Data Collection, Privacy Rights, and Public Safety in the United States: An Unresolved Issue in a Growing Technological World

Traci Brady, DBA (Email: traci.brady@salve.edu) Salve Regina University, USA
Michael T. Brady, JD (Email: michael.brady@salve.edu) Salve Regina University, USA

Data Collection, Privacy Rights and Public Safety in the United States: An Unresolved Issue in a Growing Technological World

Traci Brady, DBA (Email: traci.brady@salve.edu) Salve Regina University
Michael T. Brady, JD (Email: michael.brady@salve.edu) Salve Regina University

Abstract

This paper explores data privacy and corporate responsibility in an era of active and passive data collection by a variety of electronic devices. As the proliferation of devices continues, and the Internet of Things (IoT) broadens, this issue will continue to surface. The conversation about personal, corporate, and social responsibility as it relates to access of data by law enforcement that may provide information about criminal activity is continuing. At the core of this conversation is consideration of a "reasonable expectation of privacy."

Introduction

Personal data is collected at an incredible rate by an ever-growing number of electronic devices. Consumers are trading their personal data for the sake of convenience or social interaction. These data collection devices are so pervasive, one wonders just how aware the general public is about data collected by these devices and how concerned they are about the use of their private data.

Personal computing devices like cell phones, smartphones, tablets and laptops capture personal data via voice, text, email, video, photo and application. These devices are not the only way data is collected about individuals. Surveillance cameras, traffic cameras, point of purchase systems, loyalty cards, and GPS locators in vehicles are just a few of the other ways data are being collected about people's movements, purchases, and routines. The growing Internet of Things (IoT) provides additional devices for capturing private data about consumers. Household thermostats, refrigerators, lights, and televisions may be electronically controlled. Televisions may "learn" user preferences; refrigerators know if you need butter; and vehicles know that you typically drive home around 9:45pm on Tuesday nights. Your bank card knows how often you go to the ATM, where you are most likely to make your purchases, and where you went on vacation last March. Voice-activated devices like the Amazon Echo are always "listening" for the launch word, and consumers may not realize the incredible impact these devices, and others, have on data collection. Interestingly, it is not just the collection of the data that is concerning to some, but the storage of that data, access, and potential use of it.

Companies use data collected through their own devices to narrow their marketing efforts to those who most resemble targeted consumers or, in some cases, sell the data to other commercial enterprises looking for new customers. The terms of this data use are typically defined in a corporate privacy policy provided to consumers at various touchpoints. Most websites will provide home page links to privacy policies, and require consumer consent regarding use and resale of customer data during initial interactions. Many of these privacy policies are drafted by lawyers in language used to protect the company, and may be difficult for the average consumer to truly understand. Nonetheless, the policies exist and consumers are given the option to consent, or not, to the collection and use of their data.

Law enforcement has also emerged as a potential user of stored data collected through technological devices as evidence in criminal investigations. Although the data was certainly not collected or intended for this purpose, technological devices are actively, and sometimes passively collecting data about users. Law enforcement investigating potential criminal activity may seek access to these devices as part of an investigation. Since many of the devices are password protected, owners hold the key to unlock the device. In some cases where owners are

unable or unwilling to turn over the password, law enforcement has turned to the technology companies to request access. What responsibility do technology companies have to provide access to customer data?

Recent notable cases include a request by a Federal judge to Apple to unlock the phone of terror suspect Syed Farook, charged in the San Bernardino shootings in December 2015. In 2016, Bentonville, Arkansas police issued a warrant to Amazon for records from James Bates' Echo device for information that may be related to a murder case. In both cases, Apple and Amazon refused to release their customer's data to law enforcement.

This paper explores data privacy and corporate responsibility in an era of active and passive data collection by a variety of electronic devices. As the proliferation of devices continues, and the Internet of Things (IoT) broadens, this issue will likely continue to surface. The conversation about personal, corporate, and social responsibility as it relates to access of data that may provide important information about criminal activity continues. At the core of this conversation is consideration of a "reasonable expectation of privacy" and the growing number of electronic devices that collect and store data.

Proliferation of Technology

Anderson (2016) reports that 68% of U.S. adults own a smartphone. These devices that continue to increase in popularity are used for more and more applications every day. Many smartphone users are accessing their bank information, applying for jobs, paying their bills, posting to social media, tracking fitness goals, and conversing with others using smartphones.

