The Pennsylvania State University

The Graduate School

A PROPOSAL FOR A LAW TO PRESERVE AND PROTECT DIGITAL PRIVACY FOR AMERICAN CITIZENS

A Thesis in

Media Studies

by

Ahmed Alrawi

Submitted in Partial Fulfillment

of the Requirements

for the Degree of

Master of Arts

May 2021

The thesis of Ahmed Alrawi was reviewed and approved by the following:

Benjamin W.Cramer
Associate Teaching Professor
Thesis Advisor

Ford Risley
Professor of communications

Patrick Parsons
Professor of telecommunications

Anthony Olorunnisola
Professor, Associate Dean for Graduate Programs and Research

ABSTRACT

The problem of third parties, such as telecommunications and digital media companies, sharing people's private data with government agencies like the National Security Agency (NSA), has become more common in the Internet era. Private data like Internet search histories, contact lists, phone and video calls, pictures, health information, and so on are shared with the government by third parties. Such conduct leads to people's private data being unsecured and accessible to government security agencies. Thus, a real problem exists when third-party companies share people's private data. In addition, third parties are sharing people's private data with the government without asking for a warrant. Such conduct has resulted in a change in the application of the Fourth Amendment and the search and seizure process. Hence, lawmakers are not sure how to deal with third parties when applying the Fourth Amendment to solve privacy issues. Therefore, this thesis posits the problem of data privacy and the Third-Party Doctrine on the Fourth Amendment to the public, as well as encouraging the federal lawmakers to establish a law to stop the sharing of people's private data. Furthermore, this thesis proposes a new law called the U.S. Digital Privacy Protection Act that aims to solve the data privacy issue in the United States.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to express my gratitude to my advisor, Dr. Benjamin W. Cramer, for the support and guidance of my thesis research. Dr. Cramer's knowledge and expertise directed my thesis on the right path. I could not imagine my master's research without Dr. Cramer's assistance and supervision, and I feel I am lucky to have him as my advisor.

Additionally, I would like to thank Dr. Ford Risley for his assistance, patience, and motivation in my thesis research. Dr. Risley's efforts encouraged me to include essential material in my thesis research. I am lucky to have one of the experts and eminent professors in the field of mass communication history.

Further, I want to express my sincere thanks to Dr. Patrick Parsons for the direction and feedback, which led my thesis to a safe harbor. I am also lucky to have Dr. Parsons, who is one of the pillars of the telecommunications field in the U.S. and the world.

Lastly, I would like to thank my late father, my mother Nahidah, my sisters Deena and Dr. Zeena, my brother Dr. Zaid and his family, my lovely wife Cigdem, my son Alibartu, my mother-in-law Leyla, my father-in-law Kemal, and my brother-in-law Ozan.

Chapter 1

The Third-Party Doctrine

Most Americans live in a world surrounded by more electronics and sophisticated digital technologies. These sophisticated technologies are characterized by the fact that they store all types of data for users, including health data, social security numbers, and other types of data related to the citizenry. In the end, different types of data are brought together, thus providing a detailed picture of the lives of each and every individual. In looking closely at American law, we find that little protection is provided for the privacy of information for those electronic activities.[1] Furthermore, sharing people's private data with government security agencies may be a violation of the Fourth Amendment.[2] The repercussions, when the government has personal information, might be dangerous. This is because government employees, like security ones, might misuse people's private data when they obtain it. For example, government security employees might misuse the information obtained about specific people from a specific race or minority group against them, so people might be under extra scrutiny even though they are, in fact, innocent. The so-called Third-Party Doctrine badly distorted the Fourth Amendment and increased the rift in the relationship between the state and its citizens.[3] Companies such as Verizon, Facebook, and others collect large amounts of data from users and sell it to other advertisers.[4] According to Statista, telecommunication companies like Verizon and social media companies like Twitter and

[1] Orin S. Kerr, "The Case for the Third-Party Doctrine," *Michigan Law Review* 107, no. 4 (2009): 561-601.
[2] Patrick P. Garlinger, "Privacy, Free Speech, and the Patriot Act: First and Fourth Amendment Limits on National Security Letters," *New York University Law Review* 84, no. 4 (2009): 1105-1148.
[3] Sarah E. Pugh, "Cloudy with a Chance of Abused Privacy Rights: Modifying Third-Party Fourth Amendment Standing Doctrine Post-Spokeo," *American University Law Review* 66, no. 3 (2017): 971.
[4] Asuncion Esteve, "The Business of Personal Data: Google, Facebook, and Privacy Issues in the E.U. and the U.S.A," *International Data Privacy Law* 7, no. 1 (2017): 36-47.

Facebook shared private data of about 41% of US citizens aged eighteen to twenty-nine with government security agencies.[5] Nevertheless, this only marks the beginning of the problem because, beyond that, the major telecommunications and digital media companies give the data to the state on demand. In itself, this breaches the Fourth Amendment and search and seizure process.

The Fourth Amendment is not a complex and lengthy amendment,[6] simply stating "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 be issued, 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."[7] The Fourth Amendment consists of fifty-four words and five important terms: *persons*, *houses*, *papers*, *effects*, and *unreasonable*.[8] These five terms greatly impact the subject of privacy. In any case, the history of the Fourth Amendment has a strong relationship with the First Amendment,[9] especially in terms of freedom of speech, which connects the Fourth Amendment with the subject of privacy.[10]

The Third-Party Doctrine suggests that corporations such as telecommunications and digital media companies might be able to share peoples' private data when they give their private information to any of these business companies voluntarily and without any coercion or pressure to share this information.[11] For instance, when somebody subscribes to a telecommunication

---

[5] James Clement, "Online Privacy," *Statista,* Mar. 22, 2019, https://www.statista.com/topics/2476/online-privacy, accessed Jan 31, 2021.
[6] Susan McPherson, "Warrantless Arrest for Misdemeanor Traffic Violation Does Not Violate Fourth Amendment Protection Against Unreasonable Seizure," *Cumberland Law Review* 32, no. 1 (2001): 265.
[7] U.S. Const. amend. IV.
[8] Michael W. Price, "Rethinking Privacy: Fourth Amendment 'Papers' and the Third-Party Doctrine." *Journal of National Security Law & Policy* 8, no. 2 (2016): 247-286.
[9] Andrew E. Taslitz, *Reconstructing the Fourth Amendment: A History of Search and Seizure, 1789-1868* (New York: New York University Press, 2006)
[10] Jennifer L. McDonough, "Media Participation in the Execution of a Search Warrant Inside a Home Violates the Fourth Amendment to the United States Constitution," *Duquesne Law Review* 38, no. 4 (2000): 1119.
[11] Peter C. Ormerod and Lawrence J. Trautman, "Descriptive Analysis of the Fourth Amendment and the

company such as Verizon, the company will require the user to let Verizon use his private data such as texts messages, phone and video calls, and social security number; eventually, Verizon might share this private information with other parties like other businesses or even with the government, including government security agencies such as the National Security Agency.

The legal history of the Third-Party Doctrine goes back to the era of *Katz v. United States* (1967),[12] when the Supreme Court discussed a pivotal subject that related to the expectations of individual privacy.[13] The Supreme Court mentioned that there should be a clear definition of the places where people should expect to have privacy for their conversation and their private information.[14] After that decision, the debate among the legislators changed from the reasonable expectations of privacy to what if somebody gives his private information voluntarily to any business company, and whether business companies could use their users' private information and share it with other parties.[15] By the late 1970s, during *Smith v. Maryland* (1979), the Supreme Court came up with this conclusion suggesting that individuals should not expect any kind of protection for their private information if they decided to voluntarily give this information to any business or company.[16] At that time, the birth of the Third-Party Doctrine emerged, and the debate started regarding how people's private information might be secure if business corporations share individuals' private information with other parties.

Moreover, Congress has taken no steps to deter this rift. There are many examples of how the US has addressed privacy for particular topics but Congress has never passed any law about privacy in general. For instance, the Privacy Protection Act of 1980 protects journalists and their

---

Third-Party Doctrine in the Digital Age," *Albany Law Journal of Science & Technology* 28, no. 2 (2018): 73.
[12] 389 U.S. 347 (1967).
[13] Ormerod and Trautman, 73.
[14] Lucas Issacharoff and Kyle Wirsha, "Restoring Reason to the Third-Party Doctrine," *Minnesota Law Review* 100, no. 3 (2016): 985-1050.
[15] Ibid, 989.
[16] Michael Gentithes, "App Permissions and the Third-Party Doctrine," *Washburn Law Journal* 59, no. 1 (2020): 35-52.

works from government searches;[17] the Family Educational Rights and Privacy Act (FERPA) protects college students' data,[18] and the Health Insurance Portability and Accountability Act (HIPAA)[19] protects health care data.[20] Yet, there is no obvious law of privacy in the US like the General Data Protection Regulation in Europe. These acts and many others focused on the protection of people's private data for a specific area, but there is a need for a general privacy protection act that could limit the sharing of people's private data.

Nowadays, technology has become more advanced and complicated, such as electronic devices that do more than one function at the same time—technological convergence.[21] The Federal Communication Commission divided telecommunication transmission methods into two: wired like telephones or television (cable) and wireless like satellite TV or radio.[22] With the development of technology, it is difficult to determine the service of devices—wired or wireless. For instance, Voice over Internet Protocol (VoIP) and the Internet itself can be hard to distinguish. Such services lie between both wired and wireless methods of transmission; hence, it is difficult to impose regulations.[23] Here, the task of the old law is difficult to determine. From another corner, the executive branch relies on privacy cases that went to the Supreme Court, most notably *Smith v. Maryland*.[24] This case happened in the 1970s when there were no cell phones,

[17] 42 U.S.C. § 2000aa (1980); see also Jose M. Sariego, "The Privacy Protection Act of 1980: Curbing Unrestricted Third-Party Searches in the Wake of Zurcher v. Stanford Daily," *University of Michigan Journal of Law Reform* 14, no. 3 (1981): 519-562

[18] 20 U.S.C. § 1232g (1974).

[19] Pub. L. 104–191 (1996).

[20] Benjamin W. Cramer. "A Proposal to Adopt Data Discrimination rather than Privacy as the Justification for Rolling Back Data Surveillance." *Journal of Information Policy* 8 (2018): 5-33.

[21] Karam Castilhos and José Francisco. "Journalism in the Age of the Information Society, Technological Convergence, and Editorial Segmentation: Preliminary Observations, *Journalism* 10, no. 1 (2009): 109-125.

[22] Behrouz A. Forouzan, "Data Communications & Networking," *Microelectronics and Reliability* 45, no. 5-6 (2005): 1014-1016.

[23] Kewin O. Stoeckigt and Hai L. Vu, "VoIP Capacity-Analysis, Improvements, and Limits in IEEE 802.11 Wireless LA," *IEEE Transactions on Vehicular Technology* 59, no. 9 (2010): 4553-4563.

[24] 442 U.S. 735 (1979). See also Mark Rapisarda, "Privacy, Technology, and Surveillance: N.S.A. Bulk Collection and the End of the Smith v. Maryland Era," *Gonzaga Law Review* 51, no. 1 (2015): 121.

Internet, or convergent devices. In March 1979, a thief robbed Patricia McDonough in Baltimore, Maryland.[25] McDonough gave the police a description of the thief.[26] The police arrested the thief eventually through relying on phone records that showed that the calls McDonough received many times came from Lee Smith's phone. Regardless, the Executive Branch insists on using this case as precedent and clinging with national security.[27]

Katz v. United States is another renowned case decided by the Supreme Court that the U.S. judiciary and government agencies rely on, even though the case dates back to 1967. Katz, a resident of Los Angeles, California, was involved in sports wagering. In 1965, Katz used a public telephone booth to transmit betting information to bookmakers. The Federal Bureau of Investigation (FBI) started watching Katz closely, and decided to use a listening device known as a bug attached to the public phone booth that Katz used. After many days of eavesdropping on calls through the bugging device, the police arrested Katz on charges of illegally transmitting gambling information.[28] The devices used then, such as the phone booth, differ from what is currently used.[29]

On the other hand, third parties (telecommunication companies and digital media companies) have a different effect on the Fourth Amendment. For example, telecommunication companies like Verizon collect the people's metadata and store it as a record of each subscriber.[30] However, the new software technology that telecommunication companies have used is different than the technology that landline phone companies used in the 1960s and 1970s.[31] Today, the new

---

[25] John Applegate and Amy Grossman, "Pen Registers After Smith v. Maryland," *Harvard Civil Rights-Civil Liberties Law Review* 15, no. 3 (1980): 753.
[26] Ibid.
[27] Ibid.
[28] 389 U.S. 347 (1967).
[29] Orrin S. Shifrin, "Fourth Amendment: Protection Against Unreasonable Search and Seizure: The Inadequacies of using an Anonymous Tip to Provide Reasonable Suspicion for an Investigatory Stop," *The Journal of Criminal Law & Criminology* 81, no. 4 (1991): 760-778.
[30] Ibid.
[31] United States. Congress. House. Committee on the Judiciary. Subcommittee on Crime, Terrorism, and Homeland Security and United States. Congress. House. Committee on the Judiciary. Subcommittee on

technology that big telecommunication companies like Verizon use is enabling these companies to collect more information about the subscribers.[32] For instance, Verizon's software collects the time of the call, the call itself, the two callers, and the locations of both callers.[33] Furthermore, the applications that enable a video call in the new devices could be recorded by telecommunication companies like Verizon.[34] Also, the new technology helps telecommunication companies by recording metadata about subscribers and content.

Additionally, recording devices, such as Google Nest and Amazon's Alexa, are considered to be another tool used by third parties to collect citizens' private data and share it with the government.[35] The recording home devices connect to the internet to search for the requested information from users.[36] These recording devices store users' private data on Internet servers belonging to its companies.[37] These devices have caused a lot of debate concerning private data. The companies that own these devices are responsible for keeping private data away from the government. Unfortunately, instead of storing the data for company use only, these telecommunications and digital media companies are sharing subscribers' personal data with government agencies when requested.[38] At the same time, the Fourth Amendment stands paralyzed when it comes to sharing personal data with the government. The problem lies in the fact that the Fourth Amendment addresses the relationship between people and the government

---

Crime, Terrorism, and Homeland Security. Legislative Proposals to Update the Foreign Intelligence Surveillance Act (FISA): Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives, One Hundred Ninth Congress, Second Session, September 6, 2006. Washington: U.S. G.P.O., 2006.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Ramachandran G., R. Ramani, S. Selvaraju, B. Rajasekaran, P. M. Murali, and Department of Electronics and Communication Engineering, V.M.K.V. Engineering College, Salem, Tamandu, India. "Accident Finding and Location Identification System using Google Map," *i-Manager's Journal on Electronics Engineering* 3, no. 3 (2013): 32-37.

[36] Ibid.

[37] Ibid.

[38] Courtney Giles, "Balancing the Breach: Data Privacy Laws in the Wake of the N.S.A. Revelations," *Houston Journal of International Law* 37 (2015): 543.

only during the search and seizure process. The Fourth Amendment does not mention any other parties besides the government and the people; it applies only to searches of physical possessions and says nothing about electronic data. However, the debate focuses on whether or not the Fourth Amendment could be applied in our digital era when government agencies search private electronic data.

Lawmakers have established many acts regarding the collection of private data. The most debatable is the USA PATRIOT Act,[39] which partially expired and, in 2015, was revived again through establishing the USA Freedom Act.[40] The PATRIOT Act was established in 2001 after the 11th of September attacks, and under President George W. Bush's administration after lawmakers wanted to establish a quick new law that could help government security agencies do security investigations easily and without many legal restrictions. After that, government security agencies like the NSA started to search people's private data, and any other private information related to the citizen, with fewer restrictions.[41] The USA Freedom Act is considered a new version of the PATRIOT Act with some limitations on the collecting of people's private data by the security agencies.[42] These acts distort the search and seizure process and raise many questions about the role of lawmakers in protecting people's private data versus giving the government more power to collect people's private data for investigation purposes. Furthermore, the Third-Party Doctrine took up a lot of the debate regarding data privacy issues. Third parties, especially telecommunication and digital media companies, are justifying their sharing of people's private data with the government by asserting that people provide their private data to third parties

[39] Pub. L. 107-56 (2001)
[40] Pub. L. 114-23 (2015). Library of Congress. Congressional Research Service. USA Freedom Act Reinstates Expired USA PATRIOT Act Provisions but Limits Bulk Collection. *Congressional Research Service*, 2015.
[41] A Report to Congress in Accordance with [Section] 326(b) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), (Dept. of the Treasury, 2002).
[42] Library of Congress, USA Freedom Act Reinstates Expired USA PATRIOT Act Provisions but Limits Bulk Collection, (Congressional Research Service, 2015).

voluntarily, not under coercion.[43] Third parties state that people provide personal data in return for using their services. Third parties also claim that people's private data is important for the companies because it is needed for items like bills, payment records, and other requirements.[44]

The government alleged that security agencies such as the National Security Agency and the Federal Bureau of Investigation need to collect people's private data in order to protect America from possible terrorist threats that might happen and harm people.[45] Since September 11, the U.S. government gives more power to security agencies to collect and record people's private data in order to monitor possible suspects that security agencies think might pose a threat.[46] Some might argue that the government is doing the right action in order to protect our nation, and people should not mind letting government security agencies collect our private data in order to protect us. Yet, this argument might appear false and unconvincing, especially when government security agencies collect thousands of innocent people's private data when they do not want to share their private information with anybody else. For instance, what if government security agencies collect private information about somebody who has a secret illness and does not want to reveal it to other people? Such people might not want to let government security agencies obtain this private information. In this situation, the private information of such innocent people might not be protected. Such innocent people need to keep their information regarding social and personal aspects private.

There two main methods that government security agencies use to collect people's private data: First, directly using their own technological devices such as software and digital surveillance devices; and second, by asking businesses to allow them access to Internet servers

[43] Mary-Kathryn Takeuchi, "A New Third-Party Doctrine: The Telephone Metadata Program and Carpenter v. United States." *Notre Dame Law Review* 94 (2018): 2243.
[44] Ibid., 2019.
[45] Beth Elise Whitaker, "Exporting the USA PATRIOT Act? Democracy and the 'War on Terror' in the Third World," *Third World Quarterly 28* no. 5 (2007): 1017-1032.
[46] Steven A. Meyerowitz, "The PATRIOT Act," *Banking Law Journal* 122, no. 2 (2005): 97.

that store private user data of these companies.[47] For the direct collection of private data, government security agencies such as the National Security Agency use the old method of tapping into the main infrastructure of the network cables of telecommunication companies to intercept phone calls, text messages, and other information of subscribers.[48] The rest of the job is completed secretly by experts working with government security agencies using advanced software that filters the information before providing it to the agents in the security agencies. Based on a *TechCrunch* report, about 434.2 million phone calls were recorded during 2019 using wiretapping of the main network of telecommunication companies by the National Security Agency.[49] For the second part—collecting people's private data—the government security agencies ask the telecommunications and digital media companies to give them a specific code related to the Internet servers of some of the subscribers of these telecommunication and digital media companies in order to do comprehensive searches of the private data of the individuals.[50] In some other cases, telecommunications and digital media companies give the data directly to the government security agencies through secret private data electronic files.[51]

All of the examples mentioned above are clear evidence of the effects of third parties on the Fourth Amendment. Also, the examples illustrate that there is a need for a privacy law to deter the sharing of private data by third parties. Third parties stand between citizens and the government when it comes to the application of the Fourth Amendment. Hence, it is obvious that US law should be updated to take into account the new technology being used by third parties.

