5-2017

CIA or CEO: Who Will be Responsible for Helping Protect National Security?

Jamie Elizabeth Crandal
Utah State University

CIA OR CEO: WHO WILL BE RESPONSILBLE FOR HELPING PROTECT NATIONAL SECURITY?

by

Jamie Elizabeth Crandal

Thesis submitted in partial fulfillment of the requirements for the degree

of

HONORS IN UNIVERSITY STUDIES WITH DEPARTMENTAL HONORS

in

International Business in the Department of Management

Approved:

Thesis/Project Advisor Dr. Shannon Peterson	**Committee Member** Professor John Ferguson
Honors Program Director Dr. Kristine Miller	**Departmental Honors Advisor** Dr. Shannon Peterson

UTAH STATE UNIVERSITY
Logan, UT

Spring 2017

ABSTRACT

As technology advances businesses are being called upon to take an active role in helping protect national security. A variety of different companies and industries within the private sector, which are at the forefront of encryption and hacking technologies, have the option to aid or subvert the intelligence community by sharing breakthrough technology in the interest of helping ensure domestic tranquility.

Many industries and companies within the private sector argue that while they are not actively trying to subvert efforts to protect national security it is not in their best interest, or the best interest of their customers, to hand over proprietary technology to the intelligence community through government enforcement of a court order. As a result of the intelligence community's need for assistance from the private sector and the private sectors refusal to provide aid, both parties have turned to the courts for adjudication of the issue.

The ensuing legal battle over this question of who is responsible for protecting national security will forever change the relationship between the private sector and intelligence. Has the nature of national security been fundamentally changed as the result of technology and our information society? More specifically, is the intelligence community and other governmental agencies solely responsible for protecting national security? Or, in an age of globalization, has national security become the burden of both public and private actors?

The answers to these questions are complex and at the same time straightforward. What was discovered was that while the burden of national security falls to both the public and private sector to an extent. However, it is not the responsibility of the private sector to help protect national security by virtue of providing the intelligence community with proprietary technology or information that could compromise the integrity of a given companies business. Furthermore,

the fight to protect national security is important, living in a country that provides certain safety assurances helps businesses grow; but when providing that safety prevents people from living their lives or businesses from operating at their full potential the enemy that the intelligence community is trying to protect us from has already won.

In developing the answers to these questions, this paper takes a broad view of the players involved as well as both sides of the legal battle that has already begun. will end with a discussion of the options and opportunities that will be available to both parties as the battle over who should be responsible for helping protect our national security moves forward in the courts.

For my parents,
this would not be possible without you!

ACKNOWLEDGEMENTS

Dr. Shannon Peterson- I would first like to acknowledge Dr. Shannon Peterson, who is my thesis project advisor. I met Dr. Peterson on my first trip to visit Utah State University. Having the opportunity to work with her over the last four years has been an incredible privilege. I would like to thank Dr. Peterson for her continued support, guidance, and mentorship. This project would not be possible without her encouragement.

Professor John Ferguson- I would also like to thank Prof. John Ferguson, for being the only other member on my thesis committee. Like Dr. Peterson, Prof. Ferguson has been an incredible mentor to me over these last four years. His involvement in the project, is very much appreciated.

I would not be where I am today; or the person I am today without the support, guidance, mentorship, friendship, and encouragement of you both. I will never forget the impact that you have had on my life.

THANK YOU!

TABLE OF CONTENTS

INTRODUCTION

On December 2, 2015 fourteen people were killed and twenty-two people were injured when Syed Rizwan Farook and Tashfeen Malik opened fire at a holiday party in San Bernardino California.[1] Farook and Malik were killed in a battle with police following the attack, however, during the subsequent investigation it became necessary for law enforcement officials from the FBI to obtain a search warrant that resulted in the discovery of an Apple iPhone belonging to Farook.

That cellphone was locked, the FBI did not have the password, and it did not have the ability or the technology to unlock the phone. As a result, the FBI sought the assistance of Apple. Apple uses a high-level encryption software that makes it "near[ly] impossible for the FBI or Apple or anyone else (except the phone owner) to crack the password."[2] Apple claims that it uses this level of encryption to protect the privacy of its customers. A statement from Apple reads, "For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe… We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business."[3] What makes this case unique from other cases where law enforcement has sought help from third parties is that Apple doesn't currently have the means to help. Because of commitment to data privacy, they do not have the code to unlock the phone. The Justice Department was seeking to compel Apple to "write special software that will override those encryption features in order to

---

[1] "San Bernardino Shooting Updates." *Los Angeles Times*. December 9, 2015. Accessed May 02, 2017. http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-shooting-live-updates-htmlstory.html.
[2] Roberts, Jeff John. "Apple vs. the FBI: An Explanation of the Legal Issues." Does the FBI Have a Strong Legal Case Against Apple? Here's an Analysis | Fortune.com. February 20, 2016. Accessed May 02, 2017. http://fortune.com/2016/02/18/fbi-iphone/.
[3] "Customer Letter." *Apple*. Apple, 16 Feb. 2016. Web. 02 May 2017. <https://www.apple.com/customer-letter/>.

peer into the iPhone used by one of the San Bernardino terrorists."[4] If law enforcement were to try and extract the information without the software the contents of the phone would be erased and investigators would lose any potential evidence that may or may not be on the phone.

When Apple refused to comply with requests from the FBI, prosecutors from the Justice Department brought an additional order to the original search warrant before the Central District Court of California. Following the submission of briefs, "in an unusually detailed directive, Magistrate Judge Sheri Pym of the Federal District Court for the District of Central California ordered Apple to provide "reasonable technical assistance" to the F.B.I. in unlocking the phone.[5] That assistance should have allowed investigators to "bypass or erase the auto-erase function" on the phone, among other steps, she wrote."[6] Apple appealed the decision following the ruling. The case died during that appeals process when the FBI found a third party that was willing and able to break the encryption.

This case is key: it is the penultimate example of the clash that is occurring between the intelligence community and the private sector over national security. It is about technology that does not exist. More than that, it is about technology that the intelligence community does not have and or is unable to get – technology that, according to the intelligence community, is vital to national security. This case also brought this issue to the attention of the public. Legal experts and tech experts alike from *Yahoo Finance, Fortune,* and FBI Director James Comey touted this as the test case for big tech and government that would ultimately land on the steps of the Supreme Court and define the precedent for the coming decades. As *Fortune* put it in 2016, "It's

---

[4]Roberts, Jeff John. "Apple vs. the FBI: An Explanation of the Legal Issues." Does the FBI Have a Strong Legal Case Against Apple? Here's an Analysis | Fortune.com. February 20, 2016. Accessed May 02, 2017. http://fortune.com/2016/02/18/fbi-iphone/.

[5] Ibid.

[6] Benner, Eric Lichtblau and Katie. "Apple Fights Order to Unlock San Bernardino Gunman's iPhone." *The New York Times*. February 17, 2016. Accessed May 02, 2017. https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0.

the biggest tech case of the year, and maybe the decade…The outcome will ripple across the entire technology sector and influence governments around the world."[7] Director Comey, in his testimony before a congressional intelligence panel, agreed that the ultimate outcome of the Apple-FBI showdown is likely to "guide how other courts handle similar requests."[8]

Whether this is true or not, no one can be certain, but what is certain is that this problem is not going to go away. Technology is going to continue to advance, national security is going to continue to be threatened, and the intelligence community will likely continue to fall behind the curve when it comes to the development of technology that aids in the protection of national security. As a result, the private sector and public sector need to be ready to address whatever comes in the future. This will require the achievement of a number of things: (1) it will require understanding the current internal and external environment of both the intelligence community and the private sector; (2) understanding the issues that are preventing cooperation between the two groups (in essence understanding why the private sector won't turn over the technology being requested and why the intelligence community is unable to create the technology themselves); (3) acquiring and in depth knowledge of the legal arguments and national security implications; and (4) understanding the impacts that court decisions like the one discussed in the introduction will have on the private sector in the future.