The Consumer Technology Association (CTA) reported on technology growth year over year from 2016 to 2017 in their press release, "*2017 Tech Growth Exceeds Expectations: Industry Revenue to Reach Record Levels as Emerging Categories Soar, Says CTA*." According to the CTA press release (2017), sales of voice-controlled digital assistants, like Amazon's Echo or Google's Home, are expected to increase 53% in 2017. Sales of home automation technology, such as smart thermostats and IP/Wifi cameras, are expected to increase 50% in 2017; and the wearable category, like fitness trackers and smart watches, is expected to see a 9% increase in sales. Interest in and adoption of connected technology including smart appliances, smart televisions, wearables, digital assistants, and more continue to increase.

IHS forecasts that the Internet of Things (IoT) will grow from 15.4 billion devices in 2015 to 30.7 billion in 2020 and 75.4 billion in 2025 (Columbus, 2016). Thirty-four billion devices are expected to be connected to the Internet by 2020, comprised of twenty-four billion IoT devices and ten billion traditional computing devices (Camhi, 2015).

These devices are not the only way data are collected about the population. Surveillance cameras, traffic cameras, point of purchase systems, loyalty cards, and GPS locators in vehicles are just a few of the other ways data are being collected about people's movements, purchases, and routines. "Spyware and tracking cookies collect data about your search history, your age, location, interests, friends, items you liked but didn't purchase, and the amount of time you spend on a website." (CNN, 2014)

Data Collection and Privacy

How concerned are Americans about their privacy? Rainie (2016) reports that 74% of respondents felt it was very important to be in control of who can access their information; while 65% felt it was very important to control the information collected about them. Even with this concern about privacy and data collection, Rainie (2016) writes that "Americans still struggle with the nature and scope of data collected about them." The author goes on to report that "86% of Internet users have taken steps online to remove or mask their digital footprints." However, 61% say they felt they would like to take additional steps to protect their online privacy. Many are concerned that they don't fully understand how to best protect their online privacy.

According to Anderson (2016), a Pew Research poll found that 91% of Americans agree that "consumers have lost control of how personal information is collected and used by companies." A Pew Research Privacy Panel Survey in January 2014 found that 71% of U.S. adults surveyed were somewhat or very concerned about government accessing personal information users share on social media without their knowledge. 80% were concerned about third-party advertisers or businesses accessing information from their social media posts without their knowledge (Few Feel that the Government and Advertisers Can Be Trusted, 2014).

We live in a world where data are collected constantly, passively, without our knowledge. Davis (2016) reported from the Allstate/National Journal Heartland Monitor Poll that 53% of those surveyed felt that collection and use of data violated personal privacy and individual freedoms. Baby Boomers were most concerned (61%), the Silent/Greatest Generation were least concerned (42%), and Millennials and Generation X fell in the middle (50%). Fortune (Elmer-DeWitt, 2016) reported on a Reuters/Ipsos poll where 46% of respondents agreed that the government should be able to look at data on Americans' smart phones in order to protect against terror threats. Forty-two percent (42%) disagreed.

Government and businesses benefit from data collection and usage, as do consumers. Government uses this data to enhance public safety. Businesses use the data to narrowly direct their marketing efforts to those who may be most interested, reducing clutter and marketing costs that can translate into better efficiencies and lower prices for consumers.

The issue of how businesses and government use the data collected and for what purpose arises. How far should companies go to protect consumer privacy? What is the tradeoff between privacy and public safety? When should government be given access to private data without individual consent? What is a reasonable expectation of privacy, and to what devices does it extend?

Reasonable Expectation of Privacy

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized."*
>
> **-4th Amendment to the Constitution of the United States**

In order to appreciate what is at stake in the legal battle between the right to privacy and the right to know, we must first understand what has been recognized as a Constitutional "Right to Privacy." So what exactly is this "Right to Privacy" as far as the courts are concerned? Like many answers in criminal procedure, the answer to this legal question is, "It depends."

The Bill of Rights enumerates certain specific rights of the people and restrictions on the government familiar to many of us. Language specifically referencing the protections of Freedom of Speech, Freedom of Religion, Freedom of the Press, the Right to Keep and Bear Arms, the Right to Remain Silent in Criminal prosecutions, our Right to Counsel and many more fundamental rights are expressly mentioned in the Bill of Rights. An examination of the Constitution would reveal that there is no "Right to Privacy" found anywhere in the Constitution. So where did our right to privacy originate? The answer is that the Right to Privacy has developed over time, primarily focusing on the question of whether or not the government has violated the provisions of the Fourth Amendment when conducting criminal investigations.