The pivotal question lies in how we should persuade lawmakers that the United States must establish new and separate law regarding the privacy issue. Lawmakers should be convinced

[47] Zack Whittaker, "NSA Says Warrantless Searches of Americans' Data Rose in 2018," *TechCrunch*, Apr. 30, 2019, https://techcrunch.com/2019/04/30/nsa-surveillance-spike/, accessed Feb. 26, 2021.
[48] Ibid.
[49] Ibid.
[50] Ibid.
[51] Giles, 543.

that the Fourth Amendment no longer works in our digital era, which becomes more complicated with every new technological invention. The data privacy of people is certainly the tradeoff for using these technologies; in it lies the responsibility of lawmakers in the United States to protect people's private data.

There are many solutions provided to lawmakers to solve the problem of data privacy, many of which are represented by focusing on amended acts relevant to the privacy issue such as the PATRIOT Act, which ended by partially repealing the act and establishing the USA Freedom Act. The USA Freedom Act does not change many of the provisions that already existed in the PATRIOT Act; instead, the USA Freedom Act limited some of the power that has been given to the government agencies in searching the private electronic data of people.[52] Through looking closely at the period from during the PATRIOT Act to the period of the USA Freedom Act, and until this moment, it appears that the problem of sharing private data through third parties with government agencies still exists. This means that the heart of the problem does not lie in both acts, and essentially, the problem depends on the third parties and what could stop their sharing of private data with the government. However, many other solutions are provided by looking into the third parties and their violation of the privacy of people's data as well as their violation of the Fourth Amendment. Furthermore, other solutions are provided by looking at the digital technology itself and how it should be governed legally. Therefore, this thesis explores the problem of data privacy in the United States, as well as encouraging the federal lawmakers to establish a law to stop the sharing of people's private data. Furthermore, this thesis suggests a possible act aims to provide protection to people's private data in the United States.

The overarching purpose of this thesis is to draw legislators' attention to the sharing of personal data by third parties in cooperation with government security agencies. This thesis

[52] USA Freedom Act Summary: Amendments to U.S. Government Surveillance Authorities. Vol. 94 Congressional Digest Corporation, 2015.

describes the problems of private data sharing by exploring three important areas:

1. The application of the Fourth Amendment in history (search and seizure process).
2. The history and development of the phone and landline phone services (landline phone, cell phones, and the Internet), and
3. Analysis of old and new court cases related to privacy issues.

The next chapter will be a literature review that will explore the scholarly work about approaching the problem of sharing people's private data with the government. Also, the next chapter will explore how scholars analyze the problem of private data as well as the findings, suggestions, and achievements regarding solving the issue.

Chapter 2

Literature Review

General Review of Scholars' Work Regarding the Data Privacy Issue

People's private data have become progressively less secure in the digital technology era. Third parties (telecommunication and digital media companies) share people's data with government agencies, such as the National Security Agency (NSA), upon request. The discussion regarding how to solve the issue of people's privacy being breached is heated among scholars. In general, scholars ask lawmakers to be stricter with privacy laws and policies regarding telecommunication and digital media companies to further tighten sharing regarding people's private data.

Some scholars have looked at how old and new laws have helped telecommunication companies share people's private data with government agencies like the NSA, without any privacy laws to deter the breaching of people's private data. For instance, the USA PATRIOT Act and the USA Freedom Act have been widely used among scholars to analyze the impact of telecommunication companies on the search and seizure process. Furthermore, scholars have asked federal lawmakers to reexamine the PATRIOT Act and the USA Freedom Act to see whether government security agencies, such as the NSA, should obtain warrants before asking telecommunication companies for people's private data. The consensus among scholars regarding the PATRIOT Act and the USA Freedom Act is that both acts are enabling government agencies to obtain people's private data without obtaining warrants.[53]

[53] Reauthorization of the PATRIOT Act: Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives, One Hundred Twelfth Congress, First Session, March 9, 2011 (U.S. G.P.O., 2011).

Other scholars have looked at the Third-Party Doctrine to understand what the doctrine implies and whether the doctrine might affect the search and seizure process and the Fourth Amendment. In addition, scholars explore the application of the Third-Party Doctrine to people's private data and how telecommunication and digital media companies could share people's data with government security agencies without requesting warrants. Lastly, scholars examine the history of the Third-Party Doctrine with privacy issue cases in the United States courts.

Another group of scholars looked at the effects of telecommunication and digital media companies on the search and seizure process. Scholars mentioned that telecommunication and digital media companies stand between the government and the people in the search and seizure process. Moreover, scholars mentioned that government security agencies like the NSA request people's private data from telecommunications companies without obtaining warrants.[54] In return, telecommunication companies, such as Verizon, hand out people's private data directly to government agencies.[55] At the same time, government security agencies justify requesting people's private data as a necessary step for the security process in order to defeat any terrorist threat that might face the nation.[56]

Lastly, some scholars have investigated the effects of digital technology devices on sharing people's private data. Scholars have examined how people's data is stored in virtual repositories and how digital media companies such as Facebook share their subscribers' data without privacy law existing to prevent it.[57] Also, scholars have looked at how new digital

[54] Federal IT Security: A Review of H.R. 4791: Joint Hearing before the Subcommittee on Information Policy, Census, and National Archives and the Subcommittee on Government Management, Organization, and Procurement of the Committee on Oversight and Government Reform, House of Representatives, One Hundred Tenth Congress, Second Session, on H.R. 4791 to Amend Title 44, United States Code, to Strengthen Requirements for Ensuring the Effectiveness of Information Security Controls Over Information Resources that Support Federal Operations and Assets, and for Other Purposes, February 14, 2008 (U.S. G.P.O., 2008).
[55] Ibid.
[56] Ibid.
[57] Victoria Kisekka, Sharmistha Bagchi-Sen, and H. Raghav Rao, "Extent of Private Information Disclosure on Online Social Networks: An Exploration of Facebook Mobile Phone Users," *Computers in*

technology worsens the issue of privacy and raises many questions regarding the use of new digital technologies by telecommunication and digital media companies.

Such scholarly work mentioned above will be explored in the following sections to see the significant points that scholars found regarding the privacy issue, as well as at what point the scholars' work stops. Furthermore, the mentioned scholars will be discussed in order to see what areas are not covered by the scholars and need to be further investigated.

Scholars' Work Regarding the USA PATRIOT Act

When the USA PATRIOT Act was enacted in 2001 under President George W. Bush's administration,[58] the United States was in chaos after the 9/11 terrorist attack, and lawmakers wanted to establish a quick new law that could help government security agencies do security investigations easily and without many legal restrictions.[59] Therefore, after 9/11, Congress decided to establish the PATRIOT Act on October 26, 2001.[60] Since then, government security agencies like the NSA have obtained the green light to search people's electronic data, and any other private information related to the citizen without many legal restrictions.[61] After the PATRIOT Act was enacted, a debate was created among scholars about its effect on people's private data.[62]In fact, the United States Congress and Senate stated that the PATRIOT Act was established as a necessary tool to help government security agencies defeat terrorism attacks that might face the United States and its citizens.[63] The United States Congress mentioned that the

human behavior 29, no. 6 (2013): 2722-2729.
[58] Electronic Privacy Information Center, The USA Patriot Act, www.epic.org/privacy/terrorism/usapatriot, retrieved Jan. 31, 2021.
[59] Ibid.
[60] Ibid.
[61] Ibid.
[62] Beth Elise Whitaker, 1017-1032.
[63] To Permanently Authorize Certain Provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT [ACT]) Act of 2001, to Reauthorize a Provision of the Intelligence Reform and Terrorism Prevention Act of 2004, to Clarify Certain Definitions in the Foreign Intelligence Surveillance Act of 1978, to Provide Additional

main goal of the PATRIOT Act is to give government security agencies all the possible power to take the necessary steps to keep the nation safe.[64] However, Section 101 of the PATRIOT Act captures the attention of many scholars due to the controversial content mentioned there. The section has raised many privacy issues regarding people's private data and has distorted the search and seizure process and, ultimately, the Fourth Amendment. Specifically, according to the United States Congress, "Section 101 permanently authorizes the following nine provisions: 203(b) (authority to share electronic, wire, and oral interception information); 203(d) (authority to share foreign intelligence information); 204 (clarification of intelligence exceptions to criminal wiretap authorities); 206 (FISA "roving" authority); 207 (duration of FISA surveillance of non-US persons who are agents of a foreign power)." [65] Therefore, many scholars have examined the privacy issue through the PATRIOT Act generally and through Section 101 specifically.

In an article, "Exporting the USA PATRIOT Act? Democracy and the War on Terror in the Third World," Meyerowitz (2005) investigates the confusion of the district courts' rulings in cases related to the breaching of people's data privacy and how some US district courts use the PATRIOT Act to justify collecting people's private data.[66] Meyerowitz mentions that many judges are confused by Section 101 of the PATRIOT Act.[67] Meyerowitz illustrates that government security agencies are using people's private data without asking for a warrant because the PATRIOT Act has given them the ability to do so.[68] Moreover, the author mentions that Section 101 contradicts the Fourth Amendment and the search and seizure process.[69] Meyerowitz asks lawmakers to establish new laws that discern when the government needs to

---

Investigative Tools Necessary to Protect the National Security: Report Together with Additional and Minority Views (to Accompany S. 1266), vol. 109-85 (U.S. G.P.O., 2005). 310.
[64] Ibid, 311
[65] Ibid, 312
[66] Meyerowitz, 97.
[67] Ibid, 165
[68] Ibid.
[69] Ibid.

collect people's private data, especially in cases of suspicion of a terrorist attack or any kind of threat that might harm people.[70] Furthermore, the author mentions that the PATRIOT Act distorts the search and seizure process and the Fourth Amendment, regardless of whether an imminent attack existed or not.[71] In addition, Meyerowitz suggests revising the PATRIOT Act so that confusion about privacy issue cases could be avoided.[72] Meyerowitz's paper follows other scholars' works by focusing on the PATRIOT Act itself and linking privacy problems to some parts of the PATRIOT Act, such as Section 101. In fact, part of people's data privacy problems lies in the PATRIOT Act, but breaches that are happening to people's private data are related to third parties. Therefore, the idea of repealing the PATRIOT Act might solve part of the privacy problem but not completely. Also, lawmakers should limit the excessive power the PATRIOT Act gives security agencies.

In an article, "A Congressional Perspective on the USA PATRIOT Act Extenders," Lungren (2012) explores how a specific type of people's private data is being gathered from telecommunication companies and shared with government agencies under the cover of the PATRIOT Act.[73] Lungren's paper centers the discussion on Section 215 of the PATRIOT Act and how the section resulted in the breaching of people's private data.[74] Lungren illustrates that people's private data is breached due to Section 215 of the PATRIOT Act specifically, which permits security agencies to collect people's private data inappropriately.[75] However, Lungren highly suggests amending Section 215 and Section 101 of the PATRIOT Act, so third parties can no longer gather people's private data without warrants.[76]

---

[70] Ibid, 166
[71] Ibid.
[72] Ibid, 167
[73] Daniel E. Lungren, "A Congressional Perspective on the USA PATRIOT Act Extenders," *Notre Dame Journal of Law, Ethics & Public Policy* 26, no. 2 (2012): 427-458
[74] Ibid, 428
[75] Ibid.
[76] Ibid, 429.

In an article, "The Relevance of Relevance: Section 215 of the USA PATRIOT Act and the NSA Metadata Collection Program," McGowan (2014) examines the impact of many sections of the PATRIOT Act, such as Section 101 and Section 215, and specifies a direct effect of Section 215 of the PATRIOT Act on the Fourth Amendment and people's data privacy.[77] McGowan takes a unique approach by mentioning that the PATRIOT Act gives power to government security agencies to collect private data related to citizens; at the same time, a small amount of the collected data could be important for the investigation processes of the security agencies.[78] McGowan blames lawmakers regarding privacy data breaches and recommends reexamining Section 215 of the PATRIOT Act, as well as the other acts, to see if these sections permit investigators to gather untrammeled data.[79] Moreover, the author challenges lawmakers by asking them to look at the work of government security agencies collecting private data from third parties without a warrant.[80] McGowan mentions that in case of an imminent threat to the nation, the government security agencies should bring evidence on the suspected people and then obtain a warrant to collect data.[81] Also, McGowan further explains that the PATRIOT Act gives government agencies unlimited power to fight against terrorist actions that might threaten the United States, but at the same time, no one explained when people's private data could be used by government security agencies.[82] However, third parties sit between the Fourth Amendment and the government. Third parties are passing people's private data to government security agencies, and such conduct increases the problem of data privacy. McGowan provides an excellent analysis of the PATRIOT Act's effect on the Fourth Amendment and people's private data.

[77] Casey J. McGowan, "The Relevance of Relevance: Section 215 of the USA PATRIOT Act and the NSA Metadata Collection Program," *Fordham Law Review* 82, no. 5 (April 2014): 2399-2442.
[78] Ibid, 2399.
[79] Ibid.
[80] Ibid, 2341.
[81] Ibid.
[82] Ibid.

In an article, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment," Herman (2006) centers her analysis of the privacy issue around the PATRIOT Act through examining how the act distorts the search and seizure process and the Fourth Amendment as well as how the PATRIOT Act repealed security agencies' need to obtain warrants.[83] Herman investigates how government security agencies, like the NSA, the Federal Bureau of Investigation (FBI), and many other security agencies, began using search and seizure processes on people without obtaining warrants from the court.[84] Moreover, Herman focuses on how Section 101 of the PATRIOT Act was used as a justification during the search process by government security agencies without obtaining a warrant before starting the search.[85] Herman mentions that the PATRIOT Act has enabled government security agencies to fight terrorists to protect people in the United States from harm.[86] At the same time, Herman mentions that the PATRIOT Act harms people's privacy, and she raises many concerns regarding the breach of the Fourth Amendment that resulted from Section 101. Consequently, Herman suggests lawmakers should reexamine the PATRIOT Act to tighten the extensive authority given to government agencies such as the FBI and the NSA in search and seizure.[87] Furthermore, Herman mentions that the issue of data privacy and Fourth Amendment violations could be solved by repealing the PATRIOT Act and establishing a new act that could help government security agencies prevent terrorist threats and secure people's private data.[88] However, the paper provides a partial solution to the privacy problem because the problem of sharing people's private data does not relate to the PATRIOT Act directly. Instead, the problem lies in the lack of privacy laws that could govern the use of people's private data.

---

[83] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment*," Harvard Civil Rights-Civil Liberties Law Review* 41, no. 1 (2006): 67-132.
[84] Ibid, 68.
[85] Ibid, 69.
[86] Ibid.
[87] Ibid, 70.
[88] Ibid, 70.

In an article, "The PATRIOT Act and Crisis Legislation: The Unintended Consequences of Disaster Lawmaking," Welch (2015) examines the effect of the PATRIOT Act on the Fourth Amendment and on the search and seizures process. Welch's paper investigates the effect of Section 101 of the PATRIOT Act on people's private data and further challenges the PATRIOT Act through analyzing how US lawmakers put controversial content in the PATRIOT Act in 2001 that aimed to solve security issues quickly.[89] Welch examines the legality of Section 101 and other sections in the PATRIOT Act, mentioning that the problem of sharing people's private data with government agencies is linked to Section 101 and how this section gave security agencies more power in the search and seizure process.[90] Welch states that lawmakers traded individual privacy for national security, but people need security, private data security, and security from a terrorist threat.[91] Along the same line, Welch indicates lawmakers are confused regarding how to apply the Fourth Amendment and search and seizure process properly regarding private electronic data.[92] However, Welch's paper does not suggest repealing the PATRIOT Act; instead, the author suggests revising some sections of the PATRIOT Act, especially Section 101.[93]

In an article, "Mending Walls: Information Sharing After the USA PATRIOT Act," Sales (2010) provides an outstanding analysis related to the breaching of people's private data by government security agencies like the NSA and linked the breaching of data to the PATRIOT Act due to the powers that had been given to security agencies through the PATRIOT Act.[94] Sales asks lawmakers to consider whether or not investigators can exchange people's private data among themselves during the search process.[95] Furthermore, Sales mentions that government

[89] Kyle Welch, "The PATRIOT ACT and Crisis Legislation: The Unintended Consequences of Disaster Lawmaking," *Capital University Law Review* 43, no. 3 (Summer 2015): 481-554.
[90] Ibid, 483.
[91] Ibid, 486.
[92] Ibid, 488.
[93] Ibid.
[94] Nathan Alexander Sales, "Mending Walls: Information Sharing After the USA PATRIOT Act," *Texas Law Review* 88, no. 7 (2010): 1795.
[95] Ibid.

agencies clearly violate the Fourth Amendment, especially when their investigators rely on the PATRIOT Act during the search process, which distorts the search and seizure process and violates people's private data.[96] In addition, the paper indicates that the only solution to people's data privacy problem will be through revising specific sections of the PATRIOT Act so that investigators will not be able to request people's private data without obtaining a warrant that enables them to collect people's private data legally.[97]

In fact, telecommunication companies play a crucial role in violating the Fourth Amendment and the search and seizure process. Telecommunication companies could be responsible for sharing people's private data, and lawmakers should find solutions regarding this breaching of private data. Telecommunication companies, or third parties, save subscribers' private data and share the data with government agencies when requested to do so. Therefore, the main problem mentioned by Sales's paper is not the PATRIOT Act. Instead, the main problem lies in the third parties and how they share people's private data without any law preventing the exchanging of private data with government security agencies. As a result, lawmakers should look at establishing new laws that would limit third parties' ability to use people's private data.

In an article, " Securing Liberty: A Response to Debates on Section 215 of the USA PATRIOT Act," Cooke (2014) explores PATRIOT Act issues related to data privacy and violating the search and seizure process under the Fourth Amendment.[98] Cooke aims to find a reasonable explanation regarding the privacy issue by looking at the metadata security agencies' requests from telecommunication companies.[99] Cooke mentions that the issue of data privacy is linked directly to the PATRIOT Act, which lawmakers justify by saying that the act was founded

[96] Ibid, 1798.
[97] Ibid.
[98] Christopher Cooke, "Securing Liberty: A Response to Debates on Section 215 of the USA PATRIOT Act," *Georgetown Journal of Law & Public Policy* 12, no. 2 (2014): 889-896.
[99] Ibid, 891.

to fight terrorist actions in the case of an imminent threat.[100] Furthermore, Cooke discusses that many sections in the PATRIOT Act need to be revised, especially Section 101.[101] What is different in Cooke's paper is that the author does not link the issue of data privacy to the PATRIOT Act only. Instead, Cooke mentions that the data privacy issue is related to the rapid speed in the development of technology that helps telecommunication companies gather people's private data and share it with government agencies.

Scholars' Work Regarding the USA Freedom Act

In 2015, scholars started examining the USA Freedom Act, which renewed some of the old requirements from the PATRIOT Act and added some new rules as well.[102] The USA Freedom Act opened a new debate among scholars to look at the consequences of the act on people's data privacy. In fact, the USA Freedom Act carries some of the revisions of the PATRIOT Act, such as electronic surveillance and the collecting of metadata about telecommunication services' subscribers. Furthermore, from the PATRIOT Act era to the USA Freedom Act, government security agencies' behaviors did not change. Security agencies like the NSA are still collecting people's private data, which makes the USA Freedom Act an important subject to be discussed among scholars. As a result, scholars have discussed the act and its sections and linked the issue of people's private data to the USA Freedom Act. In addition, scholars raise many questions regarding the USA Freedom Act and whether the act results in a violation of the Fourth Amendment and the search and seizure process.