So, while it might not be possible to decipher the future, it is possible to look at the players, the issues, the legal arguments, and outline potential scenarios for the future and, in

---

[7] Roberts, Jeff John. "Apple vs. the FBI: An Explanation of the Legal Issues." Does the FBI Have a Strong Legal Case Against Apple? Here's an Analysis | Fortune.com. February 20, 2016. Accessed May 02, 2017. http://fortune.com/2016/02/18/fbi-iphone/.

[8] Ackerman, Spencer, and Sam Thielman. "FBI director admits Apple encryption case could set legal precedent." The Guardian. February 25, 2016. Accessed May 05, 2017. https://www.theguardian.com/technology/2016/feb/25/fbi-director-james-comey-apple-encryption-case-legal-precedent.

doing so, begin to truly understand and answer the question of who is ultimately responsible for helping protect national security.

PART ONE: WHO IS INVOLVED?

In examining the question of who is responsible for protecting national security there are three main entities involved. The first entity is the courts, who are acting as referee between the two parties. The second entity is the private sector; a precise definition will be outlined in the preceding sections. The third and final entity is the intelligence community.

All three of these groups have an interest in protecting national security. For the courts and the intelligence community it is part of their responsibility and mission to help protect national security. But what about the private sector? The interest of the private sector protecting national security comes from the markets. "Markets provide a variety of incentives to producers, their customers, and local communities to guard against a wide range of risks, including the possibility of terrorism." [9] However, in the age of globalization the means and extent to which private companies want to guard against acts of terror and help protect national security is changing. While companies understand that terrorism has the potentiality to completely destroy a given business by means of private and social costs, they also understand that there are other outside costs with helping protect national security. In other words all three entities want to protect national security, they all just have different ways and means by which they believe they should be able to do so. This section will look at the details of the private sector and the intelligence community. It will examine the current state of both groups and how the current state of these groups plays into the ability of each to protect national security.

A) The Private Sector

For the purposes of this paper, the private sector is a term used to describe non-governmental actors that are engaged in a variety of different sectors of business in the United States and internationally. The private sector can also be referred to as private industry. Some of the key

---

[9] Farmer, Richard D. "Homeland Security and the Private Sector." A CBO Paper. December 2004. Accessed May 4, 2017. http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/60xx/doc6042/12-20-homelandsecurity.pdf.

companies within this sector come from the sub-sector of information technology (or tech) sector. This sector, as well as several others, are responsible for the production of a variety of technologies that can be used or are relevant to the intelligence community's mission to protect national security.

The information technology sector is comprised of eight different industries. Those industries include: (1) communications equipment; (2) electronic equipment, (3) instruments and components; (4) internet software and services; (5) IT services, (6) semi-conductors and semiconductor equipment; (7) software; and lastly, (8) technology hardware, storage and peripherals.[10] Major companies in this sector include Apple, Samsung Electronics, Foxconn, Amazon.com, Alphabet Inc. (parent company of google), Dell Technologies, and LG. Some of these companies are based internationally and some are based domestically. However they all are global corporations with research and development facilities in the United States or technologies that are overwhelmingly used within the United States. As PwC indicates on its website *Strategy &*, "The tech industry is always in flux. Frequent new products and category innovation define and redefine the sector's constantly shifting landscape. But lately [it has seen] seen even greater volatility than usual, and it has begun to affect the makeup of hardware and software companies themselves".[11] With such fierce competition, companies are in constant battle for the next big thing. Once they find it they are then in a race against the clock to protect it. In an article written for the *Harvard Business Review*, "The New Logic of High-Tech R&D", Gary Pisano and Steven C. Wheelwright have shown that:

---

[10] "Information Technology Sector - Find Investments." Find Investments in the Information Technology Sector - Fidelity. Accessed May 02, 2017. https://eresearch.fidelity.com/eresearch/markets_sectors/sectors/sectors_in_market.jhtml?tab=investments§or=45.

[11] Casey, Henning Hagen Thomas. "2015 Technology Industry Trends." Strategy& - the global strategy consulting team at PwC. January 22, 2015. Accessed May 02, 2017. https://www.strategyand.pwc.com/trends/2015-technology-trends.

> Innovative process technologies are an underexploited way for organizations to protect and extend the proprietary position of their products. Great new products are two-edged swords. They create new markets, attract buyers willing to pay premium prices, and enable a company to generate significant profits. The better and more successful the product, however, the more competitors strive to imitate it. And imitators can be swift and ruthless. Companies have traditionally fended off imitators with patents, but patents rarely provide complete protection.[12]

In other words, the sector is extremely competitive and volatile , making the limited protections that patents and copyrights give to proprietary material extremely valuable. As such it becomes problematic when intelligence agencies then request proprietary technology which then could be released, leaked, or used in a way that diminishes its value to customers within the sector. Companies have little incentive to cooperate with public authorities since maintaining their value, market share, and customer base is a priority. A company wanting to protect its assets is fine on its own merits. Every company within the sector has an obligation to its shareholders to keep the company profitable, but what happens when the intelligence community needs that information to protect national security? A key problem is this inherent conflict between company survival and national security.

B) The Intelligence Community

The intelligence community (IC) is comprised of seventeen different organizations directed by the Director of National Intelligence (DNI).[13] The intelligence community operates on a disclosed budget of approximately 70 billion dollars each year. Other estimates add an additional billion dollars in funds for classified line items that cannot be disclosed. In 2010," the *Washington Post* did a two-year investigation of the current state of the intelligence community. During that investigation, the *Post* found "some 1,271 government organizations and 1,931

---

[12] Wheelwright, Gary P. PisanoSteven C. "The New Logic of High-Tech R&D." Harvard Business Review. July 31, 2014. Accessed May 02, 2017. https://hbr.org/1995/09/the-new-logic-of-high-tech-rd.
[13] "ODNI Home." Home. Accessed May 03, 2017. https://www.dni.gov/index.php/what-we-do/ic-budget.

private companies work on programs related to counterterrorism, homeland security and intelligence in about 10,000 locations across the United States. An estimated 854,000 people, nearly 1.5 times as many people as live in Washington, D.C., hold top-secret security clearances."[14] That number has only grown since 2010.

The rapid growth and expansion of the intelligence community can be directly linked to the terrorist attacks that occurred on September 11, 2001.

> The Pentagon's Defense Intelligence Agency, for example, has gone from 7,500 employees in 2002 to 16,500 today. The budget of the National Security Agency, which conducts electronic eavesdropping, doubled. Thirty-five FBI Joint Terrorism Task Forces became 106. With the quick infusion of money, military and intelligence agencies multiplied… In all at least 263 organizations have been created or reorganized as a response to 9/11. [15]

The rapid expansion of the IC also included the rapid expansion of the bureaucracy that must surround all parts of the federal government. This expansion was deemed necessary for the protection of national security. Unfortunately, there is little data to prove whether or not the rapid expansion of the IC has led to a safer America. The intelligence community cannot broadcast its successes, but everyone knows about its failures. With the rapid growth of personnel within the intelligence space, one would think that the IC would not need the help of the private sector. The problem is that more people does not necessarily mean more solutions. In a globalized and increasingly interdependent world, even with 854,000 people, the IC still needs to consult outside resources.