Within case law, the earliest reference to the concept of privacy as we know it today is found in the dissent in the case of *Olmstead v. United States*, 277 U.S. 438 (1928).

Olmstead was tried and convicted in the Prohibition era of violations of laws for possessing, transporting and selling bootleg liquor. The basis of the information gathered and used by the prosecution against Olmstead at trial was gathered by government agents who placed wiretap devices on telephone wires outside of Olmstead's homes and buildings. In a 5 to 4 opinion, the U.S. Supreme Court upheld Olmstead's conviction, opining that the information gathered by the government agents which lead to Olmstead's conviction were not searches under the 4th

Amendment, because the government agents did not physically enter upon Olmstead's property. This holding became known as the Trespass Doctrine. The Trespass Doctrine would be the sole standard used in search and seizure analysis until 1967. Contained within the dissent in *Olmstead* was important language penned by then Justice Louis Brandeis. Brandeis argued that the intent of the founding fathers was to secure rights for the people and to permit the people, "as against the Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men." *Olmstead v. United States*, 277 U.S. 438, 478 (1928). This opinion by Justice Brandeis is credited with bringing the right to privacy to legal life.

The Court seized the opportunity to structurally develop the concept of privacy in the case of *Griswold v. Connecticut*, 381 U.S. 479 (1965). The *Griswold* case involved the issue of providing birth control contraceptive devices and information to individuals, including married individuals, in violation of Connecticut law. Utilizing the provisions of several Amendments to the Constitution of the United States, the Court held that, "[T]he present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees." *Griswold* at 485. In other words, the Court recognized that while the Constitution does not specifically reference a right to privacy as a Constitutional guarantee, nevertheless, the right to privacy is a fundamental right found within the penumbra of other Constitutionally enumerated rights as contained within the 1st, 3rd, 4th, 5th, 9th and 14th Amendments to the United States Constitution.

In 1967, the United States Supreme Court again had the chance to address the concept of privacy in a context similar to the *Olmstead* case, but using different technological tools, to gather information in a criminal investigation.

The FBI suspected that Charles Katz was involved in illegal gambling. Surveillance conducted by the FBI revealed that Katz would regularly leave his apartment and walk down to the street corner, where he was observed to use a telephone booth to place telephone calls. Agents suspected that Katz was using these public telephones to place his illegal bets. In order to gather evidence against Katz, agents placed a listening device on the roof of the telephone booth where they were able to record Katz talking on the telephone within the telephone booth. Based on the information obtained through this listening device, the FBI obtained a search warrant and seized information from Katz's apartment which lead to his conviction for illegal gambling. The matter of *Katz v. United States*, 389 U.S. 347 (1967) became the next impactful case on the development of the issue of the right to privacy.

Reasoning that the agents did not trespass upon the interior of the telephone booth to gather the information which lead to the conviction of Katz, the government urged to the U.S. Supreme Court that the conviction of Katz should stand. Counsel for Katz argued that the Court should reverse the conviction of Katz and to hold that the telephone booth was a Constitutionally protected "place" and that the FBI agents violated the right to privacy of Katz by placing the listening device on the outside of the top of the telephone booth. Writing for the Court, Justice Potter Stewart and the majority of the Court held that "[T]he Fourth Amendment protects people, not places." *Katz*, at 351, and reversed the conviction of Katz.

The concurring opinion of Justice John Harlan in the *Katz* case set forth a two prong test when analyzing whether or not a reasonable expectation of privacy exists in a particular case. The first prong of the test is a subjective test; whether the person in question exhibited by their actions or conduct an actual (individual) expectation of privacy. The second prong of the test, an objective test, asks that even if the person exhibited a subjective expectation of privacy, is that subjective expectation of privacy one that society is prepared to recognize as being reasonable. *Katz* at 361.