In an article, "Foreign Intelligence, Criminal Prosecutions and Special Advocates," Walsh (2017) provides an in-depth discussion regarding the USA Freedom Act, the Fourth

[100] Ibid, 892.
[101] Ibid.
[102] Library of Congress, USA Freedom Act Reinstates Expired USA PATRIOT Act Provisions but Limits Bulk Collection (Congressional Research Service, 2015).

Amendment, the search and seizure process, and the data privacy issue.[103] Walsh illustrates that the problems in the USA Freedom Act are the same problems found in the PATRIOT Act and that lawmakers basically did not establish new sections in the USA Freedom Act but instead kept some sections of the PATRIOT Act in the USA Freedom Act.[104] Walsh's paper further analyzes some sections of the USA Freedom Act and mentions that USA Freedom sections were established to target terror threats and any kind of crime or suspicious act.[105] At the same time, Walsh explains that lawmakers added a few new provisions to the USA Freedom Act that restrict the collection of private data by government security agencies.[106] The author mentions that intelligence agencies are surveying people through new digital devices to gather people's private data, and lawmakers did nothing to stop the breach of people's data privacy.[107] Walsh indicates that the breaching of people's data privacy can be seen in the USA Freedom Act, and government security agencies still have the same power they obtained from the PATRIOT Act regarding the search and seizure process.[108] Therefore, the USA Freedom Act could solve part of the privacy problem, but in order to solve the whole problem, lawmakers should restrict the role of third parties in sharing subscribers' private data.

In an article, "Searching for Federal and Judicial Power: Article III and the Foreign Intelligence Surveillance Court," Margulies (2017) provides an insightful analysis regarding the controversial content of the USA Freedom Act.[109] Margulies' discussion explains that the USA Freedom Act does not add any protection to people's data privacy and that security investigators still take advantage of the old sections of the PATRIOT Act that lawmakers used in the USA

[103] Patrick Walsh, "Foreign Intelligence, Criminal Prosecutions and Special Advocates." *The University of Memphis Law Review* 47, no. 4 (2017): 1011-1046.
[104] Ibid, 1012.
[105] Ibid, 1013.
[106] Ibid, 1014.
[107] Ibid.
[108] Ibid.
[109] Peter Margulies, "Searching for Federal and Judicial Power: Article III and the Foreign Intelligence Surveillance Court." *George Washington Law Review* 85, no. 3 (2017): 800-822.

Freedom Act.[110] Furthermore, Margulies indicates that the bulk of data collections by government security agencies still exist and that telecommunication companies continue to help government agencies share subscribers' private data.[111] However, between the PATRIOT Act and the USA Freedom Act, the privacy issue still exists. In fact, the continued problems of data privacy with the USA Freedom Act are clear evidence that repealing or amending acts will not solve the problem completely. The problem is also linked to third parties since they share people's private data with government agencies.

Scholars' Work Regarding the Third-Party Doctrine

The Third-Party Doctrine is applied by scholars to private information voluntarily given by people to third parties such as chain stores, telecommunication companies, hospitals, and internet businesses.[112] Third parties are blaming people for agreeing to give them their information voluntarily and not coercively.[113] However, the well-known Supreme Court case *Katz v. United States* (1967) shaped the phrase "reasonable expectation of privacy" among scholars and led to a wide range of controversy regarding the use of the phrase by third parties to justify collecting people's private data.[114] Furthermore, the Supreme Court declared that when people give their private information voluntarily and not coercively, they should not expect any privacy regarding their information since they give their information to seek a benefit from using a service in return for giving that information.[115]

Lawmakers should realize that the Third-Party Doctrine increased the rift of the data privacy issue and led to a clear violation of the Fourth Amendment and the search and seizure

[110] Ibid, 802.
[111] Ibid, 803.
[112] Ormerod and Trautman, 73.
[113] Jed Rubenfeld, "The End of Privacy," *Stanford Law Review* 61, no. 1 (2008): 101-161.
[114] Ibid.
[115] Steven D. Zansberg and Janna K. Fischer, "Privacy Expectations in Online Social Media - An Emerging Generational Divide?" *Communications Lawyer* 28, no. 3 (2011): 1.

process. Ultimately, no one can guarantee that people's private data is kept secure under the Third-Party Doctrine.[116] The Third-Party Doctrine has been used for many years in US courts in cases that relate to the privacy issue.[117] However, many scholars have investigated the ramifications of the Third-Party Doctrine on people's data privacy.[118]

In an article, "The Third-Party Doctrine and the Third Person," Stern (2013) investigates the Third-Party Doctrine and analyzes how the doctrine affects people's private data, as well as how the Third-Party Doctrine impacts the search and seizure process and the Fourth Amendment.[119] Stern found that telecommunication companies have always collected private data for their own use.[120] They tend to mention the Third-Party Doctrine to protect themselves from any legal trouble when they hand the data to the government.[121] Furthermore, Stern mentions that the Third-Party Doctrine still has repercussions on data privacy and the search and seizure process.[122] However, the work of Stern illustrates that telecommunication and digital media companies still use the Third-Party Doctrine as a justification for collecting people's private data. Therefore, the Third-Party Doctrine still has some minor issues that affect people's private data.

In an article, "The Fourth Amendment Third-Party Doctrine," Thompson (2014)[123] follows the same line of analysis as Stern. Thompson explores the roots of the Third-Party

---

[116] Arianna Vedaschi, "Privacy and Data Protection Versus National Security in Transnational Flights: The EU–Canada PNR Agreement*," International Data Privacy Law* 8, no. 2 (2018): 124-139.
[117] Madison Homan, "Warrants for Data Stored Abroad do not Constitute Unlawful Extraterritorial Applications of the Stored Communications Act - in Re Search Warrant no. 16-960-M-L to Google; in Re Search Warrant no. 16-1061-M to Google," *Suffolk Transnational Law Review* 41, no. 2 (2018): 575.
[118] Ormerod and Trautman, 73.
[119] Simon Stern, "The Third-Party Doctrine and the Third Person," *New Criminal Law Review* 16, no. 3 (Summer 2013): 364-412.
[120] Ibid, 371.
[121] Ibid.
[122] Ibid, 372.
[123] Richard M. Thompson, "The Fourth Amendment Third-Party Doctrine," Congressional Research Service, https://fas.org/sgp/crs/misc/R43586.pdf, retrieved Jan. 31, 2021.

Doctrine and how the doctrine affects the search and seizure process.[124] Thompson provides a thorough explanation of the establishment of the Third-Party Doctrine and mentions that *Smith v. Maryland* and *United States v. Miller* are two important cases that shaped it.[125] The author raises important questions regarding whether or not the Third-Party Doctrine is still applicable in the digital era.[126] Thompson's paper suggests future legal remedies to the privacy issue based on an analysis of some Supreme Court cases that used the Third-Party Doctrine in the ruling decisions of the cases.[127]

In an article, "Restoring Reason to the Third-Party Doctrine," Issacharoff and Wirsha (2016) analyzed the term "reasonable expectation of privacy" under the Third-Party Doctrine by tracing the Supreme Court definition of privacy to 1976.[128] Issacharoff and Wirsha mention that as life changed and the rate of technological development increased, the Third-Party Doctrine work expanded and has affected stored private data in the new digital devices. Eventually, it gave a reason for the new digital media companies to save and share people's private data.[129] Issacharoff and Wirsha illustrate that many aspects of daily services have changed over time, such as business and education services, and that the Third-Party Doctrine has left an enormous amount of private information unsecure.[130] Furthermore, Issacharoff and Wirsha indicate that people's private data continues to be shared because of the Third-Party Doctrine.[131] However, the authors explain how people's private data should be protected and that lawmakers should pay attention to how some effect of the Third-Party Doctrine on sharing private data. Issacharoff and

[124] Ibid, 7.
[125] Ibid, 9-12.
[126] Ibid, 15-17.
[127] Ibid.
[128] Issacharoff and Wirsha, 985-1050.
[129] Ibid, 988.
[130] Ibid, 987.
[131] Ibid.

Wirsha's paper looks at telecommunication and digital media companies' effects on private data and mentions that the solution lies in the Fourth Amendment.

In an article, "App Permissions and the Third-Party Doctrine," Gentithes (2020) examines how courts are using the Third-Party Doctrine in cases related to digital devices that promise to provide reliable services like GPS services, sports activity, online news tracking, and many other activities.[132] Gentithes mentions that new digital applications send information to the application developers, such as the locations of users, health information, and online business activities, because the users agreed to install these applications.[133] Gentithes states that judges are relying on the fact that people are giving their information voluntarily when they install the applications.[134] However, the author focused on the analysis of the Third-Party Doctrine implications on people's private data and how the new digital devices increase the breach of data privacy.

Scholars' Works Regarding the New Digital Devices

The rapid spread of digital devices increases every day, and digital media companies race to provide an extensive number of services to users. In fact, many of the digital devices and technology services were created to help people by enabling users to perform multiple functions from the same device at the same time. Yet, the risk of storing people's private data in these digital devices is high. Telecommunication and digital media companies provide users with high-quality services; however, users care more about fun and convenience. Scholars argue that telecommunication and digital media companies are storing subscribers' private data through the help of new digital devices and technology. Furthermore, scholars argue that people's private data

[132] Gentithes, 35-52.
[133] Ibid, 39.
[134] Ibid.

that are stored by telecommunication and digital media companies could be shared with government security agencies upon demand. In addition, the scholars' main debate focuses on how telecommunication and digital media companies sit between the government and the stored data. Therefore, the lack of privacy laws in the US gives more freedom to telecommunication and digital media companies to play with people's private data as they want.

In an article, "Social Media Searches and the Reasonable Expectation of Privacy," Mund (2017) explores the problem of social media companies and the invasion of data privacy.[135] Mund mentions that the Fourth Amendment and the search and seizure process should be applied to digital media websites, and government security agencies should obtain warrants before requesting users' private data from digital media companies.[136] Mund explains how social media websites give people two choices before signing up.[137] The first choice implies that people can accept the terms and conditions of the site so people can use the service after accepting the terms and conditions.[138] The second choice is if people decide not to accept the terms and conditions, then they will be unable to use it.[139] Mund mentions that when people accept the terms and conditions, they can no longer expect privacy for their data.[140] However, the author blames lawmakers for lacking privacy laws that could control the sharing of people's private data.[141]

In an article, "Expectations of Privacy in Social Media," Henderson (2012) provides an excellent analysis of breaches of subscribers' private data on Facebook and Twitter. [142] Henderson's paper explores the role of government security agencies in collecting subscribers'

---

[135] Brian Mund, "Social Media Searches and the Reasonable Expectation of Privacy," *Yale Journal of Law and Technology* 19 (2017): 238-273
[136] Ibid, 244.
[137] Ibid, 245.
[138] Ibid.
[139] Ibid.
[140] Ibid, 246.
[141] Ibid.
[142] Stephen E. Henderson, "Expectations of Privacy in Social Media," *Mississippi College Law Review* 31, no. 2 (2012): 227-248.

private data from social media websites and how the electronically stored data makes the job of security investigators easier than ever.[143] The author mentions that lawmakers are still unaware of the rapid developments of digital technology and that they should take the necessary steps to stop the use of users' private data by digital media companies.[144] Furthermore, Henderson further argues that government security agencies should obtain warrants before collecting subscribers' private data from social media websites.[145] However, Henderson's paper provides a different method for evaluating the issue of sharing private data. Henderson provides an advanced solution that might lead lawmakers toward establishing new laws to control new digital devices.

On the other hand, home devices produced by big technology companies are a threat to people's data privacy. The new generations of home devices record and store people's information in cloud storage that is controlled by the digital device companies, such as Amazon and Google.[146] Many scholars argue that government security agencies are using new digital technology devices to obtain evidence against suspects. For instance, the drone is one of the most notable digital technologies used recently by the police to take pictures of suspects in order to condemn them in court.[147] However, such digital devices need to be controlled by imposing a law that restricts the companies that own these digital devices.

In an article, "Unmanned & Unregulated: Where are the Privacy Protections from Drones?" Burger and Schuderi (2018) investigated breaches of people's privacy through drones.[148] Burger and Schuderi challenge the role of lawmakers regarding the invasion of

---

[143] Ibid, 231.
[144] Ibid, 233.
[145] Ibid.
[146] Anne Pfeifle, "Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice Activated Devices," *Washington Law Review* 93, no. 1 (2018): 421-458.
[147] Matiteyahu, Taly. "Drone Regulations and Fourth Amendment Rights: The Interaction of State Drone Statutes and the Reasonable Expectation of Privacy." *Columbia Journal of Law and Social Problems* 48, no. 2 (2015): 265.
[148] Jodie Burger and Eddie Schuderi. "Unmanned & Unregulated: Where are the Privacy Protections from Drones?" *Law Society of NSW Journal* (2018): 46-88.

people's privacy and mention they did nothing to stop the breaching of people's private data by drones.[149] Furthermore, Burger and Schuderi illustrate that drones can take photographs from above someone's home, or watch people coming and going, which is more like an invasion of physical privacy.[150] The author mentioned that government agencies used to obtain warrants before searching people's private information, while digital devices now allow government security agencies to collect people's information directly and without asking for warrants.[151] However, Burger and Schuderi encourage lawmakers to look at the breaching of digital devices, asking them to establish new laws to stop government agencies from using digital devices for investigative purposes.[152]

In an article, "The Privacy of 'Things': How the Stored Communications Act has been Outsmarted by Smart Technology," Crowell (2018) explores the violation of the Fourth Amendment and the search and seizure process by sharing people's private data stored in Alexa devices.[153] Crowell mentions that many customers are not aware of the privacy implications when they use new digital devices such Alexa.[154] Crowell emphasizes that Amazon and other digital device companies must be regulated under a clear privacy law.[155]

The Fourth Amendment has become more tough to enforce due to new communications technologies. The pivotal question lies in how lawmakers should be persuaded that the United States needs to establish new and separate laws regarding the privacy issue. Lawmakers should be convinced that the Fourth Amendment is no longer working in the digital era, which becomes

[149] Ibid, 47
[150] Ibid.
[151] Ibid.
[152] Ibid.
[153] Donald L. Crowell, "The Privacy of 'Things': How the Stored Communications Act has been Outsmarted by Smart Technology." *Federal Communications Law Journal* 70, no. 2 (2018): 211-332.
[154] Ibid, 213.
[155] Ibid.

more complicated every minute with new technologies. People's data privacy is certainly the tradeoff for using these technologies.

Many scholars have examined the data privacy problem and have tried to provide lawmakers with solutions in order to prevent breaches of people's private data. Many of these scholars focus on amended acts that are relevant to the privacy issue, such as the USA PATRIOT Act, which was ended by partially repealing the act and establishing the USA Freedom Act. The USA Freedom Act basically does not change provisions that already existed in the PATRIOT Act. Instead, the USA Freedom Act limited some of the power that had been given to government agencies in searching people's private electronic data.[156] Looking closely at the period of the PATRIOT Act, the period of the USA Freedom Act, and today, it is evident that the problems posed by the sharing of private data by third parties with government agencies still exist. The heart of the problem does not lie in acts or laws related to people's privacy; instead, the problem essentially depends on third parties and stopping them from sharing private data with the government. However, many other scholars have looked at third parties and their violations of people's private data as well as the violation of the Fourth Amendment. Furthermore, other scholars looked at the digital technology itself and how it should be governed legally. Yet, fewer scholars explore the search and seizure process application over its history to see if lawmakers could solve people's private data issues solely by applying the Fourth Amendment. Therefore, the next chapter will dive deep into the historical factors that led to establishing the Fourth Amendment and the search and seizure process and explore its application by looking at historical events during the colonial era.

[156] Bart Forsyth, "Banning Bulk: Passage of the USA Freedom Act and Ending Bulk Collection." *Washington and Lee Law Review* 72, no. 3 (2015): 1307.

Chapter 3

Historical Analysis of Search and Seizure and Phone Service

The problem of third parties, such as telecommunications companies and digital media companies, sharing people's private data with government agencies like the National Security Agency (NSA) has increased. Private data like social security numbers, phone and video calls, pictures, health information, and other data are shared with the government by third parties because the government asks these companies to use this data to prevent any possible terrorist threat. Such conduct leads to people's private data being unsecured and accessible to government security agencies. As a result, a real problem exists when third-party companies share people's private data. In addition, third parties are sharing people's private data with the government without asking for a warrant. Such conduct has resulted in a change in the application of the Fourth Amendment and the search and seizure process. Hence, lawmakers are not sure how to deal with third parties when applying the Fourth Amendment to solve privacy issues.

This chapter explores the application of the search-and-seizure process by looking at historical events during the colonial era. Furthermore, this chapter dives into the historical factors that led to the establishment of the Fourth Amendment and the search and seizure process to see if lawmakers can solve the breaches of people's private data through applying the procedure of search and seizure from the Fourth Amendment. Lastly, this section will show the technological gap between old technology (landline phones) and new technology (cell phones and the internet) through tracing the development of the telephone during World War II, the 1960s, and the 1970s, until the development of the internet.

The English Experience of Search and Seizure

The story of John Wilkes, a writer and member of the British Parliament, is a good example to start with to refer to the application of search and seizure throughout history.[157] Wilkes wrote papers that criticized King George III by mentioning that people could not afford the heavy burden of the taxes that were enforced by King George III.[158] King George III ordered his employees to search Wilkes' house and seize all his papers.[159] In addition, King George III put John Wilkes in prison only for criticizing him.[160] Later on, Wilkes's case became noteworthy because it summarized the early method of search and seizure.[161] Furthermore, Wilkes' case explained how the king and his security should obtain a warrant before searching people's houses and seizing their private property, such as papers.[162] Therefore, diving into the history of the Fourth Amendment and search and seizure is important, especially when undertaking an investigation of the surveillance of people's private data.

The birth of the Fourth Amendment was the result of discontent on the part of the colonists with the so-called writs of assistance and general warrants used by English King George II.[163] Writs of assistance harmed the colonists by imposing taxes while general warrants were used to enforce defamation laws and to suppress opponents of King George II.[164] As a result, the colonists resisted the king and his actions.[165] This resistance was an essential factor in the establishment of the Fourth Amendment.[166]

---

[157] George F. Rudé, *Wilkes and Liberty: A Social Study of 1763 to 1774* (Oxford: Clarendon Press, 1962), 135-196.
[158] Ibid, 139.
[159] Ibid.
[160] Ibid.
[161] Ibid.
[162] Ibid.
[163] Price, 247-286.
[164] John C. Coates IV, "Corporate Speech & the First Amendment: History, Data, and Implications," *Constitutional Commentary* 30, no. 2 (2015): 223.
[165] Andrew E. Taslitz, *Reconstructing the Fourth Amendment: A History of Search and Seizure, 1789-1868* (New York: New York University Press, 2006), 1236-1237.
[166] Thomas Y. Davies, "Correcting Search-and-Seizure History: Now-Forgotten Common-Law Warrantless

Throughout English history, rulers often searched and seized private property, particularly writings that were against the English king.[167] In the city of Westminster, England in 1476, the king gave orders to establish a way to require a license and property rights for presses.[168] He issued the Licensing Law for Printing Presses.[169] Licenses were granted to printing presses that were in support of the king's policies and the government censored printing presses that published writings against the king or his policies.[170] The Copyright Act of 1710, or the Statute of Anne, was the first act in England to deal with copyright regulations.[171] The statute permitted the government and the courts to regulate copyright instead of private parties.[172] The Stationers' Company was one of the first companies to obtain a license from the government. They used their license to distribute papers in favor of the king and his policies.[173] The Stationers' Company, in collaboration with the government, held a monopoly in the press for many years.[174] The king supplied the company with agents who made sure to search for any unlicensed companies and seize any papers with writing that mocked the king.[175] Moreover, King Charles I, who ruled after these laws were established, punished all writers who slandered and ridiculed him and even made libel in writing a crime, which he considered "seditious libel."[176]

Arrest Standards and the Original Understanding of 'Due Process of Law'," *Mississippi Law Journal* 77, no. 1 (2007): 1.