C) Moving Forward

---

[14] Priest, Dana , and William Arkin. "A Hidden World Growing Out of Control." *The Washington Post*. 2010. Accessed May 03, 2017. http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/2.

[15] Ibid.

So why is it necessary to understand the actors involved? It is necessary to understand the private sector and the intelligence community because the make-up of both entities is completely different. They operate differently, have different priorities, and are motivated by different goals and incentives. Despite this, both groups benefit from a safe America. Business benefits because private business operates at its best in a safe environment. Markets and businesses hate uncertainty and risk. As such they have an inherent buy-in at helping protect national security; if it helps them ensure a safe operating environment, which could lead to higher profits.

Given this common interest, one is left to wonder why won't the intelligence community and the private sector play ball? On its face, some would think that there is no reason for the two not to cooperate as then President Obama put it, "we're going to need the tech community, the software designers, the people who care deeply about this stuff to help us solve it. Because what you'll find… is that after something really bad happens, the politics of this will swing, and they will become sloppy, and rushed, and it will go through Congress in ways that have not been thought through.". [16] Others argue that the only reason that the private sector won't help is because of concern for loss of profits. People opposing Apple's stance are saying that Apple may well lose some business over this. At the time of the incident President Trump called for a boycott until Apple agreed to help the FBI; subsequently many party faithful are claiming that the company is "building phones for terrorists."[17] Still others would argue that the intelligence community is seeking the technology of the private sector solely because they want the proprietary technology to keep tabs on the lives of ordinary Americans. This case in particular has the potential for massive government intrusion in the lives of everyday Americans and in the

---

[16] Elmer-DeWitt, Philip. "What Obama Said About Apple vs. FBI at SXSW." | Fortune.com. March 14, 2016. Accessed May 05, 2017. http://fortune.com/2016/03/12/obama-sxsw-apple-vs-fbi/.
[17] CNBC. "Trump calls for Apple boycott...while using iPhone." CNBC. February 19, 2016. Accessed May 05, 2017. http://www.cnbc.com/2016/02/19/trump-calls-for-apple-boycott.html.

private sector. As Apple said in one of its briefings, "If the government can invoke the All Writs Act to compel Apple to create a special operating system that undermines important security measures on the iPhone, it could argue in future cases that the courts should compel Apple to create a version to track the location of suspects, or secretly use the iPhone's microphone and camera to record sound and video."[18] Additionally, Apple proffers that "Once the process is created, it provides an avenue for criminals and foreign agents to access millions of iPhones. And once developed for our government, it is only a matter of time before foreign governments demand the same tool."[19]

This particular tension that exists between the intelligence community and the private sector once again brings up the age-old debate between security and liberty. Those erring on the side of liberty are more likely to side with Apple and the private sector fighting against the overreach of government. While others will side with the intelligence community who have decided that capitalism and the decentralization of information and authority are no longer in the interest of protecting national security.

The reality is that simplicity of those arguments do not take into account the full context of the issue. The question of who should be responsible for helping protecting national security does not come down to profit and loss, it does not come down to who has the most resources, rather it comes down to a series of factors and issues that are putting both entities at odds against one another.

PART TWO: ENEMIES UNKNOWN

---

[18] Domonoske, Camila, and Alina Selyukh. "Apple Vs. The Government, In Their Own Words." NPR. March 10, 2016. Accessed May 05, 2017. http://www.npr.org/sections/thetwo-way/2016/03/10/469994735/apple-vs-the-government-in-their-own-words.

[19] Ibid.

In addressing the question of who is responsible for helping protect national security it is not uncommon to try and figure out who the good guy is and who the bad guy is. In this case the bad guys are not the private sector nor the intelligence community, it is the people that are putting the two at odds against one another. It is the common enemy of both entities, it is the enemies of the United States who seek to cause terror and bring misfortune and pain to the citizens of this country. It is impossible for the United States intelligence community to process every piece of data, every report, and every intelligence communication. There is just too much information.

Due to the inability of the IC to provide 100 percent protection and security; it is not surprising that acts of terror occur every day, all across the globe, It is the reality of the world as it exists today. In the case of San Bernardino, the terror committed in that office space was committed by two people with guns. The technology at issue in that case was not the guns but the phone that was in the pocket of one of the shooters. The attack was not technologically complex, but the phone was and it prevented the FBI from getting information that it needed in the case that was vital to national security. Technology that may be mundane in its day to day existence can now become the key to unlocking the next big clue.

This time it was guns, the next time there is an attack on the United States it might be an act of cyberwarfare. In a statement to the Senate Committee on Homeland Security and Governmental Affairs, Robert Anderson, Jr. (the acting Executive Assistant Director, Criminal, Cyber, Response, and Services Branch, of the Federal Bureau of Investigation) stated that, "We face cyber threats from state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas— things of incredible value to all of us. They seek to strike our critical infrastructure and to harm our

economy. Given the scope of the cyber threat, agencies across the federal government are making cyber security a top priority".[20] Enemies of the United States do not telegraph their next moves; they do not send us warnings about the means by which they intend to perpetrate their next attack. The enemy now has options, and because of this the intelligence community has no way of guaranteeing that the technology that they currently possess is going to be the most relevant or the most adequate in the protection of national security. Moreover, because of the variety of weapons available to our enemies the intelligence community is struggling to handle every potential threat that comes their way. Whether they know it or not, whether they intend to or not, the enemies of the United States are winning because they are turning natural allies against one another. Both the intelligence community and the private sector are trying to respond to enemies unknown and still meet policy goals and profit margins.

PART THREE: THE COURTS

[20] Sanger, David E. "Chinese Curb Cyberattacks on U.S. Interests, Report Finds." *The New York Times*. June 20, 2016. Accessed May 03, 2017. https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html

In answering the question of who is responsible for protecting national security the answer must ultimately come from the courts, and it is likely that decision will come down from the Supreme Court. But the question that the Supreme Court will answer will not be 'who is responsible for helping protect national security?" The question that they will answer is: does the private sector have to comply with court orders that mandate them to give proprietary technology to the government in the interest of national security or in the interest of helping law enforcement with criminal prosecution? This section will examine two relevant case studies that will help to unpack the legal arguments surrounding the issue. In addition, the section will look at amicus briefs that a variety of different groups have submitted. In understanding the legal arguments, the question of who is responsible for helping to protect national security can be answered, because until Congress ways in or either side surrenders fully the courts will have the final say in the matter

A) Case Study 1

There are two pertinent cases that we can look to for guidance in this matter: cite them both here. This section will cover the first of those two cases.