So how has this reasonable expectation of privacy developed since the *Katz* decision? In 1971, the Court held no violation of a right to privacy where a police informant was wearing a "wire" and transmitted conversations with a criminal via that "wire" to an agent listening nearby (*U.S. v. White*, 401 U.S. 745 (1971)); that no expectation of privacy existed in documents voluntarily given to a bank, such as deposit slips *(U.S. v. Miller*, 425 U.S. 435 (1976)); that there is no reasonable expectation of privacy in telephone numbers dialed from a home telephone (*Smith v. Maryland*, 442 U.S. 745 (1979)); that no reasonable expectation of privacy exists in trash left out on the sidewalk for collection (*California v. Greenwood*, 486 U.S. 35 (1988)); that a reasonable expectation of privacy does exist in heat emanating from the home of a person growing marijuana, where the police measured the heat signature of the home using a thermal imaging device from a public street without a warrant (*Kyllo v. United States*, 533 U.S. 27 (2001)); where the government placed a GPS tracking device on an automobile belonging to a suspected drug dealer without a warrant, the government therefore conducted a warrantless search of the automobile within the meaning of the

Fourth Amendment and therefore in violation of his expectation of privacy under the 4th Amendment (*U.S. v. Jones*, 565 U.S. 400 (2012)). This is a small cross section of the cases decided to date involving an individual's right to privacy.

Technology appears to now be at the forefront of many 4th Amendment cases. In 2010, the Sixth Circuit Court of Appeals held that an individual has a reasonable expectation of privacy in the content of email messages (*U.S. v. Warshak*, 631 F.3d 266 (2010); a Rhode Island Superior Court judge ruled that a suspect had an expectation of privacy in the text messages on his cellphone (*State v. Patino*, C.A. NO.: P1-10-1155A (2012). On appeal, the RI Supreme Court upheld in part and reversed in part some of the lower court decision in *Patino*. Of particular note, the RI Supreme Court held that while the defendant had an expectation of privacy of text messages on *his* telephone, he had no expectation of privacy in his text messages on the *recipient's* telephone (*State v. Patino*, No. 2012 – 263 C.A. RI Supreme Court (2014). The matter of *Carpenter v. United States*, U.S. Supreme Court Docket 16-402 is currently pending before the U.S. Supreme Court and is scheduled to be argued during the 2017-2018 term. The issue in this case is whether the warrantless search and seizure of a cellphone user's past location and movement information without a warrant is a violation of his right to privacy under the Fourth Amendment.

So where does the issue of privacy go from here, in a constantly changing and evolving technological world? The answer is, at best, uncertain. Do we get the same result in a *Miller* type of a case where the banking deposit is done, not in person, but on a personal device? How does the use of drones shrink or redefine concepts of privacy in and around our homes when the drone is used by a private individual? By a government agency? Does the proliferation of government use of cameras for security and traffic control further shrink our right to be left alone? Does the almost forced need for us to use technology equate to us relinquishing by our own consent some of our rights of privacy?

A more concise question to ask may very well be that question posed by the late Justice Antonin Scalia, writing for the majority in *Kyllo* when he wrote, "[T]he question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Id.* at 29. To date, that question remains unanswered and arguably, less certain.

Public Safety

Law enforcement recognizes the value of data stored in various electronic devices. Some devices, such as a public cameras, are often used as evidence in criminal investigations. Some law enforcement agencies have confiscated locked devices (such as smartphones, tablets, and laptops) that they believe contain information critical to an investigation. These devices may hold information that law enforcement believes could be valuable in the investigation of a crime. This information may include data stored as text messages, emails, data collected by applications (apps), social media activity, website browsing history, search history, GPS data, photos, calendar entries, and more. Currently, law enforcement depends on the device owner to provide passwords to access the necessary information. In the case where the device owner is unable or unwilling to provide the password, some law enforcement agencies have requested access from the technology companies storing the data. Once such example of that is the FBI vs Apple case.

During the investigation of terror suspect Syed Farook during the San Bernardino shootings in December 2015, federal law enforcement confiscated the suspect's iPhone. Unable to gain access to the phone without the user's password, the FBI requested that Apple provide "reasonable technical assistance" to the FBI in order to gain access to the phone's content. Apple refused.

"At the time, Apple chief executive Tim Cook called the order "chilling" and said that it would require writing new software that would be 'a master key, capable of opening hundreds of millions of locks.' Cook's argument was that if the FBI could access this iPhone, nothing would stop them from doing it to many others. Law enforcement authorities insisted that it was a one-off request. As a result the case went to court." (Kharpal, 2016) Tim Cook wrote the following in *A Message to Our Customers* (February 16, 2016), "The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of

privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge."

The case against Apple was dropped when the FBI found a third-party company, Cellebrite, to create the software to access Farook's phone. The issue of corporate responsibility in providing access to consumer's private data to law enforcement for the purposes of public safety remains unresolved.

