," *Personality and Individual Differences* 52, no. 3 (February 2012): [243-249], doi:10.1016/j.paid.2011.11.007.
[45]Nadkarni and Hofmann, "Why do People," [243-249].

Social capital is present in these digital communities. There is great value in being connected with a digital community. Communication is fast and convenient, which allows for a broader and more efficient spread of ideas. In actuality, online social networks could provide for an increased social capital. A digital community could allow greater participation, because people do not actually have to be in one location. A digital community is no longer just the people around you, it is everyone you can connect with online, which is basically anyone who can get on the internet. The internet has provided a great opportunity to connect the world, which is a very valuable in terms of social capital, because we can connect with an online social network almost the size of Earth's population in a matter of seconds. Online social networks are rapidly growing. Memberships to social network sites has experienced exponential growth throughout the past couple years. It is estimated that about 68% of Americans have a Facebook account.[46]

Online social networks are so important to privacy because they basically share peoples' information throughout the networks. "At the most basic level, an online social network is an Internet community where individuals interact, often through profiles that (re)present their public persona (and their networks of connections) to others."[47] The way people interact in online social networks is self-representation through sharing of information, usually personal. This is where privacy concerns start to present themselves. The more involved individuals get in online social networks the more information they are putting out onto the internet. The concerns of individuals

[46] Aaron Smith and Monica Anderson, "Social Media Use in 2018," Pew Research Center: Internet, Science & Tech, last modified March 1, 2018, accessed April 2018, http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/.

[47] Alessandro Acquisti and Ralph Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Privacy Enhancing Technologies*, 2006, [2].

is how private that information really is, and who has access to it. As social networks online are becoming more popular, we see attitudes towards privacy changing.[48]

The internet has created a whole new way for individuals to connect to each other, by communicating and sharing information and ideas. A message can be sent to anyone in the world in the matter of seconds. As new technologies that help us connect to the internet are being produced we are being introduced to new ways of interacting with others. Internet communication and online social networks are changing the landscape of these interactions. Conversations that were once considered "over-the- fence neighbor chat" or "backyard conversations" are now being played out through cell phones or computers that might be between people miles apart. Online social networks are changing the landscape of conversation even more because they broaden the scope of conversations. As Putnam pointed out in *Bowling Alone*, social engagement creates wider friendships and larger interest groups allowing for a larger "living room" of conversation. Online social networks are taking this even further, and the "living room" for conversation is now infinite because of the virtual aspect.

Privacy concerns on the internet are similar to earlier privacy concerns that have been discussed. Mainly, disclosure of personal information, reputation, and surveillance. These concerns are enhanced by online social networks because individuals are willingly choosing to put their information out into these networks. Once the information is put into these networks, it is at risk of being compromised. "Specific privacy concerns of online social networking include inadvertent disclosure of personal information, damaged reputation due to rumors and gossip, unwanted contact and harassment or stalking, surveillance-like structures due to backtracking

[48]Acquisti and Gross, "Imagined Communities," [3].

functions, use of personal data by third parties, and hacking and identity theft."[49] The greater an individual's presence in these online social networks the more prone they are to be a victim of an attack by one of these privacy concerns.[50]

The "friending" option on Facebook may be another reason that Americans so easily give up their privacy on this social network site. Research has shown that Americans have a rather unique view of who they consider friends. Compared to other cultures, Americans are fairly quick to call someone a friend. Americans are more individualistic than people from many older cultures where deep, long, generational ties and relationships form the basis of friendships. When Americans interact with many foreigners, the foreigners are often surprised at how quick we are to invite them to our house or to go out with them socially. These interactions are often reserved for others with whom a person has a highly developed connection with in other cultures. One study, for instance, shows that West Africans tend to view friendships as a voluntary relationship, which requires acts of affection not just scripted obligations. Western Africans also feel less motivation for new friendships, because that would devalue previous friendships.[51]

Recently in the news there have been lawsuits regarding privacy concerns with Facebook, one of the most popular online social networks. Two specific cases from recent years have dealt with slanderous post, which coincide with privacy concerns of damaged reputations. The first case is a North Carolina woman who had to pay $500,000 to settle a defamation lawsuit. This story is from August 2017, and the woman being charged posted one sentence on Facebook about a former co-worker, in which she did not even mention a name. The post in question read

---

[49] Bernhard Debatin et al., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Computer-Mediated Communication* 15, no. 1 (October 1, 2009): [84].

[50] Debatin et al., "Facebook and Online," [84].

[51] Glenn Adams, "The Cultural Grounding of Personal Relationship: Enemyship in North American and West African Worlds.," Journal of Personality and Social Psychology, July 2005, [335], DOI:10.1037/0022-3514.88.6.948.

"I didn't get drunk and kill my kid," referring to the former co-worker. The co-worker sued for libel, a written statement that is slanderous, because she was not responsible or drunk during her child's death. The lawsuit was settled after two years, the woman had to woman had to pay her former co-worker $250,000 for actual damages, the emotional distress and defamation, and $250,000 for punitive damages.[52]

The next story is more recent from March of this year, also deals with a Facebook post. In this case, a Georgia woman is seeking compensatory and punitive damages resulting from being wrongfully jailed. The woman spent four hours in jail before posting bail, because of an arrest warrant by her ex-husband and sheriff deputy for her "derogatory statements" on Facebook. The case was later dropped because it was decided by that there was no basis for the arrest. The post stated "That moment when everyone in your house has the flu and you ask your kid's dad to get them (not me) more Motrin and Tylenol and he refuses," which also included and "overwhelmed" emoji. The lawsuit is being filed because this is not really a slanderous post, because it is just an overwhelmed reaction; and according to a 1982 Georgia Supreme Court decision a person cannot be charged with criminal defamation[53].

These cases are just two of many that have risen since the advent of Facebook and other online social networks. It is interesting, however to look at the responses to these privacy concerns that Americans have from using online social networks. These two specific cases dealt with reputation damages. The response in the first one is that the individual whose reputation may have been damaged was given financial compensation. This was due to the fact that there

---

[52] Lindsey Murray, "Consider This Your Warning to Be Extra Careful About What You Post on Facebook," Good Housekeeping, last modified April 17, 2017, accessed January 2018, https://www.goodhousekeeping.com/life/news/a43755/facebook-defamation-lawsuit/.

[53] "Georgia Woman Badmouthed Her Sheriff's Deputy Ex-Husband in a Facebook Post, So He had Her Arrested: Lawsuit," KTLA, last modified March 9, 2018, accessed April 2018, http://ktla.com/2018/03/09/georgia-woman-sues-ex-husband-for-having-her-arrested-over-facebook-post/.

was a slanderous post written about them. In the second case it is a little more confusing, an individual was wrongfully jailed for a post that was thought to be slanderous, but in fact was not. In both instances, the victim of damaged reputation is seeking some type of compensation for slanderous information being posted on the internet.