The facts regarding this case (*In the matter of the search of an Apple iPhone seized during the execution of a Search Warrant on a black Lexus IS300, California License Plate 35KGD203)* are explained in the introduction. In brief: a cellphone belonging to one of the attackers in the San Bernardino terrorist attack was discovered through the course of the investigation. Upon receipt of that cellphone the FBI came to discover that they were unable to unlock that device. They would need to request the help of Apple, the maker of the phone in question, to unlock the phone in the interest of national security. What makes this case different is that, as a result of newer and more advance encryption, Apple did not have the technology to unlock the phone

either. When Apple refused to aid the FBI with their request the FBI went to the courts, seeking an order that would compel Apple to create the technology needed to unlock the phone. Upon receipt of the arguments by both parties, "U.S. Magistrate Judge Sheri Pym of U.S. District Court in Los Angeles ruled that Apple must provide "reasonable technical assistance" to investigators seeking to unlock the data on Farook's iPhone 5C." [21] Apple proceeded to appeal that decision. As the appeals process moved forward the FBI was able to find a third-party vendor that was actually able to unlock the phone. At this point the case was moot, but it still provides a wealth of legal information for this case and other cases that are pending before courts across the United States in which the intelligence community (through the federal government) is requesting the same level of compliance from Apple and others like them.

a) Legal Arguments

In looking at some of the broader legal arguments made in the case: prosecutors on behalf of U.S. Attorney's office argue that the order should be granted under the "All Writs Act" or AWA. In brief the AWA gives the Supreme Court and all courts the power to issue necessary and appropriate writs in aid to their jurisdiction.[22] In essence the Act gives courts the blanket coverage that is necessary to help agencies perform their given tasks by compelling others to act as long as the action required is within the confines of the law. Apple, in contrast, has argued that the order should not be granted. They view the order as a violation of the company's First, Fourth and Fifth Amendment rights. Both party's arguments have merits but must be examined in further detail to get a clearer picture.

---

[21] Reuters. "A judge ordered Apple to help the FBI break into Syed Farook's phone." *Newsweek*. May 22, 2016. Accessed May 04, 2017. http://www.newsweek.com/apple-phone-fbi-syed-rizwan-farook-san-bernardino-shooting-december-isis-427413.

[22] Ibid.

i. First Amendment Arguments

As *CNN Tech* put it, "The [First Amendment] legal argument Apple is expected to use can be summed up like this: Code is protected speech, so the government can't compel Apple to write a new version of iOS any more than it can force an author to write a story."[23] In other words Apple does not want to write the story and the government cannot force them to write it. In arguing the First Amendment violation, Apple could potentially cite *Bernstein v. Department of Justice.* In that case, the U.S. Court of Appeals for the Ninth Circuit ruled that the code in a developer's software was protected by the First Amendment".[24] While this case is not a Supreme Court case, it is the closest that any court has necessarily come to in terms of a definitive answer on the question of code being free speech.

While the arguments are viable they are by no means full proof. The tech giant would "have to overcome years of precedent in the way that companies work with law enforcement"[25]. Apple itself has worked with law enforcement officials in the past. They must prove that this case is different and that there is a difference in the code that they were previously willing to provide and the code that they are currently being asked to provide. The biggest argument that they can make on that score, is that the code that they provided in other cases had already been written and was in existence. In this case, the code does not exist and Apple has never before provided authorities with newly written code upon request.

Secondary to the free speech argument is the 1994 Communications Assistance for Law Enforcement Act. The Act states that law enforcement lacks the power "to require any specific

---

[23] To force Apple to help the FBI unlock a San Bernardino shooter's iPhone. "Apple's case against the FBI won't be easy." *CNNMoney*. February 25, 2016. Accessed May 04, 2017. http://money.cnn.com/2016/02/25/technology/apple-fbi-court-case/.
[24] Ibid.
[25] Ibid.

design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service".[26] The relationship being that as a result of the act not requiring specific "language" in programming, the government has no right to require this kind of "language" or code from Apple.

ii. Fourth Amendment

As Grady Lowman writes in an article for *Rutgers Journal for Law and Policy*, "Apple championed its consumers' privacy rights in the media. But the concern over consumers' privacy rights that has been so prevalent in the media is mysteriously absent where it really matters—in court"[27] (To an extent the argument was brought in Court, but it mainly played out in the eyes of the media and was acknowledged in several decisions). In asserting *jus tertii doctrine* Apple would be allowed to "assert the constitutional rights of their consumers, even though the consumers aren't part of the lawsuit"[28] In 2014 the Supreme Court recognized a "constitutional privacy interest in cell phone data", this protection went beyond the initial grant of the warrant because of the ability of the government to obtain more information than the warrant would authorize. As Lowman puts it, "The concern is that, if the FBI successfully forces Apple to create a backdoor, the government will use this as precedent for carte blanche access to locked phones in the future, creating Fourth Amendment issues not only in the way the phone is accessed, but the potential for over-seizing data", thus uprooting the constitutional privacy interest in cellphone data.

[2626] Hackett, Robert. "Toward Resolving Apple's FBI Dispute." Fortune - Fortune 500 Daily & Breaking Business News. February 26, 2016. Accessed May 04, 2017. http://fortune.com/2016/02/27/apple-fbi-supreme-court-resolve/>.

[27] Lowman, Grady. "Apple vs. FBI: The Forgotten Fourth Amendment Argument." *Rutgers Journal of Law and Public Policy*. Rutgers University School of Law, March 21, 2016. Accessed December 7, 2016.

[28] Ibid.

The opposing argument to this being that the FBI is asking for extremely narrowly tailored access to the code for this one specific phone. So the threat of carte blanche Fourth Amendment violations does not exist. Prosecutors would further argue that they aren't trying to tell Apple exactly how to build the software so there is nothing stopping Apple from writing protocols into the code that would only give law enforcement access to this singular phone. The problem complicating that argument, is that Apple is saying that the software that would allow for single access does not exist, and there is no way to know if the software can be built to only unlock one phone. The arguments in the case regarding the Fourth Amendment would be left to unknown circumstances and arguments of what if.

But it is important to note, that in this case the potentiality for Fourth Amendment violations did not stop the judge from compelling Apple to assist in the case. The judge was convinced that the program could be narrowly tailored enough not to infringe on the Fourth Amendment rights of Apples customers.

iii. Fifth Amendment

In regards to the Fifth Amendment, Apple's attorneys argue, "By conscripting a private party with an extraordinarily attenuated connection to the crime to do the government's bidding in a way that is statutorily unauthorized, highly burdensome, and contrary to the party's core principles, [the government's request] violates Apple's substantive due process right to be free from the "arbitrary deprivation of [its] liberties". [29] In other words, Apple is saying that they have no direct connection to the San Bernardino shooting, and as a private entity there are no laws that outline the court's ability to compel or conscript them into action.

---

[29] Sterbenz, Christina. "Apple Is Using 2 Main Arguments in Its Epic Fight against the FBI." Business Insider. Business Insider, February 26, 2016. Accessed December 7, 2016.

The counter to this argument that could be made by prosecutors is a nod to tradition. As Justice Department spokesperson Melanie Newman said in a statement, it doesn't matter that Apple and the shooting are not substantially related; there is no due process violation as, "Law enforcement has a longstanding practice of asking a court to require the assistance of a third party in effectuating a search warrant…When such requests concern a technological device, we narrowly target our request to apply to the individual device. In each case, a judge must review the relevant information and agree that a third party's assistance is both necessary and reasonable to ensure law enforcement can conduct a court-authorized search".[30]

iv. All Writs Act

The All Writs Act of 1789 is the central argument of the federal government in cases like this one. The All Writs Act was established "to ensure courts in colonial America had the same traditional powers as those in England". [31] It is the opinion of some that the "The feds just want the court, like courts have on many other occasions, to use its power under the Act to get Apple to comply with the search warrant". [32]

This is case is not the first in which the government says that the All Writs Act gives "broad latitude to judges to request "third parties" to execute court orders". [33] There are currently nine open cases involving Apple and other technology companies that involve the AWA compelling the companies to act on behalf of the government to provide a variety of information or intelligence from their products.

---

[30] Ibid.

[31] Benner, Eric Lichtblau and Katie. "Apple Fights Order to Unlock San Bernardino Gunman's iPhone." *The New York Times*. February 17, 2016. Accessed May 02, 2017. https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0.