A 2016 Pew Research study found that 51% of U.S. adults felt that Apple should have assisted federal authorities in unlocking Farook's phone; while 38% felt that Apple should not have unlocked the phone because it jeopardizes users' security and privacy (Anderson, 2016). All research on the topic, however, did not concur at the time. Fortune reported results from four additional surveys collected online. As reported in Fortune, a 2016 MarketWatch survey found 60% of respondents supported Apple's decision to protect consumer privacy; while 36% felt Apple should comply with the court order (Elmer-DeWitt, 2016). An online study by 9to5Mac in 2016 found 86% of respondents supported Apple's position; and 11% felt Apple should have complied with the court order (Elmer-DeWitt, 2016). Fortune's online study of 4,224 respondents found 71% supported Apple; and 22% who felt Apple should have complied with the court order. In addition, Fortune reported on the findings from a Reuters/Ipsos poll which found that 46% of respondents agreed with Apple's decision to oppose the court order; while 35% disagreed (Elmer-DeWitt, 2016).

Research also suggests that media coverage of national security concerns, such as the San Bernardino case, impacts how consumers feel and that those feelings begin to change as time separates us from the media coverage. Not surprisingly, more individuals are likely to support national security initiatives (such as accessing private data without consent) immediately following a national security event. The public's willingness to allow federal authorities to access private data for the sake of public safety declines as time separates us from the national security event (Tibken, 2017).

What are the legal and social responsibilities of corporations to provide password protected data in the name of public safety and security? Corporations are stuck between protecting the privacy rights of their customers and doing what is best for public safety. Corporations must consider the impact of releasing password-protected data on consumer trust in the company, and consumer's likelihood of remaining loyal to the company. If Apple had complied with the FBI's request, would consumers fear the loss of their own privacy with Apple's products and move their allegiance to another brand? On the other hand, would Apple's compliance have won the favor of more consumers who would have praised Apple for assisting federal authorities and improving public safety? Fortune (Elmer-DeWitt 2016) reported on the findings of a Piper Jaffrey poll which asked, "How do you view Apple in light of its refusal to help the FBI?" Twenty-four (24) percent felt more favorably, 23% felt less favorably, and 17.8% felt the same (35.5% knew nothing about it).

The corporate financial impact is certainly a consideration, but the companies may not have a choice in the matter if Federal courts rule that there is no reasonable expectation of privacy when electronic devices capture personal data. It also appears that the question of reasonable expectation of privacy may be device dependent, and that the courts would need to consider the question for every different device developed over time. As of now the issue remains unresolved.

Conclusion

The conversation about privacy rights and public safety continues. The opportunity to resolve the issue in the Apple VS FBI case was lost with the third-party solution for access to Farook's iPhone. Although not resolved, the situation continues to linger while technology continues to grow and gather even greater volume of data. Privacy advocates fear we have opted into social activity and convenience at the expense of our privacy. Others support access to private data in support of public safety. Not surprisingly, research has shown that the pendulum swings more toward public safety following a national security event, and then gently returns toward right to privacy as we are separated from the event.

Consumers should be aware of the data gathered by the electronic devices they buy and use, and how the data could possibly be utilized. Consumers can only protect their privacy if they know how and when their data are collected,

and are vigilant about reading and understanding privacy policies before agreeing to them. Consumers should make a conscious choice when providing access to their data, often at the expense of convenience. They must also understand that technology companies cannot guarantee protection of their private data from government agencies holding a subpoena. No privacy policy can guarantee that protection.

Technology companies remain torn between protecting the privacy rights of their consumers and supporting public safety efforts. On one hand, releasing consumer data may violate the trust consumers have with the company which could impact corporate revenue. On the other hand, the general public may support the release of the data that aids in public safety, especially in the case of national security. Although technology companies are bound by their own privacy policies with consumers, federal authorities are not party to the privacy policy and may subpoena information critical in an investigation. As of now, most technology companies have opted to do all they can to protect their customers' privacy.

The core of this issue lies with determining the "reasonable expectation of privacy" with the growing list of technology devices that capture personal data daily. Not until this issue has been heard and resolved will a better understanding of corporate social (and legal) responsibility be addressed.

Ultimately, the conflict between a right to privacy and a government agency's right to know will be resolved by both the legislature as well as the courts. The legislature will need to carefully draft and implement new laws to address the impact technology has on privacy. The courts will need to determine how to strike a balance between a perceived right to privacy and the government's need to know on a case by case basis.