Online social networks pose great threats to users' privacy because they are based on profiles that include various amounts of individual's personal information. However, they are extremely popular and continue to bring in more memberships every year. Users of online networks are constantly trying to manage the privacy risk and the perceived benefits. One of the most beneficial aspect of online social networks is the social capital gained by creating and maintaining interpersonal relationships.[54] Social networks on the internet, allow for people to connect across the globe creating relationships that were once thought to be impossible, but also puts personal information at risk.

> Since the creation and preservation of this social capital is systematically built upon the the voluntary disclosure of private information to a virtually unlimited audience, Ibrahim (2008) characterized online networks as "complicit risk communities where personal information becomes social capital which is traded and exchanged."[p.251][55]

Now we are seeing personal information carrying a new value that can be used to connect with others online. In order to connect with better in these online networks, more personal information is needed. Online social networks are so popular, that people are willing to give more and more information.[56]

The willingness of people to give more and more personal information in order to participate in online networks is why privacy can be considered dynamic in America today.

---

[54] Bernhard Debatin et al., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Computer-Mediated Communication* 15, no. 1 (October 1, 2009): [87].

[55] Debatin et al., "Facebook and Online," [87].: Quoting Ibrahim(2008) page 251

[56] Debatin et al., "Facebook and Online," [87-88].

Americans are becoming less concerned with some aspects of privacy. The popularity of online social networks seems to suggest this. Online networks are heavily based on users providing personal information. Once the information is in these networks it is at risk of no longer private. These risk do not have a great effect on keeping people away from using online social networks. This is why the idea of privacy is changing for Americans as they embrace social media. Going further it seems that Americans are changing the way they think about private information.

As Americans are giving out more and more personal information on the internet, it is reasonable to question what we actually consider private and what we consider public. There is almost no limit on the information you can find on the internet, especially about other people. Most of this information has been provided by the individuals themselves in one way or another. The fact that the internet has all this personal information, suggests that Americans are no longer concerned with keeping this information private. The specific privacy concerns that arise from social networks still follow concerns that traditionally arose in America. However, the line between public and private is becoming less distinct. As Americans continue to embrace technology and social networks, this distinction will continue to become less clear.

Privacy is a dynamic and unstable idea for Americans today, because we are constantly changing our ideas of what we consider private information. Americans have been fixated on social networks since they started to appear on the internet at the end of the twentieth century. These online social networks create a virtual community that allows individuals to interact through profiles based on personal information. As individuals become more involved in these social networks they begin to provide more information, in order to have a better presence in these networks. The popularity of these online social networks have changed the way Americans think about their private information. If providing more information benefits how they are

perceived in these social networks, then most people will provide the information. This is why the views of private information is changing. Individuals are becoming more concerned with their social media presence than their privacy. At the same time, it is becoming more acceptable to put more information onto the internet, breaking down the idea of private information even more.

Even as the *behavior* of Americans has changed regarding privacy on the internet---we share more and more information about ourselves in cyberspace, whether through social network sites or in business transactions--our basic *ideas and beliefs* that privacy is something that should be protected seems to be as strong as ever. For instance, when asked whether they think digital privacy and privacy protections are important, Americans respond yes. For example, quora.com, a question-answer website started, ironically, by a Facebook co-founder, polled its using by asking, "In your opinion, is it important to protect online privacy when using social networking sites?" Here are a couple of responses typical of the ones posted between 2013 and 2017:

> My privacy is very important to me whether it's on the Internet or in real life. This is why I don't have pictures of myself anywhere online. I also know not to post too much information in social media and I never vent online since I never know who will be seeing it. Facebook, Instagram, Twitter or any other social media site shouldn't have to monitor, or censor, what their members put on there. It's up to us, as adults, to think before we post. It's also up to us as parents to teach our kids how to be responsible when they are on the Internet. If they are taught what is appropriate and what is not, their privacy, as well as their family's privacy, will stay safe. The minimum age a child could have social media is 13, however, few kids that age have the maturity to to online responsibly. It also doesn't help that parents lie about the kids ages so they can go on social media when they are 7. I just hope these parents are keeping a close watch on these kids. [57]

> I would say yes. Internet users started to be more concerned about their own data. Even if companies like Facebook don't charge them for using their platform, it doesn't mean they don't get money out of that. Selling clients'

[57] Alexandra Olynik, Quora update, February 16, 2014, https://www.quora.com/In-your-opinion-is-it-important-to-protect-online-privacy-when-using-social-networking-sites.

> data to others is an old profitable business tactic. This is proof for all those targeted advertising campaigns that invade your social media profiles. There were a few companies that tried to revolutionize the internet world, by introducing the "keep your data secured" concept. They didn't succeed mostly because of the internet ecosystem (back then users' data wasn't explored so intensely). Nowadays, people seem to be more responsible with regard to their personal information, so there's a big need for digital identity protection... [58]

Similarly, a Pew Research Center poll in 2017 found that 68 percent of Americans feel there is a need for more privacy protections. Pew has also found that "young adults are more focused than elders when it comes to online privacy."[59] These feelings of a need for more privacy protection are fueling new legal support for personal information in the United States. One way that information on the internet can be protected would be to put limits on the how long records of activity and information are stored. Americans are very much in favor of putting these limits into place. Many people currently try and protect their privacy online by taking steps to mask their identity, and specifically through removing their names from tagged photos.[60]

To what extent has American society, whether through the private sector or business sector, responded to continuing concerns that Americans express about the value of their privacy and the need to protect it? In the next chapter, I will examine one major response, which is the growth of the cyber insurance industry. Cyber insurance does not protect individuals as much as it protect businesses that deal with other people's information. Why is this the case? Are individual privacy concerns so dynamic that we do not have a responses yet? If we better understand cyber insurance, we might be able to better understand privacy concerns.

---

[58] Emanuel Martonca, Quora update, July 22, 2014, https://www.quora.com/In-your-opinion-is-it-important-to-protect-online-privacy-when-using-social-networking-sites.
[59] Electronic Privacy Information Center," EPIC - Public Opinion on Privacy, https://www.epic.org/privacy/survey/.
[60] "Electronic Privacy," EPIC - Public Opinion on Privacy.