[32] Roberts, Jeff John. "The U.S. vs. Apple: Does the FBI Have a Case?" *Fortune*. February 19, 2016. Accessed December 7, 2016. <http://fortune.com/2016/02/18/fbi-iphone/>.

[33] Benner, Eric Lichtblau and Katie. "Apple Fights Order to Unlock San Bernardino Gunman's iPhone." *The New York Times*. February 17, 2016. Accessed May 02, 2017. https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0.

In contrast to the broad latitude argument, Apple argues that the act has "strict limits" which are supported by precedent. Precedent concerning it will be discussed a little bit later. But the second part of Apple's argument is that Apple believes that the court won't order the company to act "if it concludes the company is "so far removed from the underlying controversy" or if would place an "unreasonable burden" on Apple". [34] Apple argues that the company is far removed from the underlying crime because they had nothing to do with the shooting and there is no definitive proof there is evidence of the crime on the phone, there is only speculation. Furthermore, the phones service provider has been able to provide phone logs and texts, but there has been no evidence that the phone itself offers any additional proof of the crime. Apple also has grounds to argue that the order would present an unreasonable burden to the company. This unreasonable burden comes as the result of two different factors. The first factor would be the burden of Apple having to come up with the code and software to unlock the phone. As has been stated the code does not exist so Apple would have to devote the time, the money, and the energies to create the code, creating an undue burden. The second factor is the burden that the order will place on Apple's revenue. The company has marketed for years on its ability to provide privacy to its customers. If Apple is compelled to comply and the program is out there it can no longer guarantee this privacy to its customers. This could cost Apple customers and market share, place an undue burden on Apple and its shareholders. The judgement of the legality of the order under the All Writs Act will mainly be determined by the latitude that the court gives to its interpretation.

In terms of precedent regarding the All Writs Act argument the courts has gone both ways. The government cited a 1977 ruling requiring phone companies to help set up a pen register, a

---

[34] Ibid.

device that records all numbers called from a particular phone line.[35] This was a case where the company was compelled to assist the government under the act and the court sustained the order under a broad interpretation. In another case, cited by Apple this time, in 2005, a federal magistrate judge rejected the argument that the law could be used to compel a telecommunications provider to allow real-time tracking of a cellphone without a search warrant".[36] So, when it comes to the All Writs Act there is no clear precedent for the courts to follow.

b) Conclusions

Had this case gone through the appeals process there is little doubt that it would have gone all the way up to be the Supreme Court. Prior to settling out of court this case was slated to set precedent for the intelligence community and the private sector for the next decade. While there is no guarantee what the exact arguments of the parties would have been or what the result of the case would have been it would have provided a strong precedent.

B) Case Study 2

a. Legal Arguments

The second case occurred in the United States District Court, Eastern District of New in February of 2016. In this incidence, a suspect by the name of Jun Feng had been arrested and brought before the court on drug charges. During the course of the investigation Feng's iPhone 5 was lawfully obtained by the police. The phone was not of immediate value to law enforcement. But as the case proceeded law enforcement believed that they needed to be granted access to the phone. Unfortunately, law enforcement was not able to gain access to the information on the

---

[35] Benner, Eric Lichtblau and Katie. "Apple Fights Order to Unlock San Bernardino Gunman's iPhone." *The New York Times*. February 17, 2016. Accessed May 02, 2017. https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0.

[36] Ibid.

phone due to the phones password protection and safety measures. Following an unsuccessful consultation with the FBI, law enforcement in New York requested the assistance of Apple. As such the State sought an order requiring Apple, to bypass the passcode security.[37] It was asserted that such an order would assist in the execution of a search warrant previously issued by the court, and that the All Writs Act, 28 U.S.C. § 1651(a) (the "AWA"), empowered the court to grant such relief.[38] (The All Writs Act was also used in the main argument of the state regarding the San Bernardino shooting which will be discussed at length in the following sections.) Apple in opposition argued that the state did not meet the minimum requirements outlined within the act, and could not prove the factors necessary for the court to order compliance under the AWA. What is interesting about this particular case, and something that is important to the its judgment, is that while the proceedings were occurring between Apple and the government to let them unlock the iPhone the suspect in the case plead guilty to charges. But rather than the order becoming a moot issue, government still sought the order requiring Apple to unlock the device. The reason that they still wanted the phone was for the purposes of sentencing and for use in the trials of Mr. Feng's co-conspirators in the case. With that being said, in February of 2016 U.S. Magistrate Judge James Orenstein ruled against the government denying the motion.

In evaluating the ruling there are several key features that stick out; and are important to the ultimate question of should government be allowed to compel private companies in assisting with matters of national security. While this was not a matter of national security, it is indicative of some of the same arguments. In this motion, the judge "applied previous legal decisions interpreting the AWA and concluded that the law does not 'justif[y] imposing on Apple the

---

[37] IN RE ORDER REQUIRING APPLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT. (UNITED STATES DISTRICT COURT EASTERN DISTRICT OF NEW YORK February 29, 2016).
[38] Ibid.

obligation to assist the government's investigation against its will." In a formulation extremely favorable to Apple, the judge wrote that the key question raised by the government's request is whether the AWA allows a court "to compel Apple — a private party with no alleged involvement in Feng's criminal activity — to perform work for the government against its will."[39] It was the belief of this judge that the law does not permit the concluding result- "both because relevant law contains limits on what companies like Apple are required to do, and because Congress never enacted any such obligations."[40]

Now had Congress enacted such obligations this would be a completely different story. But the point of the matter is that the government did not show enough evidence in support of their application under the All Writs Act. For an AWA application to be successful it must establish the following factors:

1. the closeness of the relationship between the person or entity to whom the proposed writ is directed and the matter over which the court has jurisdiction;
2. the reasonableness of the burden to be imposed on the writ's subject; and
3. the necessity of the requested writ to aid the court's jurisdiction (which does replicate the second statutory element, despite the overlapping language).

See N.Y. Tel. Co., 434 U.S. at 174-78.

In reviewing this motion, the judge held that "Apple had no involvement in Feng's crime, and it has taken no affirmative action to thwart the government's investigation of that crime. [41] In addition, "Apple lawfully sold to Feng, as it sells to millions of law-abiding individuals and

---

[39] Greenwald, Glen, and Jenna McLaughlin. "Apple Wins Major Court Victory Against FBI in a Case Similar to San Bernardino." *The Intercept*. February 29, 2016. Accessed May 04, 2017. https://theintercept.com/2016/02/29/apple-wins-major-court-victory-in-its-battle-against-fbi-in-a-case-similar-to-san-bernardino/.

[40] Ibid.

[41] In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court. (United States District Court Eastern District Of New York February 29, 2016).

entities (including the government itself), a product that can effectively secure its stored data for the protection of its owner," and "Feng used that device for criminal purposes and left it locked".[42] The ruling also emphasized that:

> "Apple is not 'thwarting' anything — it is instead merely declining to offer assistance." While a party may — or may not — have a *moral* duty to assist the government in criminal investigations, "nothing in [prior case law] suggests that the 'duty' … is legal rather than moral." Particularly since Congress has explicitly authorized companies to produce telecommunications devices with security measures, there is no basis to conclude that Apple has done anything wrong by enabling its customers to lock their devices."[43]

The lack of relationship between Apple and Feng was recognized by the judge and as such was a strike against the criteria for an AWA ruling.