References

2017 Tech Growth Exceeds Expectations: Industry Revenue to Reach Record Levels as Emerging Categories Soar. (2017, July 19). Retrieved September 10, 2017, from https://www.cta.tech/News/Press-Releases/2017/July/2017-Tech-Growth-Exceeds-Expectations-Industry-Re.aspx.

Anderson, M. (2016, March 10). 8 conversations shaping technology. Retrieved September 4, 2017, from http://www.pewresearch.org/fact-tank/2016/03/10/8-conversations-shaping-technology/.

California v. Greenwood, 486 United States Reports 35 (1988).

Camhi, J. (2015, November 06). BI Intelligence projects 34 billion devices will be connected by 2020. Retrieved September 4, 2017, from http://www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11.

Carpenter v. United States, 16-402 U.S. Supreme Court Docket (2016).

Cohen, J. R. (2016, March 21). Your iPhone and J. Edgar Hoover. Retrieved September 4, 2017, from http://www.huffingtonpost.com/j-richard-cohen/your-iphone-and-jedgar-ho_b_9518334.html.

Columbus, L. (2016, November 27). Roundup of Internet Of Things Forecasts And Market Estimates, 2016. Retrieved September 4, 2017, from https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#3b78316b292d.

Cook, T. (2016, February 16). Customer Letter. Retrieved September 4, 2017, from https://www.apple.com/customer-letter/.

Davis, L. C. (2016, February 03). How Do Americans Weigh Privacy Versus National Security? Retrieved September 4, 2017, from https://www.theatlantic.com/technology/archive/2016/02/heartland-monitor-privacy-security/459657/.

Elmer-DeWitt, P. (2016, February 24). Apple vs. FBI: What the Polls Are Saying. Retrieved September 4, 2017, from http://fortune.com/2016/02/23/apple-fbi-poll-pew/

Griswold v. Connecticut, 381 United States Reports 479 (1965).

Katz v. United States, 389 United States Reports 347 (1967).

Kharpal, A. (2016, March 29). Apple vs FBI: All you need to know. Retrieved September 4, 2017, from https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html.

Kyllo v. United States, 533 United States Reports 27 (2001).

Madden, M. (2014, November 12). Few Feel that the Government or Advertisers can be Trusted. Retrieved September 4, 2017, from http://www.pewinternet.org/2014/11/12/few-feel-that-the-government-or-advertisers-can-be-trusted/.

Maniam, S. (2016, February 22). More Support for Justice Department than for Apple in Dispute Over Unlocking iPhone. Retrieved September 4, 2017, from http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/.

Olmstead v. United States, 277 United States Reports 438 (1928).

Rainie, L. (2016, September 21). The state of privacy in post-Snowden America. Retrieved September 4, 2017, from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

Rainie, L., & Maniam, S. (2016, February 19). Americans feel the tensions between privacy and security concerns. Retrieved September 4, 2017, from http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/.

(Ret.), A. J., & Weinstein, D. (2016, March 08). Apple vs. FBI Is Not About Privacy vs. Security -- It's About How to Achieve Both. Retrieved September 4, 2017, from http://www.huffingtonpost.com/admiral-jim-stavridis-ret/apple-fbi-privacy-security_b_9404314.html.

Smith v. Maryland, 442 United States Reports 745 (1979).

State v. Patino, C.A. NO.: P1-10-1155A (Rhode Island Superior Court 2012).

State v. Patino, No. 2012 – 263 C.A (Rhode Island Supreme Court 2014).

Tibken, S. (2017, February 15). Apple's battle with the FBI leaves lingering questions. Retrieved September 4, 2017, from https://www.cnet.com/news/apple-vs-fbi-one-year-later-still-stuck-in-limbo/.

U.S. v. Jones, 565 United States Reports 400 (2012).

U.S. v. Miller, 425 United States Reports 435 (1976).

U.S. v. Warshak , 631 Federal Reporter 3rd Edition 266 (6th Circuit Court of Appeals 2010).

U.S. v. White, 401 United States Reports 745 (1971).

Zaru, D. (2015, April 30). Dilemmas of the Internet age: privacy vs. security – CNN Politics. Retrieved September 4, 2017, from http://www.cnn.com/2015/02/04/politics/deena-zaru-internet-privacy-security-al-franken/.