LEGAL IMPEDIMENTS ON TECHNOLOGY BASED EVIDENCE IN CRIMINAL INVESTIGATIONS

by

Chanel Outley

A capstone project submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Public Management

Baltimore, Maryland
May, 2017

© 2017 Chanel Outley
All Rights Reserved
Abstract:
This capstone project entitled “Legal Impediments on Technology Based Evidence in Criminal Investigations” explores the issue of the legal impediments that currently exist based on outdated laws, which in some cases have kept law enforcement officials from being able to access information from locked or otherwise inaccessible technology devices such as phones or smart speakers, to be used as evidence in criminal investigations. Throughout the paper, cases that support this claim are explored, including the case of a man who was found dead at a home which an Amazon Echo was found but could not be fully utilized as evidence, as the information on the Echo was not stored locally. This paper also explores the various legal avenues available to law enforcement officials to force citizens and companies to release private information held on technology devices, and the recent rulings that have made enforcing such requests challenging.

The results of this capstone demonstrate that there is a gap in the legal authority of the federal government to require technology companies to comply with certain subpoenas that would burden the technology company/owner of the technology; even if it is suspected that the information that would be obtained from the device would help to solve a crime. The solution proposed as a part of this capstone would offer potential relief of the issue without directly imposing additional privacy laws—which may be hard to pass due to partisan lines—however, the cost of the proposal, along with the proposed solution being optional instead of law creates potential for the lack of adaption and/or success. Nonetheless, the proposed policy may be attractive to technology companies, as they would be able to share the burden of responsibility of data ownership with the
federal government. Although this is a risk for the government, owning data that could help solve crime would significantly reduce the time and effort required by law enforcement to obtain such information, which may be considered worth the risk.
## Contents

**Abstract:** ............................................................................................................................ ii  
**Action Forcing Event:** ......................................................................................................... 1  
**Statement of the Problem:** .................................................................................................. 2  
**History:** .............................................................................................................................. 5  
**Background:** .................................................................................................................... 10  
**Policy Proposal:** ............................................................................................................... 16  
**Policy Analysis:** .............................................................................................................. 18  
**Political Analysis:** ............................................................................................................. 24  
**Recommendation:** ............................................................................................................ 28  
**Curriculum Vitae:** ............................................................................................................ 30
To: James Comey, Director of the Federal Bureau of Investigation (FBI)

From: Chanel Outley

Date: April 26, 2017

Subject: Legal Impediments on Technology Based Evidence in Criminal Investigations

Action Forcing Event:
On November 22, 2015, a man was found dead in a hot tub at the home of his friend in Bentonville, AR. The home owner, James Bates was subsequently charged with first-degree murder. During the investigation, police seized an Amazon Echo that was found in the kitchen. Police believe that data from the Amazon Echo will be pivotal in their investigation and thus, they have served Amazon with a search warrant for data covering two days around the time of the murder.¹

While Amazon has satisfied a portion of the request, the company has not released conversations recorded to its servers by the Echo, stating they object to “overbroad or otherwise inappropriate demands as a matter of course”. In recent similar cases, the government has had limited success at forcing technology companies to comply with requests to release personal information stored on private servers for the purposes of legal investigations, or at requiring technology companies to aid the government in the recovery of data from devices they manufacture.² It is important for laws to be

---


established that govern what rights technology companies and private users of technology have when utilizing Internet connected devices that may be useful in government investigations. Without government intervention, it is likely that similar cases will become increasingly popular and traditional means of investigating crimes will be increasingly ineffective, thus leading to an increase in unsolved crimes.

Statement of the Problem:
Currently, there are legal impediments which keep law enforcement officials from obtaining what could be lifesaving or crime solving information from personal devices. There are multiple technical variables that keep law enforcement and the government from obtaining personal data from devices, including strong encryption and data storage techniques. Given these technical constraints, law enforcement officials often need assistance from the manufacturing technology company, or some other legal technical avenue, in order to obtain personal information that could help them solve crimes. The federal government has expressed growing concerns around this topic and the pace at which laws are made in relation to the pace at which technology is being consumed and improved. Current laws do not take into account how much Americans rely on technology instead of other traditional means of interacting and storing personal data.

According to a recent survey conducted by the Pew Research Center, 77% of Americans own a smartphone. This number is up from the same statistic in 2015, in which Pew found that 68% of Americans owned a smartphone. The data shows an increase in trends towards not only the use of smartphones, but other technology, including tablets and other “smart” devices including televisions and speakers. This means that more and more,
information that could once be found in paper form, or physically locked in a location is now being digitally stored and secured.