Second, when it comes to the matter of 'reasonableness of the burden' imposed on the subject, "the ruling recognized that forcing Apple to compromise its own security systems at the behest of the U.S. government would impose a considerable cost far beyond financial expense".[44] Third, the necessity of the writ was called into question as a result of Feng already having plead guilty.

The arguments that the government made in this motion are extremely similar to other cases that have come before the court in recent months regarding similar requests of compliance from Apple. And the judge took notice of this fact. In his ruling Judge Orenstein wrote the following:

> "The Application before this court is by no means singular: the government has to date successfully invoked the AWA to secure Apple's compelled assistance

---

[42] Ibid.
[43] Greenwald, Glen, and Jenna McLaughlin. "Apple Wins Major Court Victory Against FBI in a Case Similar to San Bernardino." *The Intercept*. February 29, 2016. Accessed May 04, 2017. https://theintercept.com/2016/02/29/apple-wins-major-court-victory-in-its-battle-against-fbi-in-a-case-similar-to-san-bernardino/.
About:
In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court. (United States District Court Eastern District Of New York February 29, 2016).
[44] Ibid.

> in bypassing the passcode security of Apple devices at least 70 times in the past; it has pending litigation in a dozen more cases in which Apple has not yet been forced to provide such assistance; and in its most recent use of the statute it goes so far as to contend that a court — without any legislative authority other than the AWA — can require Apple to create a brand new product that impairs the utility of the products it is in the business of selling.
>
> It is thus clear that the government is relying on the AWA as a source of authority that is legislative in every meaningful way: something that can be cited as a basis for getting the relief it seeks in case after case without any need for adjudication of the particular circumstances of an individual case (as the arguments that the government relies on here to justify entering an AWA order against Apple would apply with equal force to any instance in which it cannot bypass the passcode security of an Apple device it has a warrant to search)."[45]

Even more disturbing to the judge was the government's claim that because Apple is a U.S. company and receives benefits from the United States it has duty or a moral obligation to assist the U.S Government and the intelligence community. On this score that judge states:

> "Such argument reflects poorly on a government that exists in part to safeguard the freedom of its citizens — acting as individuals or through the organizations they create — to make autonomous choices about how best to balance societal and private interests in going about their lives and their businesses. The same argument could be used to condemn with equal force any citizen's chosen form of dissent. All American citizens and companies "derive significant legal, infrastructural, and political benefits from [their] status [as such]" — but that cannot mean that they are not burdened in a legally cognizable way when forced unwillingly to comply with what they sincerely believe to be an unlawful government intrusion."[46]

C) Conclusions

What he writes in his ruling truly embodies the overall since of what is happening in cases like this across the country. Government is using the AWA as means by which they can legislate from the courts. If they were to succeed, they would be forcing Apple and companies across the private sector to help protect national security through court ordered compliance. The

---

[45] In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court. (United States District Court Eastern District Of New York February 29, 2016).
[46] Ibid.

essential ethical point that the judge is making here is that mandated government intrusion into the private sector goes against the foundations of freedom that the country is founded upon. Furthermore, Apple choosing not to cooperate is not and should not be viewed as an effort of the company to support crime or terrorism. Apple did what they believed was right and acted within the bounds of the law in an effort to do maintain the protection of their customers privacy as well.

C) Amicus Briefs

While the legal arguments made by both parties in the two case studies that have been outlined and discussed are of the utmost importance – in our case - the arguments of the two parties are not the only ones of relevance to us. In other words, the voices that are not directly related to this question can be incredibly insightful. The sheer number of groups that came out in support of Apple are telling. In total seventeen different bodies wrote amicus briefs in support of Apple and four additional individuals wrote letters to the courts. Some of these briefs were solely for the use of the San Bernardino case and some were used in both of the case studies outlined above. Some of the briefs come from groups such as: The ACLU, Amazon, AT&T the Center for Democracy and Technology, The Media Institute, and Privacy International and Human Rights Watch. All of these different groups in one voice stood up to say that they supported Apple and that they believed in some way that private industry is not responsible for national security. Moreover, they believe that the government is misunderstanding the original intent of the All Writs Act and that implementation of such a precedent would be bad for the economy, bad for the economy, and ultimately bad for the government.

For example, the ACLU argues that the governments interpretation of the All Writs Act is at its best wrong, and at its worst a make shift power grab for the government to compel third

party compliance in the interest of national security. In a blog outlining their amicus brief the ACLU writes:

> "That law gives courts the authority to issue orders necessary for it to fulfill its judicial role and enforce its decisions. It does not, however, permit courts to give law enforcement new investigative tools that Congress has not authorized. In this case, the act can't be used by law enforcement to give itself the unprecedented power to conscript an innocent third party into government service against its will. The use of this law is made all the more sweeping considering the vast cybersecurity and privacy implications of what the government wants to be able to do." [47]

The concerns that ACLU brings to the table are ones of government overreach. The brief goes onto argue that if the order in the San Bernardino case were to go into effect there is no way to roll that decision back. If the order moves forward, then Pandora's box opens and there is no limit to what the government can force the private sector to do.

In its brief Privacy International and Human Rights Watch argues that:

> "Security features – including encryption and other measures – are integral to the protection of civil and human rights. Countries may seek to compel technology companies to impair security for illegitimate purposes, including to stifle expression, crush dissent, and facilitate arbitrary arrest and torture. In these societies, secure technologies protect all members of society but especially vulnerable ones – such as journalists, human rights defenders, and political activists – by giving them a safe space to communicate, research, and organize.

[47] Sweren-Becker, Eliza. "Why We're Defending Apple." American Civil Liberties Union. March 03, 2016. Accessed May 04, 2017. https://www.aclu.org/blog/speak-freely/why-were-defending-apple.

The U.S., by compelling technology companies to roll back these protections, risks exposing the millions of individuals who reside and work in these places to abuse by their governments."

If private firms are responsible for protecting national security, how are they going to be adequately able to protect their customers? The question would then become can private industry serve two masters: national security and their bottom line This brief puts the implications of this case into a more globalized perspective. The world is watching. There is no way of knowing what will play on the world stage if the needs of the intelligence community are allowed to dictate what private firms have to do with their technology here in the United States. What will other more hostile countries force their private sectors to do? The question that needs to be asked is if the country is ready to set that kind of precedent not only for ourselves but for the world.

The last brief that should be noted here is an amicus brief filed jointly between Microsoft, Amazon.com, Box, Cisco, Dropbox, Evernote, Facebook, Google, Mozilla, Nest Labs, Pinterest, Slack, Snapchat, WhatsApp and Yahoo. These companies, which are normally fierce competitors within the marketplace, came together in unity, reflecting their deep, "shared concerns about the potential ramifications of this case for technology and for our customers. At stake are fundamental questions about privacy, safety, and the rule of law." [48]The amicus brief that was filed also called into question the veracity of the All Writs Act argument. In part the brief argues that,

"The court order in support of the FBI request cites the All Writs Act, which was enacted in 1789, and last significantly amended in 1911. We believe the issues

---

[48] Smith - President and Chief Legal Officer, Brad. "Our legal brief in support of Apple." *Microsoft on the Issues*. March 03, 2016. Accessed May 05, 2017. https://blogs.microsoft.com/on-the-issues/2016/03/03/our-legal-brief-in-support-of-apple/#sm.00000zp5rktq2tdvuyjoycbidoxcl.

raised by the Apple case are too important to rely on a narrow statute from a different technological era to fill the Government's perceived gap in current law. Instead we should look to Congress to strike the balance needed for 21st century technology."[49]

This is not the only brief that brings up whether or not the courts should be the ultimate deciding factor in this case. This brief (and others) have questioned the ripeness of this issue for the judicial branch when it has yet to be addressed by the legislative branch of the government. Many believe that this issue should be legislated on before it comes into the hands of the courts.