Chapter Three:

Cyber Insurance: The Solution That Is Not the Solution

Cyber insurance has arisen as the market's way of solving privacy problems in the digital age. As we have seen in the last chapter, Americans see the problem as two-fold--disclosure of personal information (about likes, dislikes, family, friends, and opinions) and disclosure of business and medical information (Social Security number, address, health profiles, and the like). This chapter analyzes the extent to which cyber insurance addresses these concerns. Throughout the chapter it will be noticed that cyber insurance does less to protect individuals as it does for businesses and medical groups. In analyzing this, it would appear that cyber insurance is actually not a solution because overall, its main function is not to protect the people, but mainly focused to protect the businesses.

Cyber Insurance is used to cover losses that are the result of a cyber-related data breach, hack, or any other loss of personal information. Cyber insurance is also referred to as cyber privacy insurance, cyber risk insurance, cyber liability insurance coverage.[61] In the event of a cyber-crime the organization that is victim to the crime, is responsible for the losses as well as compensation for other parties affected. These losses and compensations are the risks that organizations are faced with. Cyber insurance helps companies and organizations mitigate their risk by offsetting the cost of some type of data breach.[62]

---

[61] Brent Radcliffe, "Cyber And Privacy Insurance," Investopedia, accessed April 20, 2018, https://www.investopedia.com/terms/c/cyber-and-privacy-insurance.asp.

[62] Kim Lindros and Ed Tittel, "What is cyber insurance and why you need it," CIO, last modified May 4, 2016, accessed January 2018,

At the most basic description of cyber insurance, it appears that cyber insurance is used more to protect businesses and health groups than individual citizens. Cyber insurance also is not a protection against data breaches, but protection for the damages that result from a data breach. In most cases businesses or health groups would responsible in the event of a breach; so it makes sense that they would want to have some form of protection for the damages. An individual is still protected through cyber insurance because if a breach happens to a organization that has their information, they will be compensated. However, the main objective in cyber insurance is to protect large organizations and not individuals. The continued description of cyber insurance will further this point. This will prove that although cyber insurance is a response to privacy needs, it does not respond to privacy needs of individual citizens.

Insurance, in general, transfers risk from one party to another, it does not protect or prevent against a loss from occurring. Cyber insurance works in the same way, it does not protect organizations from cyber-crimes, instead it transfers the risk associated with a cyber-crime to the insurer. The insurers provide the financial support needed when an organization is faced with security threat. Basically, cyber insurance provides money, up to the amount agreed up in the policy, for organizations that fall victim to cyber-crimes, in order to cover the losses or pay-outs that have arisen. Cyber insurance is helpful because it can provide financial stability for companies after a cyber-attack. This type of insurance is useful for any organization that is a threat to cyber-attacks because of the fact that they store and maintain customer information, collect online payment information or use the cloud.[63]

Cyber insurance really began to catch on in 2005, and was originally rooted in errors and omissions (E&O) insurance. Errors and omissions is a type of professional liability insurance

[63] Lindros and Tittel, "What is cyber," CIO.

which protects the insured against claims that may arise from clients for negligence or inadequate work. Errors and omissions coverage covers the settlements, up to the amount in stated in the policy, as well as court costs.[64] According to PwC, PricewaterhouseCoopers, about one-third of US companies currently own some type of cyber insurance, and PwC also believes that the total value of premiums forecasted for cyber insurance will reach $7.5 billion by 2020.[65] The numbers prove that this is a rapidly growing market, and organizations are recognizing the need for cyber insurance.

Cyber insurance covers first parties' expenses, as well as third party claims, but there is no real standard for these policies. Even though there are no standards for what goes into a cyber insurance policy, there are four commonly reimbursable expenses. These expenses are investigation, business losses, privacy and notification, and lawsuits and extortion.[66] Insurance companies will pay out these expenses for a claim for the amount that is agreed upon in the policy. Investigation expenses cover the forensics investigation that are necessary for all claims. These investigations are used to determine what actually happened, how to repair the damages, and to prevent the same type of breach from happening again. Investigations are usually done by third party security firms as well as some work with law enforcement and the FBI if needed. Business losses expenses cover the first party for any deficits in business to a breach. These expenses are similar to items that are covered by and errors and omissions policy, as well as others, including monetary losses due to network downtime, business interruption, data loss recovery and costs involved in managing a crisis, which includes repairing damaged reputations.

---

[64] Investopedia, "Errors And Omissions Insurance - E&O," Investopedia, last modified March 10, 2018, accessed March 2018, https://www.investopedia.com/terms/e/errors-omissions-insurance.asp.
[65] "Insurance 2020 & beyond: Reaping the dividends of cyber resilience," PwC, https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html.
[66] Lindros and Tittel, "What is cyber," CIO.

This coverage helps companies in the event that a breach affects business operations. An example would be an online retailer's network being down, as the result of a breach, and not being able to bring in revenue. A cyber policy would cover these losses in profits by an insurer paying out some or all of the lost revenue. Privacy and notification expenses are for notifying all parties that may be affected by a breach. In most jurisdictions it is required by law that an organization that is victim to a breach must notify everyone who may be affected, usually customers. Included in these expenses is credit monitoring for customers who are or may have been affected by a data breach. Lawsuits and extortion expenses cover the all the legal fees that arise for a claim. These legal expenses are associated with release of any confidential information or intellectual property, legal settlements and regulatory fines. Included in these expenses is also the costs of cyber extortion, as in the case of ransom ware. In the case that a company is taken to court due to a cyber breach, the insurer covers the fees such a lawyers, settlements and any other payouts that may arise such as a fine.[67]

Cyber insurance is still a fairly new product that is still evolving. Cyber risks change frequently and there seems to always be new ones arising, especially with the influx in technological innovation. In many cases, organizations have tried to cover up breaches by not reporting the full impact and details of breaches, in order to protect against negative publicity and damage trust between customers. This only makes it harder for insurers to write these policies. The under reporting of cyber-attacks leave underwriters with limited data needed to determine the impact of a breach, especially the financial impact. Basically, the full risk of cyber-crimes are not yet fully understood even by insurers, which makes it suck a huge risk for all parties. The fact that cyber risk is so large but still relatively unknown, may be one reason for

---

[67] Lindros and Tittel, "What is cyber," CIO.

why cyber insurance is such a rapidly growing market. Many well-known insurance companies offer some type of cyber insurance policy, including Allianz, Chubb and Travelers. Industry experts believe that in the near future cyber insurance policies will be part of the product line for every business insurer[68].