[167] Margaret P. Hannay, "Censorship and Interpretation: The Conditions of Writing and Reading in Early Modern England," *Sidney Newsletter* 8, no. 1 (1987): 12.

[168] Robin Myers and Michael Harris, *Censorship & the Control of Print: In England and France 1600-1910* (Winchester: St Paul's Bibliographies, 1992): 234-285.

[169] Ibid, 247.

[170] Ibid.

[171] Lionel Bently, Uma Suthersanen, and Paul Torremans, *Global Copyright: Three Hundred Years since the Statute of Anne, from 1709 to Cyberspace* (Cheltenham, UK; Northampton, MA: Edward Elgar, 2010).

[172] Tyler Ochoa, "The Legacy of the Statute of Anne," *Copyright & New Media Law Newsletter* 14, no. 1 (2010): 5.

[173] Peter W.M. Blayney*, The Stationers' Company and the Printers of London, 1501-1557* (Cambridge, U.K: Cambridge University Press, 2013).

[174] Robin Myers, *The Stationers' Company Archive: An Account of the Records,* 1554-1984 (Winchester: St. Paul's Bibliographies, 1990).

[175] Price, 247-286.

[176] Charles II, King of England and England and Wales, Sovereign (1660-1685: Charles II), By the King, a Proclamation for the Better Discovery of Seditious Libelers, Vol. 1588:97.

For many years, the common law in England used the argument of "seditious libel" against the speech of writers who wrote against the king,[177] and it allowed for the issuing of "general warrants" to search and seize the papers of the dissident writers.[178] The unwarranted searching of houses was not the primary problem in England at that time. Instead, the seizing of papers and presses was the main issue. According to Price, "In 1763, Lord Halifax, the British Secretary of State, ordered the king's messengers to 'apprehend and seize the printers and publishers' of an anonymous satirical pamphlet,' but the place at that time did not define their terms, and the seizure applied to the papers."[179] In other words, searching and seizing people's private property, such as papers and presses, was the initial reason for the search-and-seizure process.

During the reign of George III, 49 people were arrested for seditious libel.[180] One of them was Wilkes, a writer and member of Parliament.[181] At that time, Wilkes objected to his detention because he was a member of Parliament. He claimed that he should be granted immunity.[182] Wilkes admitted that he was the author of a pamphlet that mocked the king, but he also argued that trespassing and seizing personal papers should be stopped since writing is a part of the individual's speech.[183]

In *Wilkes v. Wood* (1763), Wilkes sued Wood,[184] the agent who had searched through Wilkes's possessions.[185] Wilkes claimed government officials should have a reason to search

---

[177] Michelle Burnham, Folded Selves: Colonial New England Writing in the World System (Hanover, N.H: Dartmouth College Press, 2007).
[178] Myers and Harris.
[179] Price, 247-286.
[180] Fred S. Siebert, *The Rights and Privileges of the Press* (New York: D. Appleton-Century Company, Inc., 1934), 567-581.
[181] Rudé, 135-196.
[182] Ibid.
[183] Ibid.
[184] Michael Conforti, "John Wilkes, the Wilkite Movement and a Free Press in America*," Journalism History* 43, no. 1 (2017): 32-43.
[185] Laura K. Donohue, "The Original Fourth Amendment," *University of Chicago Law Review* 83, no. 6 (2012): 213-223.

personal property and the government should not give its agents the right to do so unless the government has evidence condemning the person.[186] In *Wilkes v. Wood,* Wilkes mentioned the words "private" and "concerns" for the first time in history: "Wilkes condemned the use of general warrants as enabling the 'promulgation of our most private concerns, affairs of the most secret personal nature, signifying 'an outrage to the constitution itself.' He identified the search and seizure of his private papers as the most grievous offense against him."[187] However, the issue of *Wilkes v. Wood* was whether the government could search and seize Wilkes's personal property without probable cause to condemn him. The court ruled in favor of Wilkes, which was the first-time search and seizure by the government was limited under a specific circumstance, namely that evidence must be present before a warrant can be granted to search and seize private properties.[188]

Wilkes's case became the backbone for establishing the Fourth Amendment. As Price mentions, "*Wilkes v. Wood* (1763) was known as 'the Case of General Warrants,' and it was one of the most influential cases in shaping the Fourth Amendment."[189] Also, James Otis, the eminent American legislator and activist, knew about Wilkes's case and was influenced by it.[190] Furthermore, Wilkes's case established a new era of freedom in the English courts at a time when people were suffering from the writs of assistance burdens. Price mentioned that "According to the Supreme Court, it was a 'monument of English freedom' 'undoubtedly familiar' to 'every American statesman' at the time the Constitution was adopted, and considered to be 'the true and

[186] Thomas Y. Davies, "Recovering the Original Fourth Amendment," *Michigan Law Review* 98 (1999): 119-137.
[187] Price, 247- 256.
[188] Vernon L. Porritt, *British Colonial Rule in Sarawak, 1946-1963* (New York; Oxford University Press, 1997): 412-465.
[189] Price, 247-256.
[190] William Tudor, *The Life of James Otis, of Massachusetts: Containing also Notices of Some Contemporary Characters and Events, from the Year 1760 to 1775* (Boston: Wells and Lilly, 1823): 454-498.

ultimate expression of constitutional law.'"[191] Therefore, Wilkes' case ended the period of writs of assistance and general warrants.

The American Experience of Search and Seizure

Early in the 1770s, American colonists were still facing the problem of the search and seizure of goods, which was imposed by George II. Soon after *Wilkes v. Woods*, the news of John Wilkes was spread through newspapers.[192] In the 1730s, "writs of assistance" were still used by British officials, and they continued to search American colonists' houses looking for "untaxed goods."[193] During this same period, American colonists wanted to apply the search-and-seizure experience of England in America.[194] As Tudor explains in *The Life of James Otis, of Massachusetts: Containing also Notices of Some Contemporary Characters and Events, from the Year 1760 to 1775,* the young Massachusetts lawyer James Otis was one of the opponents of writs of assistance. He attempted to imitate the English experience of search and seizure.[195] James Paxton, a Massachusetts customs employee, asked the court to grant him a writ of assistance,[196] but Otis filed a lawsuit against him in order to stop the writ of assistance, which was later referred to as "The Writs of Assistance Case" or "Paxton's Case." Otis challenged the legality of the writs of assistance, offering four arguments in court.[197] First, Otis said that the Massachusetts court could not pass the writ of assistance because it did not specify which court in America could issue said writ.[198] Second, Otis claimed that the court should not issue a writ of assistance directly to

[191] Ibid., 247-248.
[192] Samuel Dash, *The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft* (New Brunswick, N.J: Rutgers University Press, 2004): 765-789.
[193] Price, 247-256.
[194] Ibid.
[195] Tudor, 454-498.
[196] Helen Hill Miller, *The Case for Liberty* (Chapel Hill: University of North Carolina Press, 1965): 1121-1133.
[197] Ibid. 1122.
[198] Ibid.

the official employees, but rather the court should ask for clear evidence in order to issue the writ of assistance.[199] Third, Otis said that whenever asking for the writ of assistance, specification should be provided regarding the person's name, the place, and the property to be searched, and searches should not be arbitrary.[200] Fourth, Otis argued that the law of writs of assistance contradicts the principles of cause, search, and justice, and therefore the court should repeal the law.[201]

The government's lawyers responded to Otis' fourth claim by stating that the parliament delegated the Massachusetts Superior Court to grant the writ of assistance to the government's employees.[202] As a result, the Chief Justice of the court agreed with the government lawyers' argument and made the decision in favor of James Paxton.[203] However, Otis built a framework related to search and seizure, which later became the basis for the Fourth Amendment. According to Gawalt, Otis' framework was the "model for the Fourth Amendment,[204] asking to specify 'place,' 'persons,' and "things."[205] In addition, before John Adams became the second President of the Unites States, he was an attorney, a writer, and one of the famous leaders of the American Revolution.[206] Adams adopted specific words from Otis' framework and applied it to the Fourth Amendment. According to Price, "Adams, the future president, borrowed this principle from Otis nineteen years later when he drafted Article Fourteen of the Massachusetts Declaration of Rights, the model for the Fourth Amendment."[207]

---

[199] Ibid.
[200] Ibid.
[201] Price, 247- 256.
[202] Tudor.
[203] Joseph R. Frese, "James Otis and Writs of Assistance." *New England Quarterly* 30, no. 1 (1957): 496.
[204] John Phillip Reid, *The Writs of Assistance Case*. Vol. 84 (The American Historical Association, 1979): 243-288.
[205] Gerard W. Gawalt, *The Writs of Assistance Case*, Vol. 36 (The Institute of Early American History and Culture, 1979): 117-144.
[206] Ibid.
[207] Price, 247-256.

In summary, the essential aspects of the history both English and American search and seizure have two important characteristics that demand awareness. First, the Fourth Amendment specifies people, property, and things for search and seizure and states that clear evidence must be present before asking the court for a warrant. Patently, this is diametrically opposed to current issues regarding digital technology. Second, there is no doubt that the Fourth Amendment could solve the issue of search and seizure related to government employees and people. At the same time, the real problem at this point is that the government security agencies like the NSA usually claim that data surveillance is simply "collection" or "tracking", but not "search and seizure" as stated in the Fourth Amendment. Previously, the government security agencies used to search for tangible private property such as paper or books, but nowadays, the government security agencies are searching private data (intangible private property) such as the data that stores the internet in a virtual repository called the cloud. In addition, the government security agencies do not obtain private data by themselves; instead, third parties are sharing people's private data with government security agencies. As a result, the application of the Fourth Amendment might be difficult in cases related to searching for people's private data (intangible private property).

The Development of Telecommunications from Landline Phone Service to the Internet and the Legal Challenges that Resulted

This section will trace the history of the landline phone service starting from the early efforts of the famous inventors Alexander Graham Bell and Elisha Gray to modern cellular services, such as 4G and 5G. In addition, this section will explore how the invention of the internet affects data gathering and how it provides authorities the opportunity to collect more data about people more easily than before the invention of the internet.

In the Supreme court cases *Katz v. United States* (1967) and *Smith v. Maryland* (1979), the telephone and landline services played a pivotal role in the decisions of the cases as well as in

their court analyses. In two other court cases, *American Civil Liberties Union v. Clapper* (2013) and *Klayman v. Obama* (2013), the court relied on the two older cases, *Katz v. the United States* and *Smith v. Maryland*, to judge the cases. Therefore, in order to clarify the gap between old technology (telephone service) and new technology (cell phone service and technological convergence), the history of the old technology and the development of the phone and landline phone service will be traced in the following section.

Before Bell acquired the patent, Bell and his friend Thomas Watson had worked together to develop the harmonic telegraph.[208] Gardiner Greene Hubbard, the founder of Bell Telephone Company (which later on became AT&T),[209] observed the work of Bell and Watson and saw an opportunity to expand his company with them.[210] Mr. Hubbard gave financial support to Bell and Watson in order to help them develop the harmonic telegraph.[211] While working on developing the harmonic device, Bell and Watson thought about creating a device that could transmit human voice electronically.[212] In March of 1875, Bell and Watson met Joseph Henry,[213] an American scientist who worked for the Smithsonian Institution.[214] Bell, Watson, and Henry discussed the idea of creating an electrical device that could transfer voice over a long distance.[215] Henry encouraged Bell and Watson, and they continued their work with enthusiasm.[216] After investing

[208] Bernard S. Finn, "Bell and Gray: Just a Coincidence?" *Technology and Culture*. (Baltimore: Johns Hopkins University Press, 2009), 213-226.
[209] Paul Irvine, "Gardiner Greene Hubbard (1822-1897)." *Journal of Special Education* 19, no. 4 (1985): 378-379.
[210] *The Telephone Cases*, 126 U.S. 1 (1888).
[211] Charlotte Gray, *Reluctant Genius: Alexander Graham Bell and the Passion for Invention*. (1st U.S. ed. New York: Arcade Pub, 2006): 255-278.
[212] Ibid.
[213] Ibid.
[214] Kenneth B. Lifshitz, *Makers of the Telegraph: Samuel Morse, Ezra Cornell and Joseph Henry*. (Jefferson, North Carolina: McFarland & Company, Inc., Publishers, 2017): 361-376.
[215] Ibid.
[216] Leonard Everett Fisher, *Alexander Graham Bell*, 1st ed. (New York, N.Y: Atheneum Books for Young Readers, 1999): 142-196.

hard and careful work, in June of 1875, Bell was suddenly able to hear the sound of the clock in the lab next door, indicating the success of the electrical device.[217]

The nineteenth century witnessed the first simple phone after several attempts, the last of which was successful. During the 1870s, Alexander Graham Bell and Elisha Gray designed two separate electrical devices that used electrical cables to transmit human voices.[218] In 1876, lawyers took Bell and Gray's inventions to the patent office for registration.[219] Bell was able to register his patent a few hours earlier than Gray.[220] Gray later challenged Bell in court, claiming that the idea of using electrical cables to transmit voice was originally his idea and not Bell's.[221] However, the court eventually decided that Bell was the inventor of the telephone.[222]

In 1904, Bell Telephone Company developed the first phone able to transmit and receive voice, and it featured a handset.[223] In 1927, interest in phones increased, and phone services were utilized in World War II.[224] In the 1960s, the electronic switching system (ESS) was created, and the telephone service became even more widely used in the United States.[225] One of the most notable technical tools used with the landline phone service was the pen register, a device used to record the numbers that a phone called.[226] By the late 1970s, the function of the pen register became a controversial topic regarding privacy.[227] More specifically, the landline phone service

---

[217] Gray, 43-98.
[218] Ibid.
[219] Michael E. Gorman and Kirby Robinson, "Using History to Teach Invention and Design: The Case of the Telephone," *Science Education* 7, no. 2 (1998): 173-201.
[220] Christopher Beauchamp, "Who Invented the Telephone? Lawyers, Patents, and the Judgments of History," *Technology and Culture* 51, no. 4 (2010): 854-878.
[221] D.A. Hounsell, "Bell and Gray: Contrasts in Style, Politics, and Etiquette," *Proceedings of the IEEE* 64, no. 9 (1976): 1305-1314.
[222] Carolyn S. Brodie, "Always Inventing: A Photobiography of Alexander Graham Bell," *School Library Media Activities Monthly* 21, no. 4 (2004): 48.
[223] Harry M. Shoshana, *Disconnecting Bell: The Impact of the AT&T Divestiture* (New York: Pergamon Press, 1984).
[224] Andreas Markland, "Trawling the Wires: Mass Surveillance of Border-Crossing Communication in Denmark during World War II," *Technology and Culture* 60, no. 3 (2019): 770-794.
[225] Ibid.
[226] Stan Prentiss, *Introducing Cellular Communications: The New Mobile Telephone System*. (1st ed. Blue Ridge Summit, Pa: Tab Books, 1984) 65-178.
[227] P. J. Louis, *Telecommunications Internetworking* (New York: McGraw-Hill, 2000).

company kept the phone number that the subscriber's call (outgoing call) recorded in the pen register, and government agencies most likely obtained the records from pen registers from phone companies to use them in ongoing investigations.[228] *Smith v. Maryland* (1979) is the most notorious case that relied on the pen register record.[229] The telephone booth was another structure that came into existence alongside the landline phone service, which was a box furnished with lights and a door to provide privacy to its users.[230] Also, the term *metadata* was introduced in the late 1970s.[231] In the telecommunication field, it refers to a collection of information about the user's data, such as time of the call, location of the caller, name of the caller, etc.[232] In *Katz v. United States* (1967), the phone booth was used by a government agency to listen to the phone call of a suspect.[233] Later, the use of the phone booth became a controversial topic due to privacy issues.[234]

Early in the 1960s, both the United States and the Union of Soviet Socialist Republics (USSR) raced to develop a system that could send and receive wireless calls.[235] In the United States, engineers worked in the Bell laboratory to develop a mobile system.[236] During the 1960s, engineers were able to create devices that allowed one to transmit calls through analog signals,[237]

---

[228] Applegate and Grossman, 753.
[229] United States. Congress. House. Committee on the Judiciary. Subcommittee on Administrative Law and Governmental Relations and United States. Congress. House. Committee on the Judiciary. Subcommittee on Administrative Law and Governmental Relations. Civil Liberties Act of 1985 and the Aleutian and Pribilof Islands Restitution Act: Hearings before the Subcommittee on Administrative Law and Governmental Relations of the Committee on the Judiciary, House of Representatives, Ninety-Ninth Congress, Second Session, on H.R. 442 and H.R. 2415. April 28 and July 23, 1986. Washington: U.S. G.P.O, 1987
[230] Tamar R. Gibbins, "Warshak v. United States: The Katz for Electronic Communication," *Berkeley Technology Law Journal* 23, no. 1 (2008): 723-753.
[231] Maria Tzanou, "Is Data Protection the Same as Privacy? an Analysis of Telecommunications' Metadata Retention Measures." *Journal of Internet Law* 17, no. 3 (2013): 21.
[232] Ibid, 123
[233] Matthew B. Kugler and Lior Jacob Strahilevitz. "The Myth of Fourth Amendment Circularity," *The University of Chicago Law Review* 84, no. 4 (2017): 1747-1812.
[234] Ibid.
[235] M.D. Fagen, G. E. Schindler, Amos E. Joel, E. F. O'Neill, and Bell Telephone Laboratories, *A History of Engineering and Science in the Bell System* (New York: The Laboratories, 1975): 154-188.
[236] Ibid.
[237] Theodore S. Rappaport, Brian D. Woerner, and Jeffrey Hugh Reed*, Wireless Personal Communications:*

which was one of the most obvious drawbacks for these devices because it allowed anyone with radio equipment to easily eavesdrop on calls.[238] In 1965, AT&T introduced Improved Mobile Telephone Service (IMTS),[239] which used more than one radio channel in order to allow multiple calls in a limited geographical area.[240] In 1973, a Motorola researcher named Martin Cooper introduced a handheld mobile phone.[241] In 1983, the first generation network or 1G network phone was introduced in the United States by Ameritech, a telecommunication company and one of the seven Regional Bell Operating Companies.[242] In 1991, the 2G network was introduced in the United States and became popular.[243] In 2002, 3G was introduced in the United States, which had more advanced features than the first two generations.[244] In 2009, the 4G network was introduced, and in 2018, 5G was introduced in the U.S. market. [245]

With landline phone services, phone companies had limited access to subscribers' data due to the limitation of the landline phone service.[246] The invention of the internet provided the authorities more data about people.[247] Services such as voice over internet protocol (VoIP) allows telecommunication companies to record and obtain more metadata about users.[248] Therefore, the technology and the features of the landline phone service are different from the mobile cell

---

The Evolution of Personal Communications Systems (Boston: Kluwer Academic Publishers, 1996): 132-156.
[238] Ibid.
[239] Ibid.
[240] Ibid.
[241] Ibid.
[242] Bent Dalum, Christian R. Pedersen, and Gert Villumsen, "Technological Life-Cycles: Lessons from a Cluster Facing Disruption." *European Urban and Regional Studies* 12, no. 3 (2005): 229-246.
[243] Rafael Saraiva Campos, "Evolution of Positioning Techniques in Cellular Networks, from 2G to 4G." *Wireless Communications and Mobile Computing* 2017 (2017): 1-17.
[244] "IEEE Global History Network," *IEEE Transactions on Microwave Theory and Techniques* 65, no. 7 (2017): 2646.
[245] "The Evolution of Mobile Tech." *Advertising Age* 88, no. 5 (2017): 18.
[246] Richard Watson, *Fixed/Mobile Convergence and Beyond: Unbounded Mobile Communications* (Amsterdam; Newness/Elsevier, 2009): 543-587.
[247] Gwanhoo Lee, "What Roles Should the Government Play in Fostering the Advancement of the Internet of Things?" *Telecommunications Policy* 43, no. 5 (2019): 434-444.
[248] Ibid.

phone.[249] Hence, the internet made a big change in the way that telecommunication companies and authorities obtain data, and the internet helps them collect more metadata about people. The next chapter will be a legal analysis of four court cases related to the data privacy issue.