While the idea of constant monitoring is not new—as the government and private businesses participate in various surveillance activities—how such data is now being processed and stored has created a new legal constraint. With cloud storage and strong encryption in place, being able to obtain a warrant for a piece of technology is nearly no help at all in most investigations. Additionally, since not all data recorded with a piece of technology is stored on that piece of technology, additional legal action is often needed to pull information from servers, which do not belong to any one person. Thus, giving law enforcement access has the potential to compromise other people’s personal data in the process.

On March 1, 2016, FBI Director James Comey testified that through current legal avenues, the information that the FBI is able to recover from personal devices that have encryption such as cell phones is unreadable. This poses what he describes as a threat to public safety.4

Not having the legal grounds to recover data for an open investigation is becoming a common issue for the government. During his testimony on the topic of Apple iPhone Encryption, Director Comey referenced a murder investigation which remains open.5 A key piece of evidence in that case is thought to be a digital diary, which was kept on the murder victim’s cell phone and has not successfully been unlocked with its original

contents by authorities. The government has run into similar issues with multiple technologies and technology companies, including Amazon, the maker of the Echo. This has hindered the justice process and has left many cases, including the murder case of Victor Collins in Bentonville AR. unsolved.

Not having legal avenues to take to obtain personal data from devices is also being considered a national security concern. Director Comey also testified that terrorist groups such as ISIS are using encrypted forms of communication to order the killings of innocent Americans.\(^6\) This issue is tied to the larger terrorist issue of ISIS using the Internet, and eventually encrypted forms of communication to recruit and radicalize domestic followers.

The FBI is well aware of the legal limitations of warrants to obtain information from personal technology devices.\(^7\) This is also becoming a very public limitation of the government. Although the case against Apple was dropped by the FBI since they were able to employ an outside vendor to decrypt and recover the data on the phone, on the surface this can appear to be a legal “victory” for Apple over the government since they did not have to comply with the government’s request to aid in the decryption of an iPhone for the purposes of an investigation. It is likely that this “victory” has played a part in Amazon’s hesitance to fully comply with the government’s request for information.\(^8\) In the event that Amazon is also able to legally avoid having to turn over additional consumer information, specifically personal data collected from a “secure”

---


technology, there is the possibility that a trend which is unfavorable for government, and in turn unfavorable for public safety will emerge. Multiple cases in which technology companies have victories over the government or where the cases are dropped have a high probability to set legal precedence over future such court cases and are likely to be referenced accordingly by legal counsel. Additionally, a high number of cases which have to be dropped by the government sets a tone that there are no clear legal avenues to be taken on matters such as these, and thus, cases might tend to be taken less seriously.⁹

All the while, technology companies are observing, and doing more to secure their devices, since this is part of the buying attraction for consumers. Most technology companies, including Apple, list the steps they are taking to protect consumer’s private information on their public facing websites as something they are proud of. With every case that is dropped, technology companies are able to pick up the pieces, learn from the experience, and further secure their devices.

**History:**
As far back as the constitution, there has been mention of the rights of citizens to be secure while also allowing for the government to conduct its official business. The Fourth Amendment protects citizens from unreasonable searches and seizures. Through the Fourth Amendment, it is generally understood that in order for law enforcement to search private property, there must be a warrant unless a circumstance falls into a special exception category—those categories being consent, the plain view doctrine, search

---

incident to arrest, and exigent circumstances. These exceptions, particularly the search incident to arrest and exigent circumstances exceptions, have helped law enforcement over the years to resolve cases by allowing them to collect as much untampered evidence as possible early on during an investigation.

However, the increase in technological innovation has put a small caveat in what was otherwise a somewhat straightforward letter of the law. The uptick in the use of the personal computer in the early 1980s, followed by the rise of the Internet and other technologies, has changed the way humans interact. One of the most revolutionary technologies as of late was the camera phone, which first made its entrance into the United States marketplace in November of 2002. Not so long after, in January 2007, Steve Jobs—then chief executive of Apple—introduced the Apple iPhone, which is thought to be the world’s first popular “smartphone”. Since that introduction, smart technologies have continued to evolve and change the way people work, learn, and achieve personal goals.