Technological innovation in the late nineties created new risks associated with these advancements. As technologies grew larger so did their risk as well as the need and want to transfer the risk. This need to transfer the risk associated with new technology allowed for the first policies for technology to be written. The new policies being written, at first, were for the growing media and content exposure that these new technology companies now had. These policies eventually evolved to increase and change coverage. The late nineties is also when the first cyber policies started hitting the market. Many people take credit for writing the first policy so it is relatively unclear who actually did. Most of the first cyber policies varied on their basic coverage. Many of the these first cyber coverage were media policies that covered online media and some errors in data processing (EDP) policies. The first cyber policies were mostly all evolved from professional liability policies for software and media risk.[69]

At the change of the decade the cyber policies began their first change, to cover more risk. The online media policies began to cover new risks associated with the internet, this covered claims for "unauthorized access", "network security" and "viruses".[70] As these online media policies changed, they started to exclude coverage that most professional liability policies normally would. Coverage that might have been excluded included rogue employees, regulatory

---

[68] "Insurance 2020," PwC.

[69] ProWriters, "The History of Cyber Insurance," Cyber Insurance Blog, entry posted April 25, 2016, accessed March 2018, http://prowritersins.com/the-history-of-cyber-insurance/.

[70] ProWriters, "The History," Cyber Insurance Blog.

claims, fines and penalties, as well as not having first party coverage.[71] Meaning that the policy holder was not being covered, third parties were being covered, those who used or accessed the service of the policy holder.

Towards the mid-2000s was when we see policies change and have first party coverage. A few examples are Cyber Business Interruption, protecting losses that may occur for online businesses, Cyber Extortion and Network Asset Damages. These policies that covered first parties also evolved to add a sublimit on losses associated with HIPAA liability. Basically putting a limit on how much an insurer would have to pay out on a loss from a data breach associated with HIPAA liability[72].

The HIPAA is the Health Insurance Portability and Accountability Act of 1996, enacted on August 21, 1996, was put into place by the Department of Health and Human Services (HHS) to protect individual's personal health information. In order to implement the requirements for this act the HHS created the Standards for Privacy of Individually Identifiable Health Information which is also known at the "Privacy Rule". The Privacy Rule established, for the first time, national standards for protecting certain health information. These standards are used to address how individuals' health information, protected health information, is used and disclosed by organizations that are subject to the Privacy Rule, these organizations are called covered entities. There are also standards for how individual's privacy rights in order to control and understand how their personal health information is being used[73].

The goal of the Privacy Rule is to protect individuals' health information while at the same time permitting a proper flow of information between systems to allow health care systems

---

[71] ProWriters, "The History," Cyber Insurance Blog.
[72] ProWriters, "The History," Cyber Insurance Blog.
[73] "Summary of the HIPAA Privacy Rule," HHS.gov, last modified July 26, 2018, accessed February 2018, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

to have the proper information needed for public health and wellbeing to run efficiently. This rule promotes a good balance between information that is needed for well-run health care systems, as well as individuals' privacy. The privacy rule goes into much detail on the uses and disclosures of health information between health care providers, insurers, individuals and law enforcement. According to the HHS government website, individually identifiable health information is considered to be "is information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual." Basically, any information that can be used to easily identify an individual. Failure to follow the Privacy Rules, can carry civil monetary penalties, as well as, criminal penalties depending on severity of the violations. Penalties for violations are dependent on the nature and extent of the exposure as well as the nature and extent of the harm that resulted from the violation.[74]

Cyber insurance was largely affected by the California Security Breach and Information Act, which went into effect on July 1st in 2003. This legislation significantly changed the way that organizations would have to deal with a cyber breach. The act required any company that does business in California to notify any affected resident of the state about the breach, if personal information is believed to be or was accessed by unauthorized personnel. According to the act, personal information means a person's first and last name in combination with driver's license number, social security number and credit or debit card numbers or passwords. This act help set a precedent for dealing with a breach, as well as helped create another evolution for

[74] "Summary of the HIPAA," HHS.gov.

cyber insurance. As a result of this act, many states began adopting their own laws on how a data breach must be handled, that very were similar to the California act.[75]

As cyber insurance began to evolve again because of these new laws, many insurance companies started to offer new coverage, for both first and third parties. Among these new first party coverage were the inclusion of IT Forensics, PR, Credit Monitoring / Repair, and Customer Notification. The new third party coverage created the availability for Regulatory Defense & Fines / Penalties, PCI Fines and Penalties. Altogether, the California Security Breach and Information Act, was very influential for cyber insurance for both the insured and the insurers.[76]

A difficulty in the early years of cyber insurance was the amount of exposure an insurer was willing to take and reinsurance, basically insurance for insurance. This was all due to the fact that cyber insurance was very new. This stage in time is best summed up by Pro Writers cyber insurance blog, where they state:

> In the late 2000's many of the coverages being offered were only available with a small sub-limit as carriers and reinsurers were concerned about the new exposures and how to price for it. It was difficult for an insured to get the limits they desired for certain exposures and it made excess placements difficult as the excess markets were not comfortable with other carriers forms, pricing, sub-limit structure, and offering drop down limits over the sub-limits.[77]

Coverages that were only offered with small sub-limit, helped carriers keep their exposure low, because they would only have to payout small amount based on the limit, and only for specific cases. Reinsurers then had to decide if they wanted to also take on some of the risk, which was even more difficult because it was hard to tell how much exposure the carrier had because of the small sub-limits carriers were using and the obscurity of the risk. It was also difficult for those

---

[75] ProWriters, "The History," Cyber Insurance Blog.
[76] ProWriters, "The History," Cyber Insurance Blog.
[77] ProWriters, "The History," Cyber Insurance Blog.

interested in these policies, because for certain exposures that they would want to be covered for they had a hard time getting a desirable limit, how much they would be covered for, to cover their risk.

The final difficulty this new insurance market had was with excess, which is a way of covering limits. Excess is basically splitting the risk, if a company has a limit on a certain risk another company can take the excess and cover the losses that are above the limit. The excess market was problematic at this point, because each carrier differed in the way they were writing their policies. The next decade would be even bigger for cyber insurance, there was tremendous growth and opportunity and data breaches started to become a commonplace. There were now many more insurers who wanted in on the new market and offer their own cyber coverage.[78]

Throughout the 2010s, the number of carriers who offered a stand-alone cyber insurance product grew above 50 and now it is even past 60. Carriers began to see the opportunities that the cyber market offered to take on new risk and that could be very profitable. It wasn't long before claims started coming in as the result of breaches, especially large ones. In 2014 so many retailers became victim to large data breaches that it became known as the year of the Retail Breach. A few of the affected retailers included Target, Staples, UPS, Home Depot, Dairy Queen and many others. The next year, in 2015 the same thing happened to the Healthcare industry making it the year of the Healthcare Breach. Companies affected by that year's breaches included Excellus BlueCross BlueShield, Premera Blue Cross, OPM, Anthem, and a few others. Each single breach affected millions of people's information. It was now apparent that there was a large cyber threat and that cyber insurance would be needed. In 2016 and 2017 cyber insurance

[78] ProWriters, "The History," Cyber Insurance Blog.

continued to evolve with companies taking on new types of cyber risk and offering new products and services that are attached to the policy.[79]

The continuing evolution of cyber insurance could offer potential to better protect individuals. New products could be introduced for privacy claims by individual citizens. An example would be a policy to cover legal costs and damages that result from a privacy suit, like the ones previously explained about slanderous posts. The large data breaches of 2014 and 2015 also help identify the actual protection cyber insurance provides. The victims of these large data breaches were well known and popular retailers or health providers. There is a large amount of citizens who do business with these organizations and also share private information with them. As cyber insurance protects these organizations, the individual citizens are also indirectly being protected.