These are just a few examples of arguments brought up in the amicus briefs submitted on Apple's behalf, but all of them hit on some of the same themes. The government cannot use the All Writs Act to mandate that the private sector be held responsible for the protection of international security.

D) Conclusion:

Something to remember: while some of the cases discussed in this text are not directly related to national security they pose the same legal arguments and questions that cases involving national security due. In addition, any decision rendered on cases relating to or not relating to national security within this same fact pattern have helped to provide a framework for the question that is being addressed in this text.

[49] Ibid.

PART FOUR: ANSWERING THE QUESTION

The future of this question might be unknown, but there is an answer to the question right now. Based on the research and legal arguments presented at this time, it is not the responsibility of the private sector to help protect national security by virtue of providing aid to the intelligence community. The courts have thus far not compelled the private sector to do so and the private sector has not chosen to do so voluntarily. In cases directly related to national security and in

cases with similar fact patterns the courts have said it is not the responsibility of the private sector to act, with one exception. In the San Bernardino case Apple was ordered to comply with the FBI, but the case was dropped and the order withdrawn. As such no company within the private sector has been compelled to help protect national security. Now some would argue that it is everyone's job to help protect national security, and to an extent it is. But as of now it is not the responsibility of the private sector to either provide proprietary technology or create technology that will help the intelligence community protect national security, so to that extent it is not the job of the private sector to help protect national security.

PART FIVE: MOVING FORWARD

While it is not currently the private sectors responsibility to help protect national security, there is no certainty that this will be the case forever, a ruling may come down or a law may be passed where it does become the responsibility of the private sector to help protect national security. So the best thing that the private sector can do is be prepared for likely legal outcomes, and take steps now to prepare for a future that is uncertain.

A) Likely Legal Outcomes

This section addresses the most likely legal courses of action that will happen moving forward regarding this issue.

First, there is no way that this issue is going to go away on its own. From September of 2015 to February of 2016 Apple has objected to or otherwise challenged at least twelve government requests to help extract data from locked iPhones. There are currently nine cases from those twelve that are still pending before the courts at the time of this writing. And those are just cases involving Apple. Microsoft has also gone to court over similar questions regarding compliance when it comes to court orders. So what happens next?

At the time of this writing the, neither of the parties involved in Case Study 1 (regarding the Iphone of the shooter in the San Bernardino Attack) plan to refile or appeal any decision reached in the case. As for Case Study 2 (regarding the Iphone of a drug trafficker) the Department of Justice (DOJ) has made public statements that they plan to appeal the decision of Judge Orenstein to deny the motion to compel Apple to unlock the Iphone of the suspect in the case. At this time, no further information could be found regarding a further appeal, however the DOJ has said that the case is ongoing. [50]

Prior to the ruling and subsequent dismissal of the San Bernardino case experts were saying that, "No matter who wins, an appeal is virtually certain. Apple CEO Tim Cook has vowed to challenge the government's order to the Supreme Court, citing it as a threat to consumer privacy and cybersecurity. The Justice Department has also signaled that the issue

---

[50] Brandom, Russell. "Department of Justice appeals ruling in New York iPhone unlocking case." *The Verge*. March 07, 2016. Accessed May 05, 2017. https://www.theverge.com/2016/3/7/11176566/apple-fbi-encryption-appeal-new-york.

merits scrutiny by a higher court". [51] Now this never happened as the case was dismissed, but had the case not been dismissed and the ruling of Judge Pym compelling Apple to assist the FBI been staid on appeal there would be two different courts in two different districts saying to different things. You would have the California judge ruling (in essence) that private companies are responsible for helping protect national security and you would have a New York judge saying that private companies are not responsible for helping police in a criminal prosecution. While this not a technical circuit split, it had the potential to become one. And there is no reason to believe that it might not come to that eventually. With nine other cases pending before the courts, there is still very much a chance that a circuit spit could occur increasing the likelihood that the issue will come before the Supreme Court.

If the case comes before the Supreme Court, there is no telling what will happen. It will depend on the make-up of the Court, the case presented before the Court, and the need for expediency (depending on the case brought before the Court). It will depend on the ability of the given agency to justify the order that they seek under the All Writs Act. The Supreme Court case will come down to the All Writs Act. There are constitutional arguments involved in this case but it is the All Writs Act that has been the central argument of prosecutors seeking orders to compel the assistance of tech companies. It has also been the All Writs Act that has resulted in rulings against agencies seeking the help of the tech industry. The government has not been able to make the case stick (with the exception of San Bernardino) when it comes to the All Writs Act. If they can do it then they have a fighting chance, but the decisions that have been handed down, thus far, in cases discussed in this text as well as others not discussed here, have sided with the private sector.

---

[51] Ibid.

The Court will rule in one of the following ways: it will either say that it is responsibility of the private sector to aid the intelligence community; it is not the responsibility of the private sector; or they will say that it should be the issue of Congress and request Congressional action. One of these things will happen, but at this time it is not clear which one.

There is also the chance that Congress could choose to act in the matter and remove the decision from the courts entirely, as some believe Congress should. Judge Orenstein in his ruling from Case Study 2 writes, "Congress should decide how much cooperation Apple should be forced to give in the encryption case. Using the All Writs Act to force Apple to unlock an encrypted phone would transform the law "into a mechanism for upending the separation of powers by delegating to the judiciary a legislative power bounded only by Congress's superior ability to prohibit or preempt." [52] While there is no rhetoric coming from Congress that they are willing to take up this issue at this time, another high profile incident like San Bernardino might force Congress to act rather than wait for a case to make its weigh up to the Supreme Court.

Looking at the likely legal outcomes the one and only thing that is certain is that this issue is not going away anytime soon.

B) Preparing for the Unknown

Because the legal outcomes of further cases are unknown, and because the answer to the question of who is responsible for helping protect national security may change, it is important for the private sector to try and start preparing now for what may come.

a. Things to Consider

There are some important things that the private sector needs to be considering now before

[52] Ibid.

anything changes regarding the relationship between the private sector and the intelligence community. First, companies in the private sector, particularly in the tech industry, need to pick a side on this issue and they need to do so now. As was stated previously there are as many if not more unknown enemies to the United States than there are known. There is no telling where the next terrorist attack will come from and there is no telling which company will be impacted by that terror attack. So in the event that they are impacted, companies need to make a decision now as to whether or not they will choose to hand over their technology or create new technology in the interest of helping protect national security. Depending on what they choose to do they will need to be ready for a fight. Support needs to be garnered from within the company now to prepare for any potential backlash that may come no matter what the decision of a company is.

The next thing that the private sector needs to consider is public perception. When Apple refused to help the FBI some saw the move as a marketing ploy; others saw it as a genuine concern for their customer's privacy rights; and some presidential nominees called for a boycott of all Apple products resulting in backlash from members of the republican party.[53] Despite the array of opinions regarding the Apple's refusal, public perception of the move was for the most part positive as people are starting to want more of their own privacy back from the federal government. However, companies that choose to refuse to help the intelligence community are walking a very fine line when it comes to public perception of the issue. For example, what would have happened if the iPhone that belonged to the San Bernardino shooter instead belonged to one of the terrorists that orchestrated 9/11.There is little doubt that public perception of Apple would change dramatically if Apple had refused to aid the FBI under those

[53]Diamond, Jeremy. "Donald Trump calls for Apple boycott." *CNN*. February 19, 2016. Accessed May 05, 2017. http://www.cnn.com/2016/02/19/politics/donald-trump-apple-boycott/index.html.

circumstances. Some could view the decision of the private sector as unpatriotic. What is important for companies to understand is that they are walking a tight rope when it comes to the public's perception of this issue. So company's need to be prepared for a changing tide, because there may come a day where fellow industry members may support a given decision but customers do not.