[249] Ibid.

Chapter 4

Legal Analysis

U.S. courts rely on precedents from old privacy cases in decision-making. These precedents standards impact the decisions of new privacy cases. Therefore, four case studies were used to show the gap between the old and new technology, which also related to data privacy and the Third-Party Doctrine issue—*Katz v. United States* (1967), *Smith v. Maryland* (1979), *ACLU v. Clapper* (2013), and *Klayman v. Obama* (2013). The analysis of each case followed the IRAC legal form (issue, rule, analysis, and conclusion) as well as the facts of each case. Furthermore, this chapter will call for the necessity to establish new regulations regarding the new technology. Lastly, these four court cases are selected to show the gap between the old and new technologies since the first two cases are used as precedent for the new cases that deals with the privacy issue.

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

Facts

Charles Katz, a resident of Los Angeles, California, was involved in sports wagering.[250] In 1965, Katz used a public telephone booth to transmit betting information to bookmakers.[251] The Federal Bureau of Investigation (FBI) started watching Katz closely, and decided to use listening device known as bug attached to the public phone booth that Katz used.[252] After many days of eavesdropping on calls through the bug device, the FBI detained Katz on charges of illegally transmitting gambling information.[253] The FBI considered spreading the information

[250] Katz v. United States, 389 U.S. 347 (1967).
[251] Ibid., 348.
[252] Ibid., 349.
[253] Ibid., 354.

over the phone a federal crime under Title 18 of the U.S. Code as transmission of wagering information.[254]

In the U.S. District Court for the Southern District of California, Katz and his lawyer tried to suppress the FBI recordings—claiming that the FBI agents did not obtain a search warrant from the judge allowing them to connect the bug device to the public phone booth.[255] Katz appealed to the U.S. Court of Appeals for the Ninth Circuit, where three judges of the court decided that the FBI's bug device did not penetrate inside the phone booth, and hence, the FBI did not violate the Fourth Amendment—there was no need for warrant.[256] Following the District Court's decision, Katz appealed to the Supreme Court, which agreed to hear the case on appeal.

Issue

Does the Fourth Amendment require federal agents to obtain a warrant in order to use the eavesdropping device?

Rule

In 1967, the Supreme Court decided in favor of Katz—under the Fourth Amendment, any government entity should obtain a warrant from the judge in order to conduct a search and seizure operation.[257] The court dismissed looking at whether the public phone booth was an area that should be protected by the constitution or not, and dismissed looking at whether people should have the "right of privacy" based on the place they were located.[258] Instead, the court stated that the Fourth Amendment does not focus on the places but focused on protecting people's privacy wherever they were located—home, work, public places, or private places.[259] The court also mentioned that the electronic listening to and recording of people's speech would be considered a

[254] U.S. Code, 18 U.S.C. § 1084.
[255] 389 U.S. 354.
[256] Ibid, 356.
[257] Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment*, 5th ed. (St. Paul, MN: West, 2012).
[258] Ibid, 577.
[259] Ibid, 578.

violation of their privacy, and therefore, recording Katz speech by phone should be done constitutionally under the Fourth Amendment—"search and seizure".[260] Justice John Marshall Harlan had a concurring opinion in this case and mentioned that the Fourth Amendment gave people reasonable expectation of privacy in their homes and at any time they needed the privacy.[261]

I agree with the ruling of the judge in this case since there is a clear definition of the individuals' expectations of their privacy in specific places. Furthermore, the judge clearly mentioned the expectations of the privacy places in a time which the technologies were limited and did not help the telephone companies a lot to gather information about the individuals. Therefore, the judge relied on the privacy argument of the places in this case.

Analysis

Katz has the right to privacy because he was inside the phone booth and he closed the door of the phone booth so he made a private space for himself.[262] The federal agents should obtain a warrant.[263] Regardless of Katz's illegal transmission of information of wagering, he was seeking a private place while using the public phone booth.[264] Katz's conversation should have been considered private until he finished speaking and left the phone booth.[265] The FBI agents used the bug or eavesdropping device without physical intervention, but under the Fourth Amendment, Katz's privacy could still be violated even if there was no physical involvement into the phone booth, which resulted in violation of the Fourth Amendment.[266] As Justice John

[260] Ibid, 578–79.
[261] Kugler and Strahilevitz, 1747-1812.
[262] Michael Vitiello, "Katz v. United States: Back to the Future?" *University of Richmond Law Review* 52, no. 2 (2018): 425.
[263] 389 U.S. 355.
[264] Tamar R. Gubins, "Warshak v. United States: The Katz for Electronic Communication," *Berkeley Technology Law Journal* 23, no. 1 (2008): 723-753.
[265] LaFave.
[266] The FBI agents violated the Fourth Amendment and a warrant should be obtained before listening to the phone calls.

Marshall Harlan mentioned about the expectation of privacy of people and the Fourth Amendment, the FBI agents should have a warrant before recording Katz's conversation on the public phone booth, and the warrant should be for a limited time; otherwise, Katz's privacy would be violated which means violation according to the Fourth Amendment and the people's expectation of privacy.[267]

Conclusion

Yes. Katz was entitled to the Fourth Amendment protection. The police should have obtained a warrant under Fourth Amendment procedures to record his conversations inside the phone booth.

Smith v. Maryland, 442 U.S. 735 (1979)

Facts

Smith v. Maryland,[268] a case heard by the Supreme Court of the United States in 1979 which it has connection to *Katz v. United States* (1967) in terms of the search and reasonable expectation of privacy.[269] In March 1979, a thief robbed Patricia McDonough in Baltimore, Maryland.[270] Patricia McDonough gave the police a description of the thief, as well as giving the model of the car that he drove in this incident: a 1975 Monte Carlo.[271] A few days after the incident, Patricia McDonough received many calls through her landline phone from the thief asking her to look from her house window to the street.[272] The police started monitoring Patricia's house hoping to see a Monte Carlo around the house.[273] The police checked a plate number for a

[267] LaFave, § 2.1(b).
[268] Smith v. Maryland, 442 U.S. 735 (1979).
[269] Ibid., 738.
[270] Applegate and Grossman, 753-785.
[271] Ibid, 756.
[272] Ibid.
[273] Ibid.

Monte Carlo and found a plate registered to a person called Lee Smith.[274] The police reached the telephone company and asked for the pen register[275]—often called a dialed number recorder, used to record the numbers called from a specific landline phone.[276] The pen register record showed that the calls Patricia received many times came from Lee Smith's phone. The police obtained a warrant to search Smith's house, and while searching Smith's properties, they discovered an address book that had Patricia McDonough's name.[277] After collecting the evidence, Lee Smith was detained, and Patricia McDonough was able to recognize him as the person who stole from her.[278]

In the pretrial period, Lee Smith filed a suit to suppress the evidence based on the information of the pen register, which was obtained without warrant.[279] The trial court refused Smith's motion and sentenced Smith to serve six years.[280] Smith did not stop at this point, instead, he decided to appeal to the Maryland Court of Special Appeals, in which it issued certiorari.[281] The Maryland Court of Special Appeals affirmed the conviction of the trial court and mentioned that there was no reason to apply the reasonable expectation of privacy for the dialed numbers in the pen register, and therefore, there was no need for a warrant and no violation to the Fourth Amendment.[282] In conclusion, Smith appealed to the U.S. Supreme Court.

Issue

[274] Ibid.
[275] Ibid.
[276] Ibid, 758.
[277] Ibid, 759.
[278] Alexander Galicki, "The End of Smith v. Maryland? The NSA's Bulk Telephony Metadata Program and the Fourth Amendment in the Cyber Age," *American Criminal Law Review* 52, no. 2 (2015): 375.
[279] Jeremy Derman, "Maryland District Court Finds Government's Acquisition of Historical Cell Site Data Immune from Fourth Amendment - United States v. Graham," *Suffolk University Law Review* 46, no. 1 (2013): 297.
[280] Applegate and Grossman, 753.
[281] Ibid, 754.
[282] Ibid.

Did the police violate the Fourth Amendment protection against unreasonable searches and seizures because they obtained the pen register without a warrant?

Rule

Justice Harry Blackmun with the majority opinion held that: "Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a 'search' necessarily rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone. This claim must be rejected."[283] The court said that there was no violation to the Fourth Amendment, and the police did not need a warrant to obtain Smith's call information from the pen register.[284] Justice Potter Stewart dissented, arguing that people who use the landline phone service should have the expectation of privacy.[285] Justice William J. Brennan agreed with the dissent of Justice Potter Stewart, and both justices claimed that the content of the call should be private just as *Katz v. the United States* upheld.[286] However, the court declared the opinion on this case with a five to three majority: there is no reasonable expectation of privacy, which is the reverse of the rule of *Katz v. the United States*, where the court ruled that there was reasonable expectation of privacy for the content of the call.[287] Notably, the rule of the Supreme Court in both cases was different, wherein *Katz v. the United States* the rule focused on the content of the call which it considered private and the police had to obtain a warrant in order to reach the call information; while in *Smith v. Maryland* the court considered the information in the pen register was not private because subscribers of the landline phone were giving this information voluntarily. Therefore, there are different circumstances between the two cases, which has resulted in two different decisions. Also, the called or dialed phone numbers

[283] Ibid, 755.
[284] Ibid.
[285] Erwin Chemerinsky, "Protecting Electronic Privacy*," Judicature* 103, no. 1 (2019): 76-96.
[286] Robert Ditzion, "Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers," *American Criminal Law Review* 41, no. 3 (2004): 1321.
[287] Ari Herbert, "Changing Tack in the Night: The Supreme Court's Misapplication of Katz," *American Journal of Criminal Law* 44, no. 2 (2017): 253-259.

recorded by the pen register are considered an early version of what is now called metadata. The other note between *Smith v. Maryland* and *Katz v. the United States*, the technology was different. The phone booth and bug device were used in *Katz v. the United States*, while the pen register was used in *Smith v. Maryland.*[288]

I disagree with the ruling of the judge in this case since Smith has no other choice to make a phone call, and he has to subscribe to telephone service in order to make a phone call at that time. Therefore, Smith might not give his phone number to the telephone company voluntarily; instead, he might give his phone number under an indirect pressure of using the service of the telephone company.

Analysis

Justice Harry A. Blackmun issued the court opinion and stated that landline phone subscribers were giving their information to the phone company voluntarily not coercively.[289] The phone company used the pen register and other devices to check the bill, check in specific cases like fraud, and to check for any violations by the subscribers.[290] Furthermore, the phone company used the pen register to track the bill of each subscriber as well as the record of special rate subscribers.[291] From another corner, Justice Harry A. Blackmun further analyzed this case by stating that the Fourth Amendment applied to the individual who thought that the government infringed on their personal information.[292] The case of the pen register was not considered infringement to the individual's information because the subscribers provided their information voluntarily, and they should already know that the phone company kept a record of their calls as a part of their regular business conduct.[293]

---

[288] National Archives Oversight, vol. 110-542 (U.S. G.P.O., 2008).
[289] 442 U.S. 739.
[290] Galicki, 375.
[291] Applegate and Grossman, 753-778.
[292] A Bill to Authorize the Project for Environmental Restoration, vol. 107-328 (Washington, DC: U.S. G.P.O., 2002).
[293] 442 U.S. 738.

The phone company needed the telephone numbers to connect the calls, and the customer is supposed to be aware of this process. Therefore, the information in the pen register cannot be private.[294] The majority opinion in this case relied on the Third-Party Doctrine that people are giving their information voluntarily not coercively to any company.[295] Justice Thurgood Marshall and Justice William Brennan have a dissent and expressed their disagreement with the Third-Party Doctrine: "Since I remain convinced that constitutional protections are not abrogated whenever a person apprises another of facts valuable in criminal investigations. The use of pen registers, I believe, constitutes such an extensive intrusion. To hold otherwise ignores the vital role telephonic communication plays in our personal and professional relationships, see Katz v. United States, as well as the First and Fourth Amendment interests implicated by unfettered official surveillance. Privacy in placing calls is of value not only to those engaged in criminal activity."[296] However, technology played a crucial role in these two cases, and the judges explained their opinion and correlated the bug device in *Katz v. the United States* and the pen register in *Smith v. Maryland.*[297] It is important to mention that these two cases happened at a time when the use of the landline phone was pervasive in the United States, and the decisions on these two cases focused on devices related to the landline services: bug device and the pen register. Also, these two cases are still precedents even though landline phones have since been replaced by more modern devices.

Conclusion

[294] Ibid.
[295] Legislation to Implement the Recommendations of the Commission on Wartime Relocation and Internment of Civilian*s*, (U.S. G.P.O., 1988).
[296] Ibid.
[297] Civil Liberties Act of 1985 (U.S. G.P.O., 1987).

No. The reasonable expectation of privacy does not apply to the pen register and the recorded numbers. The Fourth Amendment does not apply to any information given voluntarily to the third party.

American Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013)

Facts

A legal challenge was filed by the American Civil Liberties Union (ACLU) against the United States federal government.[298] ACLU, a non-profit organization, filed a lawsuit against the National Security Agency (NSA) claiming that the latter had a program collecting phone metadata.[299] The story of this case started in the wake of a big noise in the news when a report revealed mass surveillance by the NSA of United Stated citizens and foreigners, where the media titled this event under Global surveillance disclosures.[300] A collection of classified documents released by Edward Snowden—whistleblower, employee and contractor with Central Intelligence Agency (CIA) —revealed many papers about American, Canadian, Australian, and British intelligence obtained from "Five Eyes" network.[301] Five Eyes Intelligence Alliance is an intelligence cooperation agreement between five countries (Australia, Canada, New Zealand, the United Kingdom and the United States), in which they cooperate and exchange security information about suspects, citizens, or foreigners.[302]

The *Guardian* newspaper revealed a report about a request from the NSA asking Verizon to release information related to communication records of its subscribers for a three-month

[298] American Civil Liberties Union v. Clapper, 959 F.Supp.2d 724 (S.D.N.Y. 2013).
[299] Ibid.
[300] Erin E. Connare, "ACLU v. Clapper: The Fourth Amendment in the Digital Age." *Buffalo Law Review*. 63 (2015): 395-405.
[301] Ibid, 398.
[302] Ibid, 399.

period.[303] Rather than requesting the content of the call, NSA required the following information: call location, time, duration, and numbers of both callers.[304]

The director of National Intelligence James R. Clapper was sued by The American Civil Liberties Union because of the metadata collection program.[305] ACLU claimed that the requested metadata from Verizon was considered private data and this request should have been considered an invasion of privacy and violation of the search and seizure protections meted under the Fourth Amendment, as well as a violation to the First Amendment because it could prevent free speech.[306]

In 2013, the court dismissed the case and declared that collecting metadata did not violate the Fourth Amendment.[307] In 2014, the ACLU appealed to the United States Court of Appeals for the Second Circuit.[308] In 2015, the court declared that the NSA did not violate the Fourth Amendment, and the PATRIOT Act allowed security agencies to fight against terrorism; and therefore, this is a strong reason to permit mass-data surveillance.[309]

Issue

Whether or not mass NSA surveillance violates the Fourth Amendment.

Rule

In 2013, the district court dismissed the case.[310] The district court rule was as follows: "phone users had no reasonable expectation of privacy that would give them Fourth Amendment rights. Citing the 1979 *Smith v. Maryland* decision as precedent, the court found that, under the

[303] Ibid.
[304] Ibid.
[305] Stephen L. Davis, "Conflicting Court Decisions Leave Constitutional Privacy Protections Against Mass Data Collection Uncertain," *Journal of Internet Law* 17, no. 11 (2014): 3.
[306] 959 F.Supp.2d 724.
[307] Connare, 395.
[308] 959 F. Supp. 2d 724.
[309] Ibid.
[310] William H. Pauley III, "United States District Court Southern District of New York: American Civil Liberties Union v. James R. Clapper (13 Civ. 3994)," *American Civil Liberties Union* 18, no. 13 (2015): 3.

Fourth Amendment, individuals have no expectation of privacy for information they provide to third parties, like phone companies."[311] Clearly, the United States District Court for the Southern District of New York used *Smith v. Maryland* as precedent in this case. There is a difference in technology between the two cases due the time period of each case. In *Smith v. Maryland*, the Supreme Court rule was based on the landline service and the pen register.[312] While in *American Civil Liberties Union v. Clapper*, the court looked at the cellphone service of Verizon and the other information related to the subscribers which it usually stores in the cloud. Instead, the court ruled based on a Supreme Court case (*Smith v. Maryland*) that had old technology and a different logic from what *American Civil Liberties Union v. Clapper* used for ruling in their case.[313] More specifically, there were no reasons to compare the landline service technology with the metadata and cell phone service used today.[314]

I disagree with the ruling of the judge in this case since the technology discussed in this case is different from the technology used in *Smith v. Maryland's* case. Specifically, the pen register is a simple device used to record the callers' phone numbers only, while Verizon's software is developed and sophisticated technology that enabled Verizon to collect more metadata and more private data. Therefore, the judge might consider this point when ruling in this case.

Analysis

Judge William Pauley said that there was no expectation of privacy for the cellphone subscribers, and therefore, there was no violation to the Fourth Amendment in *American Civil Liberties Union v. Clapper*.[315] The United States District Court for the Southern District of New

---

[311] 959 F.Supp.2d 724.
[312] National Archives Oversight: Protecting our Nation's History for Future Generations: Hearing before the Federal Financial Management, Government Information, Federal Services, and International Security Subcommittee of the Committee on Homeland Security and Governmental Affairs, United States Senate, One Hundred Tenth Congress, Second Session, May 14, 2008, vol. 110-542 (U.S. G.P.O., 2008).
[313] Ibid.
[314] ACLU v. Clapper, 785 F.3d 787 (motion for appeal, 2015).
[315] Connare, 395-398.