The boom of the camera phone and then smartphone presented a unique time for law enforcement officials and law governing bodies, as people were able to easily take photographs and videos of events and store them on their phone. Under such technology, searching a phone as a part of one of the aforementioned exceptions to the Fourth Amendment was less cumbersome. If a phone was found on a person during an arrest, or

---

in some other situation where there was probable cause for the search, law enforcement officials were generally able to collect cellphones as physical evidence, and use information from the phone as evidence. However, overtime, technology evolved and people started to use their smartphones for purposes far beyond photos and videos. The growth in popularity of smartphones and other smart technologies have connected people through devices and the Internet, but also has increased the amount of personal and sometimes sensitive data a person is carrying with them at any given time. Smartphones can store a lot of data, often including normal GPS routes taken, bank account information, redeemable purchased tickets for sporting events, shows, and airline flights, time, location, and date stamped photos and videos, written communications and so much more. The rise of social media, online banking, mobile payments, emails, mobile GPS applications, and digital health information changed the level of sensitivity around smartphones and other Internet connected devices and their data.

To adapt to these changes, technology companies have enhanced security features far beyond a four digit pin to unlock devices. Today biometrics such as fingerprint readers can be found on smartphones and are commonly used to unlock devices. Laptops and other devices also commonly use facial and voice recognition technology in order to unlock. Additionally, most devices are built with timeout features, which will lock the device, or even completely wipe all data from the device, in the event a wrong password or pin is entered multiple times within a certain timeframe. Thus, unlike traditional evidence—such as drugs, a weapon, or physical documents or pictures—that can be recovered under an exception to the Fourth Amendment, recovering a technology device is generally useless under these exceptions, as there is no language in the law that forces
the owner of the device or the manufacturer of the device to unlock it, even if law enforcement legally has possession of the device.

Commonly at the point in the investigation where law enforcement officials have a device that they cannot gain entry into because they do not have the password, a warrant is obtained to gain more information on the individual—say account information and history or a search of other physical property belonging to a person—that will aid in the opening of the device and/or additional clues needed to solve a crime. However, the scope of a warrant usually only goes as far as what is relevant to solve the crime. Thus, with the evolution of cloud technology, it has become increasingly difficult to legally determine how much of an obligation technology companies—who store data in the cloud—have to provide law enforcement to fulfill requests, including those for assistance with unlocking devices and/or accessing cloud backup of information.

Law enforcement has tried to work with and around the divide that clearly exists between law enforcement and the lock on personal smart devices. In June of 2014, the Supreme Court ruled that cellphones and smartphones generally could not be searched by police without a warrant during an arrest.14 This ruling struck down various lower level court rulings. However, somewhat of a legal loophole exist. In March of 2016, the American Civil Liberties Union (ACLU) released findings that indicated that federal law enforcement has attempted at least 63 times to force technology companies break into the personal phones of suspects ranging from at least 22 states.15 In all 63 cases, the All

---


15 Jose Pagliery, “Here are the places the feds are using a controversial law to unlock phones,” CNN, March 30, 2016, http://money.cnn.com/2016/03/30/technology/phones-all-writs-act/
Writs Act was referenced. The law, which was signed by President George Washington over 200 years ago, allows judges to fill in the gaps of other, more explicit laws.\textsuperscript{16} The use of the All Writs Act used to be fairly common, however, as of late it is mostly only used in extraordinary circumstances where no other laws properly apply. Pervious court cases where the All Wits Act has been invoked to obtain personal information from/about a phone can be dated back to 1977 when phone companies were ordered to help set up devices that recorded all numbers called from a specific line. The Act was referenced in another ruling pertaining to phones in 1999 in the Public Safety Act of 1999 which requires all cellphone providers to be able to geolocate their customers’ phones.

Many of the federal court records found by the ACLU were sealed and most of the 63 noted cases which date back to 2012 have been closed. Beyond those cases involving the All Writs Act, law enforcement officials make thousands of requests to technology companies for user information annually. In 2015 during a six month time period from January to June, law enforcement officials submitted more than 34,000 requests for user data.\textsuperscript{17}

The research indicates that federal law enforcement has been somewhat successful at obtaining some information—mostly usernames and passwords—under court orders issued under the All Writs Act.\textsuperscript{18} The greater legal challenge comes into play when username and password information is insufficient to gain access to the information law

\textsuperscript{17} Lucas Jackson, “Here’s how often Apple, Google, and others handed over data when the US government asked for it,” Quartz Media, February 19, 2016, https://qz.com/620423/heres-how-often-apple-google-and-others-handed-over-data-when-the-us-government-asked-for-it/
enforcement is seeking. It is in these instances that technology companies have found their own legal loopholes. Technology companies, including Apple and Google, have either stated that they would or actually have pushed back on court orders that would require them to develop new technology to fulfill any government request. In some instances, including the 2014 case of illegal gambling businesses which were operated out of three villas at the Caesar’s Palace Hotel in Las Vegas, technology companies—in this case Apple—have simply implied that it would take an extended period of time to develop the kind of technology needed to fulfill requests from the federal government. Historically in such cases, the prosecutors have either gathered other evidence or used outside vendors, such as hackers, to access the data they need in order to continue investigations.