Carriers began using new technologies that allow for better evaluations of insured companies and developed new risk appetites based on previous claims. The larger insurance companies were in a better position now to take on risk based on experience, as well as the size of their books. Pricing for cyber insurance policies, at this point, is all over the place within the industry. One carrier may provide a broad quote for the same risk that another company provides a very detailed and limited policy. The premiums between carriers also fluctuate, one insurer could ask for double or triple what another is asking for basically the same coverage. Additionally, carriers go back and forth with their risk appetite. There may have been a risk they were all over in a previous year, and now they don't want it. Each company is trying to find the best market for their products, in order to find a balance between the risk they take on and the revenue they are making. One carrier could be pursuing large retailers and another could be

[79] ProWriters, "The History," Cyber Insurance Blog.

pursuing small firms, and then by the next year they are going after a completely different market. Getting a quote also depends and varies on the type of market and size of the risk. The application can be a few short questions, or many extensive questions. Carriers may also require a call or meeting with a third party risk assessment firm.[80]

Cyber insurance and its markets are constantly changing and volatile would be the best way to describe it. The volatility of cyber insurance can be expected for its future as well. We can expect to see a change in risk appetites, drastic differences in pricing, using new technology to assist underwriters, many different forms, and new risk management services being added to policies. Cyber risk is real and so are the threats, this is a risk that should not be ignored or taken lightly. Cyber insurance is a great coverage that is becoming much more important and helpful for mitigating risk. The fast growth and volatile market of cyber insurance are good indications that it is here to stay.[81]

All these factors added up point to the direction of even larger growth. Especially with rapid introduction of technological innovations, the room for the cyber insurance market to grow seems endless[82]. As of 2016, the annual gross written premiums for cyber insurance were estimated at $2.5 billion, according to PwC. They also estimate that by the end of the decade that number will grow to about $7.5 billion.[83] The potential for cyber insurance is huge. However, this is still a relatively untapped opportunity for insurers and reinsurers, the market is fairly new and many are unaware of the potential. Businesses across every sector are just now realizing the how important cyber insurance is, and how dangerous cyber risk can be due to the increasing

[80] ProWriters, "The History," Cyber Insurance Blog.
[81] ProWriters, "The History," Cyber Insurance Blog.
[82] ProWriters, "The History," Cyber Insurance Blog.
[83] "Insurance 2020," PwC.

complexity and riskiness of the digital landscape. Many are cautious of cyber risk and feel it can't be trusted. However, many insurers believe they can take advantage of this new opportunity and be in the right spot as this market matures and expands.[84]

Those involved in bringing in and writing cyber policies are helping take on as much risk as possible without creating too much exposure. Cyber insurance could soon become an expectation of clients and even part of the product line for insurers. The insurers that are not yet willing to embrace cyber risk are losing out on growth opportunities now, as well as other business if cyber products don't become part of the policies they offer. Cyber threat is is always out there and always changing. Criminals are constantly changing their tactics, probing for weakness, and looking for their next victim. The criminals themselves are changing as well they could anyone anywhere behind a computer, or even an employee. The targets of a cyber-crime are also changing, an example being a company being hacked for tracking data on cargo shipments. It is hard to tell who is going to be the next criminal, as well as who the next victim will be. A huge part of this is the introduction of new technologies and the vast capabilities of the internet. All these factors combined mean that cyber-crime is not only hard to detect and difficult to combat the threat, it is also costly. Cyber risk is truly a risk that is like no other.[85]

What makes cyber insurance so unique? The uniqueness of cyber insurance is based on a few different reasons that I would like to explore, all that can be described as an absence of the proper data and knowledge. This is due to the fact that cyber risk itself is such a fairly new risk, that the coverage, cyber insurance, is also very new. We are at a point in history where technology is continuing to advance at faster and faster rate, however this is also the case for

---

84 "Insurance 2020," PwC.

85 "Insurance 2020," PwC.

cyber risk. Innovative technology allows for the potential of new threats. The newness of cyber risk leaves the insurance companies and underwriters with shortages of data that could be very helpful with assessing the risk. As a result, Cyber insurance is not only hard to price but it is also difficult to understand how what the risks actually are.[86]

Cyber-attacks are seen as a huge threat to potential growth of business. According to PwC, "71% of insurance CEOs, 79% of banking CEOs and 61% of business leaders across all industries see cyber-attacks as a threat to growth, ranking it higher than shifts in consumer behavior, the speed of technological change and supply chain disruption."[87] Cyber risk is so volatile that it creates many vulnerabilities for both the policy owner and the insurer. The vulnerabilities associated with cyber risk is one example of how it is unlike any other. The world has become so highly interconnected as a result of the digital revolution, that there is basically no one place that contains endless amounts of data, most of which is sensitive. As a result, the sensitive data is susceptible to fraud, theft, and other compromises. Not to mention the added risks of malware, denial of service and other malicious attacks. Altogether cyber insurance is slowly become one of the biggest threats for our generation.

The first aspect of cyber risk that creates so much vulnerability is how severe and frequent the attacks are. Cyber-attacks are not only very costly, but the happen quite often as well. Claims associated with a cyber-attack can be huge losses and result in tremendous financial loss. PwC estimated that "Cyber-crime costs the global economy more than $400 billion a year[88]." It is also believe that this number will continue to grow. A single cyber-attack is very

---

86 "Insurance 2020," PwC.