York found that there was no violation to the Fourth Amendment if the subscribers give their information voluntarily to the cell phone company.[316] The subscribers should not expect their data remains private, and the cellphone company has the right to share such data with government agencies if needed.[317] In addition, the court used of the USA PATRIOT Act of 2001 to justify the legality of the using NSA's program.[318] The court also used Section 215 of the USA PATRIOT Act of 2001 to justify the legality of using NSA's program. "In adopting §215 of the USA PATRIOT Act of 2001, Congress intended to give the government, on the approval of the Foreign Intelligence Surveillance Court, broad-ranging investigative powers analogous to those traditionally used in connection with grand jury investigations into possible criminal behavior."[319] The court analysis further claimed that Section 215 of the USA PATRIOT Act of 2001 gives government security institutions flexibility in their work[320] in order to undermine terrorist threats;[321] and therefore, the court should not require a warrant from the NSA in order to collect metadata from the cellphone company (Verizon).[322]

The court also analyzed this case from another corner by comparing it to *Smith v. Maryland*. The United States District Court for the Southern District of New York found that in both cases *American Civil Liberties Union v. Clapper* and *Smith v. Maryland* the subscribers gave their information voluntarily and not coercively, and in both cases the phone companies needed the data for routinely business.[323] Furthermore, the court found the NSA program in *American Civil Liberties Union v. Clapper* was similar to the bug device in *Smith v. Maryland*, which in

[316] Mark D. Young, "National Insecurity: The Impacts of Illegal Disclosures of Classified Information," *I/S: A Journal of Law and Policy for the Information Society* 10, no. 2 (2014): 367-406.
[317] 785 F.3d 787.
[318] USA PATRIOT ACT § 215; 50 U.S.C.S. § 1861.
[319] 785 F.3d 787-788.
[320] Ibid, 787; U.S.A.PATRIOT ACT §215; 50 U.S.C.S. §1861.
[321] 959 F.Supp.2d 726.
[322] Ibid, 728.
[323] Nadine Strossen, "Why the American Civil Liberties Union Opposes Campus Hate Speech Codes," *Academic Questions* 10, no. 3 (1997): 33-40.

both cases recorded basic information about the subscribers.[324] The court added that in both cases the technology helped the government agency to find out important information about the suspect.[325] Finally, the court said in the *Smith v. Maryland* findings that there was no expectation of privacy to the data of the subscribers since they gave it voluntarily to the phone company; and therefore, in *American Civil Liberties Union v. Clapper* the court should follow the same path since the subscribers voluntarily gave their information to Verizon.[326]

Conclusion

No. Collection of data by the National Security Agency without a warrant is not a violation of the Fourth Amendment.

Klayman v. Obama, 957 F. Supp. 2d 1 (D.C.D.C. 2013)

Facts

Klayman v. Obama was decided by United States District Court for the District of Columbia on December 16, 2013.[327] The story of *Klayman v. Obama* started when international news media revealed secret information about the United States' National Security Agency (NSA) as well as global surveillance,[328] reporting both agencies were involved in mass surveillance of US citizens and citizens from other countries.[329] Just as in the American Civil Liberties Union v. Clapper case, Edward Snowden, the former employee of and contractor for the Central Intelligence Agency (CIA), inspired the *Klayman v. Obama* case,[330] in which the press, including

[324] 959 F.Supp.2d 729.
[325] Ibid, 731.
[326] Ibid, 732.
[327] Klayman v. Obama, 957 F. Supp. 2d 1 (D.C.D.C. 2013).
[328] Joshua M. Mastracci, "Klayman v. Obama: The D.C. District Court Misinterprets the NSA Metadata Collection Program as a Violation of Individual Fourth Amendment Rights," *Tulane Journal of Technology and Intellectual Property* 17 (2014): 365-374.
[329] Christopher J. Deist, "Taking a Stand: Addressing the Issue of Article III Standing Against the NSA Metadata Collection Program Following Obama v. Klayman," *George Mason Law Review* 24, no. 1 (2016): 285.
[330] Damacio V. Posadas, Jr., "After the Gold Rush: The Boom of the Internet of Things, and the Busts of

The Washington Post and *The Guardian,* published information about surveillance to attract the public's attention.[331]

Shortly after the secret papers were revealed in *The Washington Post* and *The Guardian*, Larry Klayman, an independent lawyer and political activist,[332] filed a lawsuit against NSA challenging the legality of using a program that collected phone metadata information.[333] Larry Klayman's lawsuit considered another challenge to NSA's order of metadata collection program of personal information.[334]

In 1978, Congress established the Foreign Intelligence Surveillance Act (FISA),[335] which prohibited any kind of domestic surveillance except orders approved by the Foreign Intelligence Surveillance Court (FISC).[336] Initially, FISC could grant orders for electronic domestic surveillance to law enforcement agencies in cases where there was convincing evidence of probable cause to indicate the planning of terrorism or a harmful act.[337] FISA has been amended many times since 2001.[338] The last FISA updated was In 2008 to give national security agencies a wider power to use electronic surveillance due to the 2001 terrorist attacks on the United States.[339]

Issue

Does the use of the program by the government without warrant violate the Fourth Amendment?

Data-Security and Privacy," *Fordham Intellectual Property Media & Entertainment Law Journal* 28, no. 1 (2017): 69-108.

[331] Marc Sketchler, "I Didn't Say That: The Ninth Circuit's Novel and Important Extension of Copyright Protection in Garcia v. Google, Inc.," *Tulane Journal of Technology and Intellectual Property* 17 (2014): 353-364.

[332] Deist.

[333] 957 F. Supp. 2d 1.

[334] Ibid.

[335] Ibid.

[336] Ibid.

[337] Ibid.

[338] Ibid.

[339] Ibid.

Rule

In 2013, Judge Richard J. Leon, District Judge of the District Court of Columbia,[340] declared that metadata collection by the NSA violated the Fourth Amendment, "I cannot imagine a more 'indiscriminate' and 'arbitrary' invasion than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval... Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment."[341] The court considered the collection of metadata by the NSA invasive to the privacy of Verizon's customers.[342] Judge Leon looked at the case away from the FISA court, where it was granted approval for search and surveillance because of what they called an "imminent attack" by terrorists, and here the defendant relied heavily on this reasoning.[343] Judge Leon mentioned that NSA failed to provide any evidence showing that there was an imminent attack,[344] and the NSA security agencies failed to explain whether there was important reason to stop attack or harm to the people,[345] and so thus they had no reasonable excuse to collect the metadata information without warrant.[346]

The Judge mentioned that the situation in *Smith v. Maryland* was different than in this case.[347] Judge Leon said that in *Smith v. Maryland* the pen register used in collecting the information about the landline phone subscribers was necessary for the phone company at that time.[348] In this case, the NSA used a different technology device (specifically a computer program) to collect metadata about people; hence, different technology used in different time.[349]

---

[340] Arthur Herman and John Yoo, "A Defense of Bulk Surveillance - The NSA programs enhance security without uniquely compromising privacy," *The National Law Review* 8 (2012): 132-164.
[341] 957 F. Supp. 2d 1.
[342] Ibid.
[343] Ibid.
[344] Mastracci, 365-74.
[345] Young, 367-406.
[346] Herman and Yoo.
[347] Ibid.
[348] Ibid.
[349] Ibid.

Judge Leon said that the Fourth Amendment needed to be updated based on the digital technology age.[350]

I agree with the ruling of the judge in this case because there is a difference between the technology used in the court cases related to the privacy issue during the 1960s and 1970s and the technology in today's privacy court cases. Judges might need to look at the circumstances that surrounded the privacy cases and compare the evidence used between the old and new court cases before using the old ones as precedents for the new court cases.

Analysis

The United States District Court for the District of Columbia said that the plaintiff claimed that collecting a bulk of metadata information was breaching the privacy of Verizon's phone subscribers, and the NSA needed to obtain a warrant from the court before collecting information.[351] Judge Richard J. Leon said that although that the court did not find any evidence of analyzing Verizon subscribers' personal data,[352] he believed that having the subscribers' information without a warrant from the court or without their consent[353] lead to a violation of the Fourth Amendment.[354] Judge Leon mentioned that NSA's search violated the reasonable expectation of privacy and thus, violated the Fourth Amendment.[355] The court investigated further and compared this case with *Smith v. Maryland*.[356] The court said that in *Smith v. Maryland*, the government collected data from a pen register of a landline about a suspect.[357] The court said that in *Smith v. Maryland*, the government provided evidence about the suspect, but in this case the

[350] Ibid.
[351] Ibid.
[352] Mastracci, 365-74.
[353] Ibid, 368.
[354] Dalmacio V. Posadas Jr., "After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy," *Fordham Intellectual Property Media & Entertainment Law Journal* 28 (2017): 69-98.
[355]Ibid, 73.
[356]Ibid.
[357] Mastracci, 365-74.

government failed to provide a single piece of evidence about stopping what they called an imminent attack.[358] Finally, Judge Leon emphasized the idea that *Smith v. Maryland* has become an outdated precedent.[359]

Conclusion

Yes. The government violated the Fourth Amendment.

The cases mentioned above clearly show that telecommunication companies are sharing their subscribers' private data with government security agencies, as seen in *American Civil Liberties Union v. Clapper* and *Klayman v. Obama*. Most importantly, government agencies have made multiple "gentlemen's agreements" with telecommunication companies based on shrewd and indirect political pressure. In the telecommunication industry, a gentlemen's agreement is a non-binding verbal agreement between telecommunications companies' government departments, especially security ones, and is usually concluded without written documentation.[360] Telecommunication company subscribers' private data is usually shared due to gentlemen's agreements. In many cases, the security agencies coerce telecommunication companies to share their subscribers' private data under the justification of a suspected terrorist attack that threatens the American people, as shown by *American Civil Liberties Union v. Clapper* and *Klayman v. Obama*.

There are also laws, such as the PATRIOT Act, the Cybersecurity Information Sharing Act,[361] and the Communications Assistance for Law Enforcement Act,[362] that require

[358] Dalmacio V. Posadas. Jr., "The Internet of Things: Abandoning the Third-Party Doctrine and Protecting Data Encryption," *Gonzaga Law Review* 53, no. 1 (2017-2018): 89-116.
[359] Jane Chong, "Government Files Reply in Klayman v. Obama, ACLU Moves to Participate in Oral Argument," *Lawfare: Hard National Security Choices* 8 (2013):119-148.
[360] David Allen, "The Gentleman's Agreement in Legal Theory and in Modern Practice," *Anglo-American Law Review* 29, no. 2 (April-June 2000): 204-227.
[361] Pub. L. 114-113 (2015).
[362] Pub. L. 103-414 (1994).

telecommunication companies to hand data over to the government. For example, the Cybersecurity Information Sharing Act (CISA) is a federal law signed under Obama's administration back in 2015 that aims to share users' private information on the Internet between the telecommunication companies with the government, specifically, the security agencies.[363] The Obama administration mentioned that applying CISA will ensure that the sharing of people's private data with the government security agencies will enhance the cybersecurity in the US.[364] Furthermore, CISA, along with other laws like the Communications Assistance for Law Enforcement Act and the PATRIOT Act, gives telecommunication companies a reason to share people's private data with government security agencies. As a result, there is no control of the subscribers' private data that is transferred from the telecommunication companies to the government security agencies, such as the transfer of Verizon subscribers' private data to the NSA as discussed in *American Civil Liberties Union v. Clapper* and *Klayman v. Obama*.

The same issue is associated with the USA PATRIOT Act and the USA Freedom Act, where the government mandates the sharing of private data between telecommunication companies and government security agencies. The USA PATRIOT Act was established on October 26, 2001, under President George W. Bush's administration.[365] The USA PATRIOT Act gives a lot of power to government security agencies to collect people's private data under the pretext of fighting terrorism.[366] The United States Congress and Senate mentioned that the main goal of the USA PATRIOT Act is to give government security agencies all the possible power to take the necessary steps to keep the nation safe.[367] On the other hand, the USA Freedom Act was

[363] John Heidenreich, "The Privacy Issues Presented by the Cybersecurity Information Sharing Act." *North Dakota Law Review* 91, no. 2 (2015): 395.
[364] Jungmihn Ahn, "Issues Presented by Cybersecurity Information Sharing Act *2015*." *Yonsei Law Review* 28, no. 4 (2018): 259-282.
[365] Ibid, 263.
[366] Carol R. Van Cleef, "The USA PATRIOT Act: Statutory Analysis and Regulatory Implementation," *Journal of Financial Crime* 11, no. 1 (2004): 73-102.
[367] Ibid.

established in 2015 and carries some revisions of the USA PATRIOT Act, such as electronic surveillance and the collecting of metadata about telecommunication services' subscribers.[368] The USA Freedom Act forced some limitations on the collection of people's private data by government security agencies.[369]

One important fact has to be mentioned regarding the type of property being searched by government security agencies. For instance, government security agencies, such as the NSA, claim that the Fourth Amendment requires a warrant to search people's private property, such as books, papers, etc. (tangible property). At the same time, the government security agencies are saying that the Fourth Amendment does not require a warrant to search new types of private property, such as electronic data (intangible property). In this situation, the government security agencies are using this claim of a new type of property (intangible property) to search people's private data without obtaining a warrant. Therefore, lawmakers should recognize that there is a difference between the type of private property being searched (tangible versus intangible private property), and this basically happened in old cases such as *Katz v. United States* and *Smith v. Maryland*, versus the new cases, such as *ACLU v. Clapper* and *Klayman v. Obama*. Last, the Clapper and Klayman cases are split precedents; while they were largely about the same issue in different courts, each case had a different ruling because of the effects of the technology on the cases' decisions in the courts. The reason for the different decisions is that in the Clapper case, Judge Pauley talked about terrorism and did not mention technology in the analysis of the case. In the Klayman case, Judge Leon focused only on the new technologies and did not talk about terrorism in the analysis of the case.

[368] Tom Leithauser and John Curran, "Sen. Leahy Offers New USA Freedom Act Backed by Privacy Groups, White House." *Cybersecurity Policy Report* (2014).
[369] Ibid.

To summarize, *Katz v. United States* and *Smith v. Maryland* are used heavily today in the courts as a precedent to solve new cases related to data privacy. The judges in *ACLU v. Clapper* and *Klayman v. Obama* came up with a split precedent for the same issue. In both cases, *ACLU v. Clapper* and *Klayman v. Obama*, the NSA was involved in collecting subscribers' private data. Also, in both cases, the NSA did not obtain a warrant before collecting people's private data. The only difference between the two cases *ACLU v. Clapper* and *Klayman v. Obama* is that two different judges had different opinions on the cases. In *ACLU v. Clapper*, the judge used *Smith v. Maryland* as a precedent in his ruling and mentioned the NSA does not have to obtain a warrant before collecting subscribers' private data, while in *Klayman v. Obama,* the judge mentioned that *Smith v. Maryland* could not be used as a precedent due to different circumstances between *Klayman v. Obama* and *Smith v. Maryland*. Clearly, there is confusion on how to solve the privacy issue cases that are related to searching people's private data (the intangible private property). The essential point that should be mentioned is that there is a gap in the technology between the old (e.g., landline) and the new (e.g., cell phone/internet) and the type of data. Hence, the differences between the two technologies made the use of the old privacy cases such as *Katz v. United States* and *Smith v. Maryland* not applicable in new privacy cases like *ACLU v. Clapper* and *Klayman v. Obama*. From my personal standpoint, judges should not apply old cases as a precedent to new cases related to new technologies and new types of data. Judges should adopt Judge Leon's position. Through *Klayman v. Obama* (2013), we see that there is only one judge who mentioned that there should be a separation between the old privacy court cases that carry the old technology and the new court cases that have different technology. The U.S. courts need more judge voices like the voice of Richard J. Leon, District Judge of the District Court of Columbia, who declared that the era of the old privacy court cases should be abandoned due to the technological gap between the 1960s and 1970s and today's privacy court cases. Furthermore, the U.S. courts need more judges looking at the effects of the new technology devices used by the

telecommunications and digital media companies, which breaches the privacy of the people's private data. Lastly, the application of the Fourth Amendment could be difficult for new cases that are related to new technology, such as cell phones and the internet.

Chapter 5

Discussion

People's private spaces have become smaller and smaller in the wake of new means of online communications and advancements in telecommunications technology that allow third parties (telecommunication and digital media companies) sharing of personal information. These third parties can share private data with the government, yet there is still no law in the U.S. to govern these parties. Hence, it becomes increasingly crucial for lawmakers to pay extra attention to the problem of data privacy propagation and the third-party impact of telecommunications and digital media companies.

This thesis investigates three important areas related to the privacy issue represented by the application of the Fourth Amendment over the history, the development of the telephone and landline phone services over history, and analysis of old and new court cases related to privacy issues.

For the first part of the investigation regarding the data privacy issue— the application of the Fourth Amendment and the search and seizure process over the history—the thesis explored how the search and seizure process applied historically to surveillance issue cases, which could help lawmakers understand why and for what reasons the Fourth Amendment was established in the United States. As a result, lawmakers could apply the Fourth Amendment in a proper way, especially in privacy issue cases. Furthermore, in this part, the thesis sheds light on the factors behind establishing the Fourth Amendment—specifically, the search and seizure process during the colonial era. Important areas were explored, such as what made Founding Fathers like James Madison and others in 1789 introduce the Fourth Amendment at that time.[370] Therefore, the

[370] Mary Helen Wimberly, "Rethinking the Substantive due Process Right to Privacy: Grounding Privacy in the Fourth Amendment," *Vanderbilt Law Review* 60, no. 1 (2007): 283.

essential points explored from the history of the establishment of the Fourth Amendment are the following:

First, the application of the Fourth Amendment and the search and seizure process over history reveals a single relationship when applying that process—namely, the government and the citizens did not show any other party involved in the search and seizure process. Yet, currently, third parties like telecommunications and digital media companies collect people's private data and share it with government agencies—as happened in *American Civil Liberties Union v. Clapper*, where Verizon shared a subscribers' metadata with the NSA. In this situation, Verizon, which stands between the government and the citizens, shared subscribers' metadata with government security agencies, such as the NSA. The sharing of people's private data by third parties changes the search and seizure application and eventually changes the application of the Fourth Amendment. As a result, applying the Fourth Amendment might now be difficult in cases involving new types of data privacy issues. Therefore, establishing privacy law focused on protecting private data could solve the problem of sharing people's private data, and judges would have newer statutes that are grounded in current realities.

Second, the application of the search and seizure process over time reveals that a warrant should be obtained before starting the process. Still, nowadays, government security agencies search people's private data without obtaining a warrant. That is to say, government security agencies like the NSA obtain people's private data without spending the time and effort to obtain warrants, as required by the Fourth Amendment. The government security agencies claim that the Fourth Amendment requires a warrant to search people's private property, such as books, papers, etc. (tangible property), but a warrant is not required to search for the new types of private property, such as electronic data (intangible property). Therefore, lawmakers should pay attention to the change of the private property being searched (tangible versus intangible private property) and establish new privacy laws that could protect people's private data because the Fourth

Amendment might not work with the new type of privacy data issue cases.