**Background:**
While at a high level it could be assumed that the topic of having legal access to technology devices for the purposes of investigations and crime solving is thought to be a government vs. Silicon Valley issue, there are mixed views on the use of and access to personal technology data within the government and even within political parties. There are some, like Jeff Sessions who believe that technologies that protect personal information, such as encryption, are important, however, should be able to be overcome “under lawful authority, when necessary to the furtherance of national-security and criminal investigations”.\(^{19}\) Sessions, who is the newly confirmed Attorney General of the United States, will certainly have a say in the way the country moves forward on this

---

issue and issues similar to it. Similarly, President Trump has spoken against Apple’s actions and in favor of expanding the powers of the government in matters of national security. As such, it is likely that under the Trump administration, the government will continue to pursue legal avenues to have technology companies comply with requests for obtaining personal information from devices. And with the Trump administration just beginning and the potential for reelection, there is plenty of time for a legal precedence to be set, seeing as though up until this point, there have been minimal clearly set laws and directives as it relates to the government’s reach into technology companies for personal technology data. This is key to note, as there are various legal proceedings, including the legal matter that served as the action forcing event for this memo, which have been open since before the change in political power (from the Obama (Democratic) administration to the Trump (Republican) administration), which can be swayed in a different direction under different leadership. It also important to note that cases involving personal data and technology companies can be appealed all the way up to the Supreme Court, where there is currently a vacancy.

Prior to end of his term, President Obama nominated Merrick Garland to fill the position made open by the death of Justice Antonin Scalia. Garland, who is known as being moderate-to-liberal in his rulings would have created the first liberal majority in the Supreme Court in more than 40 years. Garland has been known to lean to the right in cases involving terrorism, including during his involvement in the Oklahoma City bombing case and the arrest of the so-called Unabomber. These involvements and

---

outlook may have brought a unique perspective to the Supreme Court on similar topics such as the government’s reach into technology companies for personal data, however, Garland’s nomination expired in January at the end of the Obama administration, after a successful block by Senate Republicans who did not even consider his nomination.

Early into his term, President Trump has nominated Federal Judge, Neil Gorsuch to fill the position on the high court. Gorsuch, much to Trump’s promise to nominate someone with a similar political stance as Justice Antonin Scalia, is a conservative. While Gorsuch has not explicitly provided his view on encryption, Gorsuch has a history of arguing that the meaning of the law is for judges to decide, not federal bureaucrats.21 If Gorsuch is confirmed, the Supreme Court will remain majority conservative. This is particularly important to note, as Justices serving the Supreme Court are typically there until they are no longer physically able and/or until they pass away. And since Gorsuch is only 49 years old, his stance and opinion will have long lasting impacts on law in the country.

In addition to the President, Attorney General, and potentially the next member of the Supreme Court being in favor of government backdoors to secure technologies, the FBI Director James Comey—who assumed his role under the Obama Administration and remains in his role under the Trump Administration—is a long standing advocate for government font doors into encrypted devices. In 2014, a year before the San Bernardino shooting which lead to the legal case with Apple, Director Comey stated that instead of attempting to use any backdoor approach to obtain data from locked devices, he hoped to

“use the front door, with clarity and transparency, and with clear guidance provided by law.”

While it is clear that the FBI Director, Attorney General, and President are in favor of some governmental power over data stored on devices when there is a matter of public safety, there are those government officials who believe that technology companies should not have to make any special provisions for the government, including Senator Ron Wyden who is a member of the Senate Select Committee on Intelligence. Senator Wyden has been known to be a leading voice on the protection of personal data via methods such as encryption and has spoken out against giving the Department of Justice more power to get consumer data from technology companies. Like many others who oppose giving the government increased power to collect personal data about consumers from technology companies, Wyden believes that too often under current law, innocent Americans have their data collected as a part of massive “sweeps” or investigations, instead of having targeted requests and approaches to only obtain the information needed to solve a particular case. In an interview with the New York Times, the Senator spoke about his opposition for increased government power over personal data and the passing of what is known as Rule 41. Rule 41 is intended to make it easier for the FBI to carry out complex computer investigations. Under the rule, law enforcement agencies can search multiple computers across the country with a single warrant. It may surprise some that Rule 41, which clearly leans towards increased government insight over

---

personal technology data, was passed during a time of democratic majority in the House and Senate. This far contradicts the normal partisan lines that have been drawn on the issue.