87 "Insurance 2020," PwC.:1322 CEOs interviewed for PwC's 18th Annual Global CEO Survey (www.pwc.com/ceosurvey)

88 "Insurance 2020," PwC.: 'Net Losses: Estimating the Global Cost of Cybercrime', Centre for Strategic and International Studies, June 2014. The report estimates that the annual losses are between a "conservative estimate" of $375 billion and a "maximum" of $575 billion, giving a "likely" estimate of "more than $400 billion".

costly, one attack could easy cost a million dollars, and in some cases has exceeded tens of millions of dollars. This demonstrates just how severe cyber-crime can be. A more exact statistic from PwC, is that for companies with revenue greater than $1 billion the average financial loss due to security incidents in 2014 was $5.9 million[89]. Again, we can see just how great the potential consequences are from a security breach. The scale of potential losses for insurance companies on cyber risk are fairly close to the losses associated with natural catastrophes, which in most cases are very unlikely. If the severity wasn't enough, the frequency for cyber-crimes is also very high. The likelihood of a cyber-attack is tremendous, especially for the financial impact that could result from each attack. In 2014, the number of security incidents detected were nearly 43 million, equivalent to more than 100,000 attacks per day[90]. As you can see there are cyber-attacks happening every day, making it one of the most frequently occurring risks to be covered by insurance. The combination of both the severity and frequency of cyber-attacks lead to the potential for cyber insurance to be very dangerous for an insurance company. An insurance company that has a decent amount of cyber risk exposure, could be confronted with a series of severe losses. It would be very hard for the insurer to absorb the impact from those losses or be forced to rebuild their balance sheet, which is commonly done during a catastrophic event. The potential losses and regularity of cyber-crime are the first steps in understanding cyber vulnerabilities.[91]

The next cyber vulnerability that impacts cyber insurance is that loss contagion is hard to maintain. This is basically determining the impact of a cyber-attack. This is very difficult to do

---

89 "Insurance 2020," PwC.:Figure 2, PWC

90 "Insurance 2020," PwC.: 'Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015', PwC (http://www.pwc.com/gx/en/consulting-services/informationsecurity-survey)

91 "Insurance 2020," PwC.

because of the nature of breach. The tail of a cyber-breach is usually long and unpredictable. The tail refers to the damages that are a result of the claim that are noticed any time after the breach has been discovered, and in some cases can be far in the future. In the case of cyber-attacks, a long unpredictable tail means that impacts may not be show up at first but could come to light later in the future. The impact of a cyber-breach could not be felt or known until many months after the breach. This is especially dangerous because of how interconnected and interdependent so many businesses have become. All these businesses that are mutually dependent are in positions where it is not just their own systems and data that are vulnerable to attacks but those of their business partners, suppliers and customers. The interdependency between companies leads to increased exposure to security breaches, which can cause a breach to be very impactful. Adding to the fact that cyber-attacks have long tails, the full scope of the impact from the attack may take a while to be realized. A business may not realize they too could have been impacted by a cyber-attack on one of their partners. The more companies share information the more vulnerable they will become making it harder to control losses, because there is a greater chance for a large impact due to a breach. Realizing the impact of security breach is the second step in understanding the vulnerabilities of cyber risk. A cyber breach may not just impact one organization rather anyone who shares information or does business with the victim may also fall victim to the attack, and it may not be noticed when the breach occurs.

The last cyber vulnerability is that the risks are hard to detect, evaluate and price. As a result of cyber risk being fairly new, there is limited actuarial data on the financial impact of cyber-attacks. It is considerably difficult to evaluate or price this risk with precision because of the lack of data. An underwriter may be able to easily estimate the cost of getting systems back up and running after a breach, in a similar way as if the systems were shut down by a flood or

fire. However, there is not enough data to estimate any further losses as the result of brand impairment or compensation payments to customers, suppliers, etc. This uncertainty around risk assessment and pricing is also added to the fact that security breaches are very hard to detect. It is possible for a cyber-breach to undetected for several months, and could possibly go years without being noticed. These two ideas combined make it possible to have unexpected accumulated and compound losses in the future. The lack of data surrounding cyber-attacks and the difficulty detecting a breach is the last cyber vulnerability. It makes it very difficult for underwriters to understand and estimate the risk they are willing to take on, but to also reasonable price any coverage they may offer.[92]

Cyber risk is definitely a real problem that many people are beginning to realize, including the need for safeguards against large scale and damaging cyber-attacks. Cyber insurance is one option that can be used for risk transfer. Many insurers have eagerly embraced this new market that presents revenue growth opportunities through cyber insurance products. On the other hand, there are many who believe that the risk is too great for them to take on. They think the risk outweighs the reward, and that writing a cyber-policy will only lead to a loss. Fortunately, there are many people, including many well-known insurance companies that believe they can profit in such an unpredictable market.[93]

Cyber insurance offers a considerable opportunities for revenue growth among insurance companies, which are always looking to bring in new business and tap into new markets. Although there are great risks that might not full be understood, insurance companies that do write cyber policies believe they have the resources and the proper formula to take on the risks.

---

92 "Insurance 2020," PwC.

93 "Insurance 2020," PwC.

In order to limit their cyber risk exposure, insurers rely on conservative pricing strategies and tight policy terms and conditions. The tight policy terms and conditions are put into place in order to mitigate loss. The insurer will only cover losses associated with cyber breaches that are specifically stated and agreed upon in the policy. This allows insurance companies to know the exact situations that they would be liable to provide coverage. Conservative pricing techniques allow for insurers to make they are bringing in proper revenue depending on the exposure of the risk. The premiums for a policy with more coverage, or for riskier coverage will be more expensive compared to a policy with less coverage or a less risky coverage.[94]

Insurance companies desire to bring in new business for revenue growth would beg the assumption that pricing for cyber policies would be pretty favorable. Cyber insurance being such a new market, many would think insurers would want to write a ton of new business, basically as much as they can, at low prices to be more appealing to those looking. However, this is not the case. The pricing on cyber policies is very high. Especially if you take into consideration the limit of what the insurer is willing to pay out, which are usually low. In fact, the pricing relative to limits for cyber policies is three or four times that of policies of more established general liability risk[95]. On reason for such high pricing is due to the limited number of insurers offering cyber policies. This is the more obvious reason because there are less insurers then those who need insurance, allowing for insurers to set the prices. The other, much bigger reason is the uncertainty around how much money to allocate for a potential loss. At the time a claim is filed, insurance companies put aside an estimated amount that they believe will cover the potential loss. The magnitude of a cyber-related loss is so hard to predict that insurers are forced to charge

---

94 "Insurance 2020," PwC.