For the second part of the investigation regarding emerging telecommunication technologies, landline phone service widely diffused during the 1960s and 1970s. At that time, the technology that was used with the landline phone service had a limited feature that allowed the telephone companies to record only the outgoing calls.[371] From the early 1980s to the following years, the first generation network (or 1G network) was introduced to the market,[372] followed by a 2G network.[373] With 1G and 2G networks, telecommunications companies were able to have more data recorded about the subscribers, like their names and addresses,[374] as well as necessary metadata like the times of the calls and whether they were outgoing or incoming.[375] Hence, lawmakers should pay attention to the gap between old technology and new technology—landline phones vs. cell phones. Furthermore, the gap between the old and new technology increased after introducing 3G and increased even more with a 4G network.[376] With the 4G network, telecommunication companies can collect more metadata about subscribers by using software and other advanced technological tools.[377] As a result Congress should consider updating existing privacy laws, or enacting a new law, to address the collection of private data by third parties. For the third and final part of the investigation regarding the court cases, the U.S. district courts have been using old Supreme Court cases, as shown in chapter 4. The U.S. courts have been relying on old cases as precedents to address new disputes in new cases with new technology. *Katz v. United States* and *Smith v. Maryland* happened at a time when the

[371] Philip J. Weiser, "Institutional Design, Fcc Reform, and the Hidden Side of the Administrative State," *Administrative Law Review* 61, no. 4 (2009): 675-721.
[372] Ibid, 678.
[373] Ibid.
[374] Ibid.
[375] Ibid.
[376] Niharika Singh and Singh Saini Mandeep, "Performance Evaluation of Secure Asymmetric Key Exchange Mechanisms for 4G Networks," *International Journal of Computer Applications* 118, no. 23 (2015): 10-15.
[377] Mohammed Ahmed Truki AlSudiary, "Perspectives of Managing Mobile Service Security Risks," *International Journal of Distributed Sensor Networks* 311, no. 7 (2015): 592-634.

telecommunication means and digital technology were very simple compared to *ACLU v. Clapper* and *Klayman v. Obama*, where the technology was more complicated than before. Furthermore, nowadays, the Internet impacts the way people's private data is collected and stored, such as the way that people's private data is collected in *ACLU v. Clapper* and *Klayman v. Obama*. During *Katz v. United States* and *Smith v. Maryland*, the Internet had not been invented, and the judges relied on evidence related to basic technology to rule on the cases. Also, in the old court cases such as *Katz v. United States* and *Smith v. Maryland*, the distinction between private and public place is obvious, while in the new cases like *ACLU v. Clapper* and *Klayman v. Obama*, the distinction between the public and private places is not obvious. For example, it is not clear whether the Internet servers are private or public places where people's data is stored in it, so people should expect privacy for their information if it is in private places. Therefore, *Katz v. United States* and *Smith v. Maryland* are different than the new court cases. These differences might have an effect on the legality of the decisions in the new court cases that are related to the privacy issue. Therefore, legislators should establish new laws regarding new technologies to stop the sharing of people's private data. However, there are seven main factors further analysis the logical and legal differences between the old court cases *Katz v. United States, Smith v. Maryland*, and the new court cases—*ACLU v. Clapper* and *Klayman v. Obama*, and explain how these factors hinder the old court cases from being used as precedents in the new privacy issue cases. These factors are as follows:

The first factor that must be mentioned is the technology. Technology plays a pivotal role in the decisions of old court cases. Specifically, in *Smith v. Maryland*, the decision of the court relied on the pen register, an old electronic device used to record the callers' phone numbers.[378] The court mentioned that the reasonable expectation of privacy does not apply to the pen register

[378] Christian Schultz and David Hammel, "Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute," *The Notre Dame Law Review* 76, no. 4 (2001): 1215.

and the recorded numbers. The Fourth Amendment does not apply to any information given voluntarily to a third party. On the other side, in *American Civil Liberties Union v. Clapper*, the court used *Smith v. Maryland* as a precedent, and the judge used the same argument as *Smith v. Maryland by* mentioning that the reasonable expectation of privacy does not apply to Verizon's software that collects people's data. Furthermore, the court in *American Civil Liberties Union v. Clapper* mentioned that Verizon's subscribers gave their data voluntarily and not coercively to Verizon. Therefore, there is no expectation of the privacy of their data. As a result, there is no difference between the pen register versus Verizon's software and its uses in collecting people's private data.

The second factor is "reasonable expectations of privacy." In *Katz v. United States*, the judge ruled in favor of Katz and mentioned that the government could not record people if they are in a place where it could consider a private place. In *Katz v. United States*, the judge considered a public phone booth a private place, with "reasonable expectations of privacy." However, one of the critical problems with the decision in *Katz v. United States*, especially as it relates to new cases with new types of private data, is that the decision solely depends on the judge's decision about whether a place is considered private or not. The "reasonable expectations of privacy" in *Katz v. United States* might no longer work when defining the private and public places in our digital technology spaces, where digital data is stored and shared in a virtual space like servers. For instance, will judges consider data that the telecommunications companies obtain from cell phones and store in the cloud private or public? Are people's activities on digital network sites like Twitter and Facebook considered private or public? Furthermore, there is also a distinction between the conversation of Katz in *Katz v. United States* versus the metadata collected in the new cases like *American Civil Liberties Union v. Clapper*. Therefore, *Katz v. United States* might no longer be used as a precedent in new court cases that deal with new types of digital privacy issues.

The third factor is establishing new acts that force the telecommunication companies to share people's private data with government security agencies under the pretext of maintaining cybersecurity. Acts like the Cybersecurity Information Sharing Act and the Communications Assistance for Law Enforcement Act require telecommunication companies to hand data over to the government security agencies. These acts increase the pressure on the telecommunication companies to share the private data of their subscribers with the government in order to enhance cybersecurity in the United States. Those acts could cause pressure and lead to the sharing of subscribers' private data. It would be transferred by the telecommunication companies and government security agencies. This happened in new court cases such as *American Civil Liberties Union v. Clapper* and *Klayman v. Obama*. This kind of pressure did not exist in older court cases like *Katz v. United States* and *Smith v. Maryland*, since there were no such acts that required the telecommunication companies to share subscriber's private data with the government to enhance cybersecurity. As a result, the rules on *Katz v. United States* and *Smith v. Maryland* were in different circumstances than *American Civil Liberties Union v. Clapper* and *Klayman v. Obama*.

The fourth factor is the difference between the types of data being searched in old and new cases. For example, in *Smith v. Maryland*, the type of the data searched by the police at that time included physical pen register records (tangible records, like papers that have lists of the caller's name and phone numbers); in *American Civil Liberties Union v. Clapper,* this search included intangible property (data stored in virtual repositories, like call times and voice records). At this point, the intangible property could be collected or recorded instead of searched and seized like the data in *American Civil Liberties Union v. Clapper* because this type of data cannot be physically touched by hand unless the conversation is written on paper. At this point, the paper would be considered tangible property and might need a warrant before it is collected. As a result, the Fourth Amendment could be applicable in *Smith v. Maryland*. Still, it might not apply to *American Civil Liberties Union v. Clapper* since the data was not searched and seized physically.

Therefore, the difference in the type of searched data between old and new court cases makes the old ones inapplicable as precedents for the new cases.

The fifth factor is the Internet. The Internet helps telecommunication and digital media companies collect more digital private data and store them in temporary repositories called servers. In our current era, the Internet has made massive changes in the way data is collected and stored by telecommunication companies. Previously, the telephone companies used simple means to record the subscribers' available private data like numbers and names. Therefore, judges might forget that both *Katz v. the United States* and *Smith v. Maryland* happened in the 1960s and the 1970s when there was no Internet service. For instance, in the ruling for *Katz v. the United States*, the court relied on the information that the police obtained from listening to a public phone booth to analyze as well as to judge the case. The court mentioned that the phone booth is considered an area that should be protected by the Constitution, and people should have the "right of privacy" inside the phone booth. As a result, the police's obtained information from the phone booth has violated the Fourth Amendment. In both cases, *American Civil Liberties Union v. Clapper* and *Klayman v. Obama*, peoples' private data were stored on the Internet in a cloud. At this point, the difference here is the Internet, which offered a new place to store the data. The argument in this situation is the data is neither "searched" nor "seized" from the Internet; instead, the data could be "tracked" and "recorded" from the Internet. As a result, "tracking" and "recording" have nothing to do with the Fourth Amendment since it's not "searching" and "seizing." Therefore, the Internet and its use make the old privacy court cases inapplicable as a precedent in the new privacy court cases.

The sixth factor is the limitation of the old cases' collected data versus the plethora of collected data in the new court cases. The limitation versus surfeit of the private data could be a complementary point to the technology and the Internet points mentioned earlier. Previously, there were limitations on the collection of people's private data. Today, telecommunication and

digital media companies exploit technology and the Internet to collect a large amount of private data. In the ruling *Smith v. Maryland,* the Supreme Court mentioned that the telephone company kept only a limited record of dialed calls and number of subscribers in conducting their regular business,[379] while in *American Civil Liberties Union v. Clapper* and *Klayman v. Obama*, there was evidence that a lot of people's private data were collected, including names, calls, messages, time of calls, and many other types of data.[380] The limitation of the amount of the data collected in *Katz vs. the United States* and *Smith v. Maryland* might justify the collecting of data for business needs. Still, it does not justify the massive amount of data being collected by telecommunication companies today. As a result, there is a difference in the amount of the data being collected between the old and new court cases, and this difference makes the old court cases insufficient as a precedent for the new court cases.

The seventh factor is related to the people use of the digital technology. In *Smith v. Maryland*, the court mentioned that people are giving their information voluntarily not coercively to the telephone companies. Back in *Smith v. Maryland*'s time, people used to send the papers through the U.S. Postal Service, students physically searched books and papers in the library, and patients used to give their information to the doctors in person. Today, people use the Internet and digital technology; most students search through a virtual library using digital devices, and patients send their information through emails. Theoretically, people still have the choice to use traditional means to finish their daily tasks; however, it is impractical for people to use these old-fashioned methods. For instance, is it reasonable for a student to ask his or her professor to send papers through the mail instead of email? Will this be a practical way to communicate between professors and students, especially in our digital era? The central problem in *Smith v. Maryland* is

[379] 442 U.S. 735.
[380] Davis, 3.

that people had no privacy expectations when they gave their information voluntarily. In *Smith v. Maryland's* time, people had old but familiar means to fulfill the requirements of individuals. Today, individuals have new ways to meet their requirements, such as digital technology tools, and they almost have no choice but to use these technologies. Therefore, in *Smith v. Maryland's* time, people gave their information voluntarily, not coercively, but today, people are almost giving their information indirectly coercively, not voluntarily. As a result, *Smith v. Maryland's* case might not be a good choice to use as a precedent for the new digital privacy issue cases.

A suggested recommendation introduced in this thesis after the investigation of three main parts is that Congress should pass a new law to control the sharing of people's private data by third parties with the government security agencies and to restrict the use of the new technology in sharing people's private data. Moreover, this thesis recommends new judicial interpretations of the Fourth Amendment.

Proposed Law—U.S. Digital Privacy Protection Act

From a personal standpoint, the term "digital privacy" could be defined as the ability of the individuals to decide when their private digital data can be shared, with whom their digital information can be shared, and how and why their digital data might be shared. Privacy is an essential part of our lives, especially in the Internet and digital technology era, when people rely on cyberspace and digital technology to accomplish their needs and tasks. Individuals might be skeptical at the same time when using the Internet and digital technology due to the lack of privacy trust. This is why privacy is essential for increasing the trust among people with regard to using the Internet and digital technology; individuals can take full advantage of both, especially in countries like the United States, where people are eager to do this to progress in various areas. Therefore, this thesis recommends a privacy law for the United States called "U.S. Digital Privacy Protection Act" (U.S. DPPA). The thesis offers a set of standards that come with this law

to ensure individuals' proper privacy protection. The standards are the following:

A. The Imposition of Privacy in the Design of Current and New Digital Devices

U.S. DPPA mandates a restriction on the design of current and new digital technologies, including limitations on collecting digital private data through the Internet and cloud storage. Also, U.S. DPPA requires controls on digital devices' design in terms of the way that these devices share digital private data unless people want to provide their private information voluntarily in exchange for some service.

B. Transparency Requirement

U.S. DPPA requires that telecommunication and digital media companies must create transparent, precise, and short user privacy policy agreements so people can easily understand their privacy rights. As a result, people could actually consent to the company's policies instead of hastily agreeing to the terms because of the long policy pages and arcane language used by the digital and telecommunication companies.

C. Observation of the Application of the U.S. DPPA

The U.S. DPPA ensures the monitoring of telecommunication and digital media companies in terms of whether they apply the law correctly or not. The U.S. DPPA forces telecommunication and digital media companies to apply the privacy law entirely and correctly by imposing sanctions on any company or business that does not apply the law as required.

D. Subscribers' Control Over their Private Data

The U.S. DPPA mandates telecommunication and digital media companies to give their subscribers complete access to control of their private digital data. Telecommunication and social media network subscribers should have the ability to remove, add, or share their private data without the need for permission from the companies that they subscribe to.

E. Mandates Liability

The U.S. DPPA requires telecommunication and digital media companies to be liable for

keeping their subscribers' data secure. If private data is shared by mistake, these companies are responsible for solving the problem as well as compensating their subscribers for the mistake.

F. Requires a Warrant from the Government Security Agencies

The U.S. DPPA law requires that government security agencies obtain a warrant from the court that endorses them to request a "limited" amount of data for suspects in terrorist or criminal action. Moreover, the warrant should be granted after providing clear evidence related to the person that the government security agency aims to obtain his private data.

Other Possible Laws

One of the possible solutions for lawmakers is to establish a law that could give the right to people to ask telecommunication and digital media companies to omit their data whenever they want. In this case, as much as the telecommunication and digital media companies collect private data, they cannot share them when deleted. Furthermore, lawmakers should specify the law to apply to the new types of data stored on the Internet so that judges may discern between the cases involving tangible and intangible private data.

The other law that lawmakers could provide is a law that forces the telecommunication and digital media companies to collect a limited amount of private data for their business purposes only. The type and the amount of people's private data should be defined precisely in the law so that no extra private data will be collected. Furthermore, telecommunication and digital media companies should ask for the subscribers' consent before sharing their private data with any entity and for any reason. At this point, a small amount of private data could be stored by the telecommunication and digital media companies, including names and phone numbers; people will be aware when their private data is shared.

Another law that could be successful in solving the privacy issue is one that requires the telecommunication and digital media companies to grant access to their cloud to their users. Each

user should be able to modify his or her cloud storage so that they can erase any unwanted, stored private data in their cloud. This solution might be attainable if the telecommunication and digital media companies use their technologists to allocate cloud storage for each user.

To summarize, many scholars focused their analysis regarding the data privacy problem on amending acts that are relevant to the privacy issue, such as the USA PATRIOT Act and the USA Freedom Act. Specifically, scholars try to amend or delete some sections in the PATRIOT Act and the USA Freedom Act in order to improve privacy protection. Other scholars analyze the impacts of the new digital devices on people's private data, for instance, how the new digital devices enable telecommunication and digital media companies to collect more private data, and how these private data could be shared with the government. Other scholars linked the problem of data privacy to the Third-Party Doctrine, and they explained that there is no privacy expectation when people give their data voluntarily to any third party such as telecommunication or digital media companies. However, this thesis took a different route than other scholars' analysis of the data privacy issue by investigating the history of the application of the Fourth Amendment and search and seizure process and analyzing four important court cases related to the privacy issue: *Katz v. United States*, *Smith v. Maryland*, *ACLU v. Clapper*, and *Klayman v. Obama*. The application of the Fourth Amendment and search and seizure process throughout history is considered a vital part of analyzing the privacy issue to see whether the Fourth Amendment is enough to solve the privacy issue or not, especially in the new types of privacy issues that relate to digital private data. Analysis of the four court cases aims to evaluate the use of old court cases as precedents in new court cases (such as the old cases *Katz v. United States*, *Smith v. Maryland* and the new court cases *ACLU v. Clapper* and *Klayman v. Obama*. Furthermore, the four court cases reveal the gaps in technology between the old and new court cases, the type of property being searched, the Internet, and the judges' decisions about the expectation of privacy. Lastly, third parties like telecommunications and digital media companies should be considered as the

heart of the problem: lawmakers should look at how to stop them from sharing private data with the government. Therefore, lawmakers in the United States should pass a new law to control third party sharing of people's private data. A law could stop third parties from handing people's private data to government security agencies like NSA and others.

Bibliography

Ahn, Jungmihn. “Issues Presented by Cybersecurity Information Sharing Act 2015.” *Yonsei Law Review* 28, no. 4 (2018): 259-282.

AlSudiary, Mohammed Ahmed Truki. "Perspectives of Managing Mobile Service Security Risks. *“International Journal of Distributed Sensor Networks* 311, no. 7 (2015): 592-634.

Allen, David. “The Gentleman's Agreement in Legal Theory and in Modern Practice.” *Anglo-Am. L. Review*. 29 (2000): 204-317.

Applegate, John and Amy Grossman. “Pen Registers after Smith v. Maryland.” *Harvard Civil Rights-Civil Liberties Law Review.* 15 (1980): 753-811.

Beauchamp, Christopher. “Who Invented the Telephone? Lawyers, Patents, and the Judgments of History.” *Technology and Culture* 51, no. 4 (2010): 854-878.

Bently. Lionel, Suthersanen Uma, and Paul Torremans. *Global Copyright: Three Hundred Years since the Statute of Anne, from 1709 to Cyberspace.* Cheltenham, UK, 2010.

Blayney, Peter. *The Stationers' Company and the Printers of London, 1501-1557.* Cambridge, U.K: Cambridge University Press, 2013.

Brodie, Carolyn S. “Always Inventing: A Photobiography of Alexander Graham Bell.” *School Library Media Activities Monthly* 21, no. 4 (2004): 48.

Burger, Jodie and Eddie Schuderi. “Unmanned & Unregulated: Where are the Privacy Protections from Drones?” *Law Society of NSW Journal* (2018): 46-88.

Burnham, Michelle, “Folded Selves: Colonial New England Writing in the World System.” *The New England Quarterly* 81, no. 1 (2008): 150-152.

Campos, Rafael Saraiva. “Evolution of Positioning Techniques in Cellular Networks, from 2G to 4G.” *Wireless Communications and Mobile Computing* 20, (2017): 1-17.

Castilhos, Karam and Francisco José. “Journalism in the Age of the Information Society, Technological Convergence, and Editorial Segmentation: Preliminary Observations.” *Journalism (London, England)* 10, no. 1 (2009): 109-125.

Charles II, King of England and England and Wales, Sovereign (1660-1685: Charles II), By the King, a Proclamation for the Better Discovery of Seditious Libelers, Vol. 1588:97.

Chemerinsky, Erwin. “Protecting Electronic Privacy.” *Judicature* 103 (2019): 76-96.

Chong, Jane. “Government Files Reply in Klayman v. Obama, ACLU Moves to Participate in Oral Argument.” *Lawfare: Hard National Security Choices* 8 (2013):119-148.

Clement, James. “Online Privacy.” *Statista*, Mar. 22, 2019, https://www.statista.com/topics/2476/online-privacy, accessed Jan 31, 2021.

Conforti, Michael. “John Wilkes, the Wilkite Movement and a Free Press in America.” *Journalism History* 43, no. 1 (2017): 32-43.