It is commonly thought that many conservatives (Republicans) are in favor of more government and legal power/oversight over personal data while liberals (Democrats) are thought to be widely oppose to increased oversight. Given that Republicans now have majority in both the Senate and the House, it is likely that more conservative individuals and laws will be confirmed and passed. Historically, conservative politicians have associated the government’s reach into personal data with matters of national security. Jeb Bush—who ran for the Republican Presidential nomination in 2016—sated during his campaign “If you create encryption, it makes it harder for the American government to do its job—while protecting civil liberties—to make sure that evildoers aren’t in our midst”.25 Carly Fiorina, the former chief executive officer (CEO) of technology company Hewlett-Packard (HP) and 2016 Republican primary candidate for President stated that there was a need to “tear down cyberwalls” when asked about Apple and Google’s implementation of end-to-end encryption.

Yet, the passing of Rule 41 during Democratic majority in the Senate and House is not the only note worth anomaly in this matter. President Trump, a Republican, has also provided mixed signals when it comes to his stance on technology companies and matters of privacy. In December of 2016 as the President-Elect, Donald Trump held a meeting in Trump Tower with the executives of a variety of technology companies, including

---

Google’s parent company, Facebook, Microsoft, Amazon, and Tesla, among others. The tone of the meeting was reported to be exceptionally positive, as Donald Trump was quoted saying “we’re (the government) going to be there for you”.26 The meeting focused heavily on ways technology could be used to reduce government waste and the topic of government oversight and reach into personal data was not specifically addressed.

However, from the meeting, the then President Elect indicated that there would be future quarterly meetings with technology executives, which will be coordinated by Trump’s son-in-law and advisor, Jared Kushner. His interest in hosting technology company executives and giving them complements drastically contrasts some of his other remarks, which leaves some question as to where Donald Trump actually stands with the use of technology and the practices of technology companies.

During the height of the FBI vs. Apple battle, Donald Trump sided with the FBI during an interview with Fox and Friends. He stated “To think that Apple won’t allow us to get into her cellphone? Who do they think they are?”27 These comments along with his recent pick for National Security Advisor, Lt. Gen. H.R. McMaster—who was a welcomed addition to the Trump administration by various Republicans, including Senate Armed Forces Chairman John McCain (Republican-Arizona)—demonstrates that while Trump may have an interest in building relationships with technology companies to improve government, most historical indications point towards him pushing for increased government authority over them.

Policy Proposal:
The proposal of this policy is that the government partner with one or various technology companies and establish a “government approved” domain in their existing data centers. This government approved domain would be partially funded through nonrefundable tax credits provided to the technology company as a part of the deal. In return, the federal government would own all the data saved on that domain. Consumers will have the option when purchasing an Internet connected device which sends and stores data on the cloud to opt into having their data stored on the government approved servers. If they choose to opt in, the price of their device will be reduced through a rebate.

In order for this proposal to be enacted, there must first be legislation, passed by Congress that would allow for the tax credit for the technology companies and consumers. To ensure the highest possible chance for success, I propose that members of the Senate and House Judiciary Committees who are a part of the bipartisan encryption working group participate in the writing of the legislation. The tax credit, which would last for the next five years, would be capped at $25,000 for technology companies and $100 rebates for consumers. The tax credits would go into effect in the fiscal year (FY) immediately following the passing of the legislation and the building of the government owned environment. Based on the Republican majority in the House and the Senate, it is estimated that the legislation may be able to be passed in the next government FY, which starts on October 1st. 28

In order to make this offer attractive to the public, the government approved environment will function very similarly to the current/non-government owned environment with a

---

few exceptions. Users of the government domain will be given more storage capacity and storage duration than users who do not use the government domain. The same privacy laws will apply in both domains, except in respect to subpoenas. If a law enforcement agency or the government is granted a subpoena for an electronic device—say an Amazon Echo—the government has the right to access that user’s personal data with no additional permissions/requests required. This policy will allow technology companies to maintain transparency with their consumers, while providing the government with better odds of being able to access the information needed to solve violent crimes.