95 "Insurance 2020," PwC.:'UK Cybersecurity: The role of insurance in managing and mitigating the risk', UK Government, March 2015

so much for cyber policies in order to make sure they can allocate the proper funds in the event of a loss.[96]

The other way that insurance companies are reducing their risk exposure in the cyber market is specifically in the writing and language of the policy. The first way policy writing allows insurers to mitigate the high risk of cyber insurance is by setting low limits. In the case of a loss, insurers will only have to pay out up to the limit agreed upon in the policy. This helps reduce their risk exposure because now the insurer is only responsible for the loss up to the limit. Many insurers are setting limits below what most customers are looking to get. Again, this is possible because of the limited number of insurers in the market, the lack of competition creates low supply and the need for coverage creates a large demand. The next way that policy writing can provide an opportunities for insurance companies to mitigate cyber risk is through imposing restrictive exclusions and conditions. Including restrictive exclusions and conditions allows for the insurer to only pay out losses that specific to the policy. The policy may only cover specific breaches or may not pay out losses if specific guidelines are not followed. Specific examples are state-of-the-art data encryption or 100% updated security patch clauses, both provide difficulties for businesses to maintain. The high prices, low limits, and terms and conditions that are written into the policy have many policyholders asking whether or not their cyber insurance policies are delivering real value.[97]

There are still concerns around the magnitude of losses associated with cyber, despite insurance companies' tactics to mitigate their risk exposure. Even with the restrictive term and conditions and limits placed on policies in order to reduce the potential losses, there are concerns

---

[96] "Insurance 2020," PwC.

[97] "Insurance 2020," PwC.

about the accumulation and concentration of cyber exposure. The belief is that the full potential of cyber risk is still unknown, and that accumulating too much can be devastating in the event that there is an unforeseen data breach with potentially huge losses. An even bigger concern, is for companies that are writing cyber policies that do not completely understand or could struggle to withstand the potential losses. It is believed that there may be regulations put into place to reduce or even stop these companies that do not sufficiently understand cyber risk.[98]

The capacity for cyber insurance will continue to grow over the next few years which could lead to a more competitive market. As the market becomes more competitive there will be more pressure to lower premium rates, raise limits and have more relaxed terms and conditions. As the market continues to mature, there will be more data available to help understand the risks better and more actually price the policies, which will also help lower premiums. The cyber risk market is still speculative, but there are a few steps that can be taken to help cyber insurance become more sustainable, and allow insurers to take advantage of the profitable growth.[99]

Pricing will continue to play a major role in sustainability of cyber insurance. Insurers, as the always do, will need to be able to judge what they could lose and how much they can afford to lose. An absence of actuarial data for cyber insurance, pricing will not just be based purely on science and math but will need just as much judgment and reasoning. It may become possible for insurers to develop a clear understanding of their total maximum losses allowing them to have a clearer idea of the risks they want to take on the risks they can take on. This would help insurance companies judge the best industries to concentrate their focus, allowing for further coverage in some places and less in others. The more knowledge an insurance company receive

---

98 "Insurance 2020," PwC.

99 "Insurance 2020," PwC.

will also play a major role the sustainability of cyber insurance. One way an insurer could go about this would be bringing in help from outside the industry. This would be in the forms of technology companies or intelligence agencies. The more that is known about potential risk the easier it will become to assess them. Enlisting the help of others from different fields can help develop a more effective threat and client vulnerability assessment. In this case, the risk assessment and pricing would not only include the work of underwriters and actuaries but also technology experts that could provide insight on the data and systems aspects. The final way that cyber insurance can become more sustainable would be through sharing of more data. An increased in the amount, as well as the effectiveness of data sharing is need for a better pricing accuracy. As discussed before, more data can only help where to price certain cyber risks, but also lead to a better understanding of the risks and what they are. A problem that has become more evident is that companies have been concerned about admitting to breaches for reputational purposes. On the other side, there are insurance companies withholding data because of the concerns for loss of competitive advantage. The legislation put into place requiring notification upon a breach by the U.S. government helps increase the volume of available data. Other countries are beginning to adopt similar laws that will only added to the data volume as well. These are only a few suggestions on how cyber insurance can become more sustainable. Only time can tell how the cyber market will change and develop.[100]

The cyber insurance market is a new, fast growing market that provides the potential for tremendous revenue growth. As of now there are a limited number of providers, with tons of risks to be transferred. This allows for insurance companies to be very precise in their policies on what is actually covered and to charge high premiums. The fact that, this type of risk is so new

[100] "Insurance 2020," PwC.

provides little data on what the risks are and what the potential loss might be. The lack of data is also a factor in the high premiums being charged by insurers and the low limits associated with coverage. Underwriters are unaware of the full exposures from cyber risk and write policies based upon the information they do have. The uncertainty around the risks associated with cyber insurance make it a somewhat speculative market, which has many concerned of potentially huge losses. In many cases this concern is keeping others from joining the market that could provide new revenue opportunities.[101]

Cyber insurance is definitely a response to privacy concerns; nonetheless, it does not specifically a response of individuals. Individuals are concerned with who has access to their information and what the result of unwanted accesses may be. These concerns are being covered in cyber insurance. However, cyber insurance is covering organizations that already have individual's information. Cyber insurance is not a great solution for individual's privacy, but is for organizations that handle private information. A better solution is needed for individual privacy concerns.

---

[101] "Insurance 2020," PwC.

Conclusion

In this project I sought to explore American concerns and feelings about privacy, and if these concerns and feelings are correlated to the developing growth of cyber insurance. In trying to explore this topic, I first needed to know more about privacy as an American idea. In doing this, I found a significant amount of information about the history and traditions of privacy in America. I then looked at the privacy in the view of the American public today. I was able to see the connection to the traditional views of privacy, but also the changing views that are a result of the technological innovations. These innovations are allowing people to interact in ways that were once unimaginable. New forms of interaction also expose private information to new threats. I wanted to take this new knowledge, and see how it correlated to the growth of a new market, that is cyber insurance.

Unfortunately, it seems as if cyber insurance is more of a solution for organizations that collect information, rather than individuals who expose their own information. In my research I started off wanting to believe that cyber insurance growth was strongly fueled by American's strong concern for privacy and their infatuation with internet interaction that add new exposures to their privacy. In the end, I have figured out that cyber insurance is not exactly the response I was looking for. Cyber insurance is a solution that helps organizations who collect personal information. It is not directly a solution for individuals who share their personal information. It can still be said that cyber insurance is a result of a concern for privacy. American's concerns that their personal information may be used in malicious ways is still fueling the cyber insurance market. The concerns that personal information will be stolen is being dealt with through cyber insurance. However, it is indirectly protecting individuals. I thought that cyber insurance would

be more of a direct response to American concerns. It still is, but not in the way I thought it would be.

The one area of my project that could be explored further, especially in years to come is the American feelings toward privacy and social media. There is an apparent contradiction between Americans continuing concerns for privacy, on the one hand, and their continued use of social media networks and online retail. The areas where Americans' communicate between each other has moved into virtual settings that give the illusion of private spaces like a "living room" or "water cooler". These once private settings are no longer such. The ever increasing participation into these networks in cyber space creates this contradiction. Americans have such a strong connection to digital technologies, which have made it impossible to give up these new conceptions of private space even as they hold onto the traditional conceptions of privacy. I feel like I hear another story about Facebook in the news every day, however Americans continue their use and share all kinds of information with their "friends".