Lastly, the government is not the same as it was when this issue was in the spotlight in 2016. In February 2016 President Obama sided with the intelligence community on the issue of whether or not Apple should help the FBI, but saw that there was the potential for harm in doing so.[54] In contrast, then Candidate Trump called for a boycott of Apple products. Candidate Trump is now President Trump and Republicans now have control of both the House and Senate. Companies who are trying to make the decision of whether or not be responsible for helping protect national security are facing a very different political climate than when the issue was a hot topic. For companies in the private sector all this means is that they need to know and understand who they will be up against, no matter what side of the issue they come down on. They need to understand that the next time this issue comes up it will probably end up before the Supreme Court or Congress.

b. If the status quo stays the same…

If the status quo stays the same and the private sector is not held liable for helping to protect national security, then the intelligence community will have to turn to third parties or one of their

[54] Machkovech - Mar 11, 2016 10:35 pm UTC, Sam. "Obama weighs in on Apple v. FBI: "You can't take an absolutist view"." *Ars Technica*. March 11, 2016. Accessed May 05, 2017. https://arstechnica.com/tech-policy/2016/03/obama-weighs-in-on-apple-v-fbi-you-cant-take-an-absolutist-view/.

1,931 private companies to get needed information.[55] A prime example is the San Bernardino case, the only reason that the case was dropped was because Apple found someone else to unlock the phone. So, that also means that the technology that Apple did not want to create for fear of it getting misused by the government, is technology that the government now has. This means that Apple will need to either once again upgrade its encryption software or try to now compel the FBI to turn over the software that gave them access to the phone. From there Apple will have to re-adapt its own software. In other words, the situation has now evolved from both Apple and the FBI standing outside the locked door to just Apple standing outside the locked door of getting customers information. Now Apple will have to spend time, spend money, and re-task valuable research and development personnel so that Apple can relock the door and keep government out of reach of the key that it has worked so long and hard to try and keep out of reach of the intelligence community and itself.

c) If the status quo changes…

If the status quo changes and companies are held responsible for helping protect national security then they will face an entirely different set of problems. As a result of the change companies will be forced to either hand over their technology or create technology when ordered to do so by the courts. This means handing over technology that could be leaked to other companies, thus losing its value – or it could mean giving government blanket access to every phone in the country; which then gives the intelligence community the potential for misusing the technology. If this occurs it will force companies to spend the time to create new software or spend the time creating software that will only give the intelligence community access to one

---

[55] Priest, Dana , and William Arkin. "A Hidden World Growing Out of Control." *The Washington Post*. 2010. Accessed May 03, 2017. http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/2.

phone. In order to do this and comply with a given court order companies will either spend significant amounts of their own research and development budgets or wait to be reimbursed by the government. No matter what the private sector would be significantly impacted by a change of the status quo and companies need to be aware of the impacts that those changes would have now, before the status quo changes. In other words, the best defense is a good offense, no matter what side of the issue a given member of the private sector falls on companies must try and stay ahead of the curve when it comes to the issue of who is responsible for protecting national security.

PART SIX: PERSONAL REFLECTION AND AUTHORS BIOGRAPHY

When I first started this project I literally had no idea what I was getting myself into. At the point that I was first starting my project I was just finishing my scholar semester for the Huntsman Scholars Program. Due to my participation in the program I was in teams writing long papers and doing extensive research, so I thought doing one on my own would not be so bad, and

doing own on the topic of my choosing meant that it would be even easier than a Scholars project. I could not have been more wrong.

Writing my honors thesis has been one of the most challenging things I have done in my academic career. It has also been one of the most rewarding things that I have ever done in my academic career. The experience that I gained from writing something of this magnitude was something that I never expected to get out of my college education. When I was a freshman I never thought that I would be sitting here writing this reflection.

Now let me tell you a little bit about my thesis. When I set out to try and pick a topic for my thesis I knew that I wanted it to be cross disciplinary and I knew that I wanted it to involve national security. What I didn't know was the struggle that I would face trying to pick a topic. At this point picking my topic wasn't a priority, unfortunately like most college students it wasn't on my radar until about a week before it was due. At this point I reached out to my now mentor Dr. Shannon Peterson. I do have to say that choosing Dr. Peterson as my mentor and Professor Ferguson as my committee member was by far the easiest part of my project. Doctor Peterson sat me down and walked me through my ideas to help find a common thread that I could put together for a topic.

Once we figured out my topic all I then had to do was right it. Let me pause now to give my first piece of advice to anyone who is currently in the position of trying to write an honors thesis. Think about how long it will take you to complete your thesis… then triple it. It always looks so much easier at the outset. Because my thesis is primarily literary based I needed sources and a lot of them. Some sources were easy to find and some were not so easy, but make sure if your project was literary based like mine was give yourself enough time to get into the material.

I did not start writing my thesis until pretty late in the game, and it would have been a lot less stressful for everyone involved if I had been writing as I went. What is that saying, do as I say not as I do. Please don't make the same mistakes I did. The other mistake that I made in writing my thesis was that up until the day before it was due I wasn't writing my thesis for me. Sure, I was passionate about my topic and everything but I was not writing my thesis for me. I was writing it to graduate with honors. I was so scared that it wasn't going to be good enough. I was so scared that it wasn't adequate to have my committee members' names on it that it almost paralyzed me, and I honestly almost didn't finish. I wasn't writing it for me, I was writing it be perfect. In reply to an email that I sent to my mentor in almost total panic she told me that ultimately my thesis was something that I needed to be proud of. That was the moment that had you been with me you would have seen the light bulb go on over my head. I realized that I had to do this for myself, I had to finish it for myself, and have it be meaningful and successful for me.

In that moment, I went from wanting to rewrite the entire thing for a third time (at that point I had rewritten almost every part twice) to taking a step back and looking at the totality of what I had written rather than looking at it piece meal, and being overwhelmed with what I had accomplished. That day and into the next I made last edits on my thesis, and I could honestly not be prouder of my final product. I have no doubt that my thesis is not perfect, but it is perfect for me.

If I could tell a student who is considering writing a thesis any two pieces of advice it would be these. If you are considering doing an honors thesis, do it, it is well worth your time; if you are writing it for yourself. And find a good mentor, I can honestly say that this project would

not be completed without Dr. Peterson. Dr. Peterson if you are reading this, thank you! There is no way I could have done this without you.

Jamie Crandal

Jamie Crandal came to Utah State University as an out-of-state student hoping to find a second home here at USU. In her time here she not only found a second home, but a family. Jamie quickly became involved in a variety of on campus organizations. In addition to her involvement Jamie was involved in the Honors Program and the Huntsman Scholars Program at USU. Through being involved in Honors and Scholars, Jamie found a passion for learning. Upon graduation from USU in May 2017 with Bachelor's degrees in International Business and Law & Constitutional Studies. She plans to continue her education at law school in the Fall of 2017 pursuing a Juris Doctorate. Jamie hopes that through her involvement, she has been able to give back to USU a small part of what USU has given her.