Connare, Erin E. “ACLU v. Clapper: The Fourth Amendment in the Digital Age.” *Buffalo Law Review.* 63 (2015): 395-405.

Coates IV, John C. "Corporate Speech & the First Amendment: History, Data, and Implications." *Constitutional Commentary* 30, no. 2 (2015): 223.
Cooke, Christopher. "Note: Securing Liberty: A Response to Debates on Section 215 of the Patriot Act." *Georgetown Journal of Law & Public Policy* 12 (2014): 889-912.
Cramer, Benjamin W. "A Proposal to Adopt Data Discrimination Rather than Privacy as the Justification for Rolling Back Data Surveillance." *Journal of Information Policy* 8 (2018): 5-33.
Crowell, Donald L. "The Privacy of 'Things': How the Stored Communications Act has been Outsmarted by Smart Technology." *Federal Communications Law Journal* 70, no. 2 (2018): 211-332.
Dalum, Bent, Christian R. Pedersen, and Gert Villumsen. "Technological Life-Cycles: Lessons from a Cluster Facing Disruption." *European Urban and Regional Studies* 12, no. 3 (2005): 229-246.
Dash, Samuel. *The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft*. New Brunswick, N.J: Rutgers University Press, 2004.
Davis, Stephen L. "Conflicting Court Decisions Leave Constitutional Privacy Protections Against Mass Data Collection Uncertain." *Journal of Internet Law* 17, no. 11 (2014): 3-15.
Davies, Thomas Y. "Correcting Search-and-Seizure History: Now-Forgotten Common-Law Warrantless Arrest Standards and the Original Understanding of 'Due Process of Law'." *Mississippi Law Journal* 77, no. 1 (2007): 1-224.
------. "Recovering the Original Fourth Amendment", *Michigan Law Review* 98 (1999): 119-137.
Deist, Christopher J. "Taking a Stand: Addressing the Issue of Article III Standing against the NSA Metadata Collection Program following Obama v. Klayman." *George Mason Law Review.* 24 (2016): 285.
Derman, Jeremy. "Constitutional Law-Maryland District Court Finds Government's Acquisition of Historical Cell Site Data Immune from Fourth Amendment-United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012)." *Suffolk University Law Review.* 46 (2013): 297-343.
Ditzion, Robert. "Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers." *American Criminal Law Review* 41, no. 3 (2004): 1321-1342.
Donohue, Laura K. "The Original Fourth Amendment." *University of Chicago Law Review* 83, No. 6 (2012): 213-223.
Electronic Privacy Information Center. The USA Patriot Act, www.epic.org/privacy/terrorism/usapatriot, retrieved Jan. 31, 2021.
Esteve, Asunción. "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA." *International Data Privacy Law* 7, no. 1 (2017): 36-47.
"The Evolution of Mobile Tech." *Advertising Age* 88, no. 5 (2017): 18.
Fagen, M.D., G. E. Schindler, Amos E. Joel, E. F. O'Neill, and Bell Telephone Laboratories. *A History of Engineering and Science in the Bell System*. New York: The Laboratories, 1975.

Finn, Bernard S., "Bell and Gray: Just a Coincidence?" *Technology and Culture.* Baltimore: Johns Hopkins University Press, 2009.
Fisher, Leonard Everett. *Alexander Graham Bell*. 1st ed. New York, N.Y: Atheneum Books for Young Readers, 1999.
Forouzan, Behrouz A. "Data Communications & Networking," *Microelectronics and Reliability* 45, no. 5-6 (2005): 1014-1016.
Forsyth, Bart. "Banning Bulk: Passage of the USA Freedom Act and Ending Bulk Collection." *Washington and Lee Law Review* 72, no. 3 (2015): 1307.
Frese, Joseph R. "James Otis and Writs of Assistance." *New England Quarterly* 30, no. 1 (1957): 496-508.
Galicki, Alexander. "The End of Smith v. Maryland: The NSA's Bulk Telephony Metadata Program and the Fourth Amendment in the Cyber Age." *American Criminal Law Review* 52 (2015): 375-424.
Garlinger, Patrick P. "Privacy, Free Speech, and the Patriot Act: First and Fourth Amendment Limits on National Security Letters." *New York University Law Review.* 84 (2009): 1105-1148.
Gawalt, Gerard W. *The Writs of Assistance Case*, Vol. 36 (The Institute of Early American History and Culture, 1979): 117-144.
Gentithes, Michael. "App Permissions and the Third-Party Doctrine." *Washburn Law Journal* 59 (2020): 35-52
Giles, Courtney. "Balancing the Breach: Data Privacy Laws in the Wake of the NSA Revelations." *Houston Journal of International Law* 37 (2015): 543-579.
Gorman, Michael E. and Kirby Robinson. "Using History to Teach Invention and Design: The Case of the Telephone." *Science Education* 7, no. 2 (1998): 173-201.
Gray, Charlotte. *Reluctant Genius: Alexander Graham Bell and the Passion for Invention*. 1st U.S. ed. New York: Arcade Pub, 2006.
Gubins, Tamar R. "Warshank v United States: The Katz for Electronic Communication." *Berkeley Technology Law Journal* 23 (2008): 723-745.
Hannay, Margaret P. "Censorship and Interpretation: The Conditions of Writing and Reading in Early Modern England." *Sidney Newsletter* 8, no. 1 (1987): 12-26.
Heidenreich, John. "The Privacy Issues Presented by the Cybersecurity Information Sharing Act." *North Dakota Law Review.* 91 (2015): 395-432.
Henderson, Stephen E. "Expectations of Privacy in Social Media." *Mississippi Law Journal.* 31 (2012): 227-248.
Herbert, Ari. "Changing Tack in the Night: The Supreme Court's Misapplication of Katz." *American Journal of Criminal Law* 44, no. 2 (2017): 253-259.
Herman, Arthur and John Yoo. "A Defense of Bulk Surveillance - The NSA Programs Enhance Security Without Uniquely Compromising Privacy." *The National Law Review* 8 (2012): 132-164.
Herman, Susan N. "The USA PATRIOT Act and the Submajoritarian Fourth Amendment." *Harvard Civil Rights-Civil Liberties Law Review* 41, no. 1 (2006): 67-132.
Homan, Madison. "Privacy Law." *Suffolk Transnet's Law Review* 41 (2018): 575.
Hounsell, D.A. "Bell and Gray: Contrasts in Style, Politics, and Etiquette." *Proceedings of the IEEE* 64, no. 9 (1976): 1305-1314.

"IEEE Global History Network." *IEEE Transactions on Microwave Theory and Techniques* 65, no. 7 (2017): 2646.
Irvine, Paul. "Gardiner Greene Hubbard (1822-1897)." *Journal of Special Education* 19, no. 4 (1985): 378-379.
Issacharoff, Lucas, and Kyle Wirsha. "Restoring Reason to the Third-Party Doctrine." *Minnesota Law Review.* 100 (2015): 985-1050.
Kerr, Orin S. "The Case for the Third-Party Doctrine." *Michigan Law Review* 107, no. 4 (2009): 561-601.
Kisekka, Victoria, Sharmistha Bagchi-Sen, and H. Raghav Rao. "Extent of Private Information Disclosure on Online Social Networks: An Exploration of Facebook Mobile Phone Users." *Computers in Human Behavior* 29, no. 6 (2013): 2722-2729.
Kugler, Matthew B. and Lior Jacob Strahilevitz "The Myth of Fourth Amendment Circularity," *The University of Chicago Law Review* 84, no. 4 (2017): 1747-1812.
LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*. Vol. 4. West Group Publishing, 2004.
Lee, Gwanhoo. "What Roles should the Government Play in Fostering the Advancement of the Internet of Things?" *Telecommunications Policy* 43, no. 5 (2019): 434-444.
Leithauser, Tom and John Curran. "Sen. Leahy Offers New USA Freedom Act Backed by Privacy Groups, White House." *Cybersecurity Policy Report* (2014).
Library of Congress. Congressional Research Service. USA Freedom Act Reinstates Expired USA PATRIOT Act Provisions but Limits Bulk Collection. Washington, *District of Columbia: Congressional Research Service*, 2015.
Lifshitz, Kenneth B. *Makers of the Telegraph: Samuel Morse, Ezra Cornell and Joseph Henry*. Jefferson, North Carolina: McFarland & Company, Inc., Publishers, 2017.
Louis, P. J. *Telecommunications Internetworking*. New York: McGraw-Hill, 2000.
Lungren, Daniel E. "A Congressional Perspective on the Patriot Act Extenders." *Notre Dame Journal of Law, Ethics & Public Policy* 26 (2012): 427-466.
Margulies, Peter. "Searching for Federal Judicial Power: Article III and the Foreign Intelligence Surveillance Court." *George Washington Law Review.* 85 (2017): 800-822.
Markland, Andreas. "Trawling the Wires: Mass Surveillance of Border-Crossing Communication in Denmark during World War II." *Technology and Culture* 60, no. 3 (2019): 770-794.
Mastracci, Joshua M. "Klayman v. Obama: The DC District Court Misinterprets the NSA Metadata Collection Program as a Violation of Individual Fourth Amendment Rights." *Tulane Journal of Technology and Intellectual Property.* 17 (2014): 365-374.
Matiteyahu, Taly. "Drone Regulations and Fourth Amendment Rights: The Interaction of State Drone Statutes and the Reasonable Expectation of Privacy." *Columbia Journal of Law and Social Problems.* 48 (2014): 265-278.

McDonough, Jennifer L. “Media Participation in the Execution of a Search Warrant Inside a Home Violates the Fourth Amendment to the United States Constitution.” *Duquesne Law Review* 38, no. 4 (2000): 1119-1142.
McGowan, Casey J. “The Relevance of Relevance: Section 215 of the USA PATRIOT Act and the NSA Metadata Collection Program.” *Fordham Law Review.* 82 (2013): 2399-2456.
McPherson, Susan. “Warrantless Arrest for Misdemeanor Traffic Violation Does Not Violate Fourth Amendment Protection Against Unreasonable Seizure.” *Cumberland Law Review* 32, no. 1 (2001): 265-285.
Meyerowitz, Steven A, “The Patriot Act.” *Banking Law Journal* 122, no. 2 (2005): 97-98.
Miller, Helen Hill. *The Case for Liberty*. Chapel Hill: University of North Carolina Press, 1965.
Mund, Brian. “Social Media Searches and the Reasonable Expectation of Privacy.” *Yale Journal of Law and Technology.* 19 (2017): 238-273.
Myers, Robin. *The Stationers' Company Archive: An Account of the Records, 1554-1984.* Winchester: St. Paul's Bibliographies (1990).
Myers, Robin and Michael Harris*, Censorship & the Control of Print: In England and France 1600-1910*. Winchester: St Paul's Bibliographies. 1992.
Ochoa, Tyler. “The Legacy of the Statute of Anne.” *Copyright & New Media Law Newsletter* 14, no. 1 (2010): 5.
Ormerod, Peter C. and Lawrence J. Trautman, “Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age.” *Albany Law Journal of Science & Technology* 28, no. 2 (2018): 73-149.
Pauley III, William H. “United States District Court Southern District of New York: American Civil Liberties Union v. James R. Clapper (13 Civ. 3994).” *American Civil Liberties Union* 18, no. 13 (2015): 3.
Pfeifle, Anne. “Alexa, What Should We Do about Privacy: Protecting Privacy for Users of Voice-Activated Devices.” *Washington Law Review.* 93 (2018): 421-58.
Porritt, Vernon L. *British Colonial Rule in Sarawak, 1946-1963*. New York; Oxford University Press, 1997.
Posadas Jr., Dalmacio V. “After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy.” *Fordham Intellectual Property Media & Entertainment Law Journal* 28 (2017): 69-98.
------. “The Internet of Things: Abandoning the Third-Party Doctrine and Protecting Data Encryption.” *Gonzaga Law Review.* 53 (2017): 8119.
Prentiss, Stan. *Introducing Cellular Communications: The New Mobile Telephone System*. 1st ed. Blue Ridge Summit, Pa: Tab Books, 1984.
Price, Michael W. “Rethinking Privacy: Fourth Amendment ‘Papers’ and the Third-Party Doctrine.” *Journal of National Security Law & Policy* 8, no. 2 (2016): 247-286.
Pugh, Sarah E. “Cloudy with a Chance of Abused Privacy Rights: Modifying Third-Party Fourth Amendment Standing Doctrine Post-Spokeo.” *American University Law Review.* 66 (2016): 971-984.

Ramachandran, G., R. Ramani, S. Selvaraju, B. Rajasekaran, and P. M. Murali. "Accident Finding and Location Identification System Using Google Map." *i-Manager's Journal on Electronics Engineering* 3, no. 3 (2013): 32-125.
Rapisarda, Mark. "Privacy, Technology, and Surveillance: NSA Bulk Collection and the End of the Smith v. Maryland Era." *Gonzaga Law Review.* 51 (2015): 121.
Rappaport, Theodore S., Brian D. Woerner, and Jeffrey Hugh Reed, *Wireless Personal Communications: The Evolution of Personal Communications Systems*. Boston: Kluwer Academic Publishers, 1996.
Reid, John Phillip. *The Writs of Assistance Case*, Vol. 84 (The American Historical Association, 1979).
Rubenfeld, Jed. "The End of Privacy." Stanford Law Review 61, no. 1 (2008): 101-161.
Rudé, George F. *Wilkes and Liberty: A Social Study of 1763 to 1774*. Oxford: Clarendon Press. 1962.
Sales, Nathan Alexander. "Mending Walls: Information Sharing After the USA PATRIOT Act." *Texas Law Review.* 88 (2009): 1795-1843.
Sariego, Jose M. "The Privacy Protection Act of 1980: Curbing Unrestricted Third-Party Searches in the Wake of Zurcher v. Stanford Daily." *University of Michigan Journal of Law Reform* 14 (1980): 519-562.
Schultz, Christian and David Hammel. "Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute." *The Notre Dame Law Review* 76, no. 4 (2001): 1215-1245.
Shifrin, Orrin S. "Fourth Amendment: Protection Against Unreasonable Search and Seizure: The Inadequacies of using an Anonymous Tip to Provide Reasonable Suspicion for an Investigatory Stop." *The Journal of Criminal Law & Criminology* 81, no. 4 (1991): 760-778.
Shoshana, Harry M. *Disconnecting Bell: The Impact of the AT&T Divestiture*. New York: Pergamon Press, 1984.
Siebert, Fred S. *The Rights and Privileges of the Press*. New York: D. Appleton-Century Company, Inc. 1934.
Singh, Niharika and Mandeep Singh Saini. "Performance Evaluation of Secure Asymmetric Key Exchange Mechanisms for 4G Networks." *International Journal of Computer Applications* 118, no. 23 (2015): 10-15.
Sketchler, Marc. "I Didn't Say That: The Ninth Circuit's Novel and Important Extension of Copyright Protection in Garcia v. Google, Inc." *Tulane Journal of Technology and Intellectual Property.* 17 (2014): 353-376.
Stern, Simon. "The Third-Party Doctrine and the Third Person." *New Criminal Law Review* 16, no. 3 (2013): 364-412.
Stoeckigt, Kewin O., and Hai L. Vu. "VoIP capacity—analysis, improvements, and limits in IEEE 802.11 wireless LAN." *IEEE Transactions on Vehicular Technology* 59, no. 9 (2010): 4553-4563.
Strossen, Nadine. "Why the American Civil Liberties Union Opposes Campus Hate Speech Codes." *Academic Questions* 10, no. 3 (1997): 33-40.
Takeuchi, Mary-Kathryn. "A New Third-Party Doctrine: The Telephone Metadata Program and Carpenter v. United States." *Notre Dame Law Review* 94 (2018): 2243-2265.

Taslitz, Andrew E. *Reconstructing the Fourth Amendment: A History of Search and Seizure, 1789-1868*. New York: New York University Press, 2006.
Thompson, Richard M. "The Fourth Amendment Third-Party Doctrine." Congressional Research Service, https://fas.org/sgp/crs/misc/R43586.pdf, retrieved Jan. 31, 2021.
Tudor, William, *The Life of James Otis, of Massachusetts: Containing also Notices of Some Contemporary Characters and Events, from the Year 1760 to 1775*. Boston: Wells and Lilly, 1823.
Tzanou, Maria. "Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures." *Journal of Internet Law* 17, no. 3 (2013): 20-33.
United States. Congress. House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security and United States. Congress. House. Committee on the Judiciary. Subcommittee on Crime, Terrorism, and Homeland Security. *Legislative Proposals to Update the Foreign Intelligence Surveillance Act (FISA): Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives, One Hundred Ninth Congress, Second Session, September 6, 2006*. Washington: U.S. G.P.O, 2006.
United States. Congress. House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security. Reauthorization of the PATRIOT Act: Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives, One Hundred Twelfth Congress, First Session, March 9, 2011. Washington: U.S. G.P.O, 2011.
Van Cleef, Carol R. "The USA PATRIOT Act: Statutory Analysis and Regulatory Implementation." *Journal of Financial Crime* 11, no. 1 (2004): 73-102.
Vedaschi, Arianna. "Privacy and Data Protection Versus National Security in Transnational Flights: the EU–Canada PNR Agreement." *International Data Privacy Law* 8, no. 2 (2018): 124-139.
Walsh, Patrick. "Foreign Intelligence, Criminal Prosecutions, and Special Advocates." *U. Memphis Law Review* 47 (2016): 1011.
Watson, Richard. *Fixed/Mobile Convergence and Beyond: Unbounded Mobile Communications*. Amsterdam; Newness/Elsevier, 2009.
Weiser, Philip J. "Institutional Design, Fcc Reform, and the Hidden Side of the Administrative State." *Administrative Law Review* 61, no. 4 (2009): 675-721.
Welch, Kyle. "The Patriot Act and Crisis Legislation: The Unintended Consequences of Disaster Lawmaking." *Capital University Law Review*. 43 (2015): 481-554.
Whitaker, Beth Elise. "Exporting the Patriot Act? Democracy and the 'War on Terror' in the Third World." *Third World Quarterly* 28, no. 5 (2007): 1017-1032.
Whittaker, Zack. "NSA Says Warrantless Searches of Americans' Data Rose in 2018." *TechCrunch*, Apr. 30, 2019, https://techcrunch.com/2019/04/30/nsa-surveillance-spike/, accessed Feb. 26, 2021.
Wimberly, Mary Helen. "Rethinking the Substantive Due Process Right to Privacy: Grounding Privacy in the Fourth Amendment." *Vanderbilt Law Review* 60, no. 1 (2007): 283-312.

Young, Mark D. “National Insecurity: The Impacts of Illegal Disclosures of Classified Information.” *A Journal of Law and Policy for the Information Society* 10 (2014): 367-384.
Zansberg, Steven D., and Janna K. Fischer. “Privacy Expectations in Online Social Media-an Emerging Generational Divide.” *Communications Lawyer.* 28 (2011): 1-24.

Court Cases

ACLU v. Clapper*,* 785 F.3d 787, (2015) U.S. Section 215 (50 U.S.C.S. § 1861).
Katz v. United States, 389 U.S. 347 (U.S. Supreme Court, 1967).
Klayman v. Obama, 957 F. Supp. 2d 1 (D.C.D.C. 2013).
Smith v. Maryland 442 U.S. 735 (1979).
The Telephone Cases, 126 U.S. 1 (1888).