Although cyber insurance may not be a solution for individuals when it comes to privacy concerns on the internet, there may be some things to consider as solutions for these concerns. Self-monitoring/self-censoring is the best way to protect yourself. Being conscious of what you information you share, and who you share it with. Doing this will allow you to know exactly what personal information is on the internet and can be seen by others. Another solution would be to push for better legislation. It should be more written more clearly in laws what is protected and what isn't protected by the government. Laws should be updated to consider social media as a potential source for libel and slander. Better laws will also help people understand what they should and shouldn't do on the internet.

Personally, I find that privacy is one of my rights, and one that I would like to protect. I have noticed, even before writing this paper, that the internet is a scary place that can really infringe upon my privacy. I would say that, I try and self-monitor/self-censor what I do on the internet. When I am online, I do my best to share as little personal information as I can. In the case that I do have to give out personal information, I try my best to make sure the sites are legitimate and have privacy policies. My social media footprint is also relatively low, I really only use Facebook. On Facebook, I have very little personal information shared, and I also have the privacy settings changed so only my friends can view my whole profile.

Bibliography

Acquisti, Alessandro, and Ralph Gross. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." *Privacy Enhancing Technologies*, 2006, 36-58.

Adams, Glenn. "The Cultural Grounding of Personal Relationship: Enemyship in North American and West African Worlds." *Journal of Personality and Social Psychology*, July 2005, 333-47. DOI:10.1037/0022-3514.88.6.948.

Currier, Fredrick A. *Proceedings of the Fitchburg Historical Society and Papers Relating to the History of the Town*. Vol. 1. N.p.: The Historial Society, 1895.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences." *Computer-Mediated Communication* 15, no. 1 (October 1, 2009): 83-108.

The Editors of Encyclopedia Britannica, ed. "Quartering Act." Encyclopedia Britannica. Last modified July 12, 2016. Accessed April 2018. https://www.britannica.com/event/Quartering-Act.

"Electronic Privacy Information Center." EPIC - Public Opinion on Privacy. https://www.epic.org/privacy/survey/.

"Georgia Woman Badmouthed Her Sheriff's Deputy Ex-Husband in a Facebook Post, So He had Her Arrested: Lawsuit." KTLA. Last modified March 9, 2018. Accessed April 2018. http://ktla.com/2018/03/09/georgia-woman-sues-ex-husband-for-having-her-arrested-over-facebook-post/.

"Insurance 2020 & beyond: Reaping the dividends of cyber resilience." PwC. https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html.

Investopedia. "Errors And Omissions Insurance - E&O." Investopedia. Last modified March 10, 2018. Accessed March 2018. https://www.investopedia.com/terms/e/errors-omissions-insurance.asp.

Kasper, Debbie V.S. "The Evolution (Or Devolution) of Privacy." *Sociological Forum* 20, no. 1 (March 2005): 69-92. http://www.jstor.org/stable/4540882.

Lindros, Kim, and Ed Tittel. "What is cyber insurance and why you need it." CIO. Last modified May 4, 2016. Accessed January 2018. https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html.

Madden, Mary, and Lee Rainie. "American' Attitudes About Privacy, Security and Surveillance." Pew Research Center: Internet, Science & Tech. Last modified May 20, 2015. Accessed

January 2018. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Martonca, Emanuel. Quora update. July 22, 2014. https://www.quora.com/In-your-opinion-is-it-important-to-protect-online-privacy-when-using-social-networking-sites.

Montanye, James A. "Bowling Alone (Book Review)." *Independent Review* 5, no. 3 (Winter 2001). http://web.b.ebscohost.com/ehost/detail/detail?vid=3&sid=4210404c-1558-44b9-bb15-a21255be7619%40sessionmgr103&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=4097410&db=aph.

Murray, Lindsey. "Consider This Your Warning to Be Extra Careful About What You Post on Facebook." Good Housekeeping. Last modified April 17, 2017. Accessed January 2018. https://www.goodhousekeeping.com/life/news/a43755/facebook-defamation-lawsuit/.

Nadkarni, Ashwini, and Stefan G. Hofmann. "Why do People use Facebook?" *Personality and Individual Differences* 52, no. 3 (February 2012): 243-49. doi:10.1016/j.paid.2011.11.007.

Olynik, Alexandra. Quora update. February 16, 2014. https://www.quora.com/In-your-opinion-is-it-important-to-protect-online-privacy-when-using-social-networking-sites.

Post, Robert C. "The Social Foundations of Privacy: Community and Self in the Common Law Tort." *California Law Review* 77, no. 5 (October 1989). http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1210&context=fss_papers.

ProWriters. "The History of Cyber Insurance." *Cyber Insurance Blog*. Entry posted April 25, 2016. Accessed March 2018. http://prowritersins.com/the-history-of-cyber-insurance/.

Putnam, Robert D. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster, 2000.

Radcliffe, Brent. "Cyber And Privacy Insurance." Investopedia. Accessed April 20, 2018. https://www.investopedia.com/terms/c/cyber-and-privacy-insurance.asp.

Rainie, Lee. "The state of privacy in post-Snowden America." Pew Research Center. Last modified September 21, 2016. Accessed February 2018. http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

Rosen, Jeffrey. "The Silver Bullet: Protecting Privacy and Security through Law and Technology." *Proceedings of the American Philosophical Society* 151, no. 3 (September 2007): 291-99. http://www.jstor.org/stable/4599072.

Seipp, David J. *The Right to Privacy in American History*. Harvard University, 1981. Accessed February 2018. http://pirp.harvard.edu/pubs_pdf/seipp/seipp-p78-3.pdf.

Smith, Aaron, and Monica Anderson. "Social Media Use in 2018." Pew Research Center: Internet, Science & Tech. Last modified March 1, 2018. Accessed April 2018. http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/.

Solove, Daniel J. "A Brief History of Information Privacy Law." *Proskauer On Privacy*, 2006. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2076&context=faculty_publications.

"Summary of the HIPAA Privacy Rule." HHS.gov. Last modified July 26, 2018. Accessed February 2018. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

SUPREME COURT OF THE UNITED STATES. Report no. 13-132. October 2013. https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

Widmer, Ted. "How Privacy became an American Value." BostonGlobe.com. Last modified May 18, 2014. Accessed February 2018. https://www.bostonglobe.com/ideas/2014/05/17/how-privacy-became-american-value/fVrcUTX0h2M39HcjOtBbIN/story.html.