The tax credits and rebates will last for the next five years so that the government can measure effectiveness and cost benefits. The procurement of the environment and the partnership will be largely managed by the National Security Agency (NSA) and other government identified resources with the expertise to ensure that the environment is properly installed and maintained and that only technology companies who have met the requirements outlined in the legislation are eligible for the tax credit. In order to fund the tax credits and as a part of the legislation, Congress will need to provide funding from mandatory spending. In the first year of the proposed legislation, the budget for the tax credits and rebates should be $2 million, with the amount being split evenly among what is allotted for technology companies and consumers. This budget will allow for up to 40 technology companies and 10,000 consumers to participate within the first year. In following years, the budget should be increase by $2 million dollars each year, so that partnerships can be maintained and potential new partnerships can be formed but on a selected basis. In addition to the cost associated with the tax over the course of 5 years, the policy would cost the government $10 million. Under this proposal, the technology
company would still be responsible for the hardware and software associated with the environment, including physical and virtual security and 24/7 monitoring for vulnerabilities.

There are various goals associated with this policy proposal. The most important is to lower the amount of legal impediments that law enforcement officials must deal with when attempting to solve crimes. The policy proposal also aims to create a more collaborative relationship between the federal government and large technology companies, without the companies feeling as if the government is overstepping its legal reach, or creating a privacy issue between technology companies and their customers. This policy strives to make cooperating with the government as a private citizen easier and more transparent, as the government will have the right to view or investigate a consumer’s personal data only via a subpoena. Through the policy, it is also hoped that some of the speculation around the government’s reach into technology companies will be taken away.

**Policy Analysis:**
In the event this policy is successfully implemented and executed, it would be groundbreaking for collaboration between the federal government and private technology companies. While the federal government is known to use private contractors to host technology systems and storage environments, the government is typically creates the rules by which the contractor must design within. The main regulation being the Federal Information Security Management Act (FISMA). The private contractor must provide a data center that is compliant with FISMA generally before it can store federal data. Various IT controls that should be in place to ensure compliance are outlined by the
National Institute of Standards and Technology (NIST). Partnering with a technology company in the capacity outlined by this policy proposal would mean the technology company still would have the freedom to design the servers and devices in a way that moves with the fast pace of technology change and competing technologies designed by other companies. There would not be a requirement to comply with FISMA or other federal information technology protection acts. Thus, consumers who choose to use the government domain will not lose any of the functionality commonly associated with the device/devices they are accustom to from the company, and relations between the government and technology company and similar companies would improve, as a clear partnership and guidelines would exist. This would also allow the government to achieve the ultimate goal of this policy—to reduce the amount of time it takes for the government to obtain the information it needs from locked technology devices during a criminal investigation—without having to pass legislation on the matter of privacy directly, which could also be time consuming, as the legislation would have to go through various reviews and voting.

Technology companies may be receptive to this policy because it allows them to share the responsibility of the data with the government and data breaches are costly to correct. In an annual study completed by The Ponemon Institute in 2015, it was found that the cost of data breaches to a company is rising and that the average data breach costed a company over $3.8 million.  

Under the proposed policy, although the partnering technology company would be responsible for protecting the virtual and physical infrastructure, the government would own the data. This is important because in the event of a breach or loss of data by other means such as insider threat, the government would technically have ownership of the data. Thus, it would be mostly the government’s responsibility to fund any remediation activities, notify the affected public, and work to regain consumer trust, which is a huge cost benefit to technology companies. On the other hand, there is the government, which would incur additional costs for remediation in the event of a breach or loss of data.

However, since large scale data breaches generally occur less often than violent crimes, it may be beneficial for the government to take this risk. Most of the criminal cases where a locked technology device could serve as evidence involve extensive investigations.

According to the 2015 report released by Mother Jones, lengthy police investigations are paid for largely by the government and contribute to $12.8 million spent daily to cover gun related deaths and injuries, totaling around $229 billion a year.\(^3\) In comparison, the total cost associated with a large scale government breach—in this case the OPM breach—is expected to be $330 million through 2018.\(^4\)

While there are costs and responsibility advantages for technology companies, there are also multiple associated risks, including the potential for business and revenue loss in the event a privacy incident—even if only on the government domain—impacted the company’s cloud storage environment. The technology company would also have to spend some additional funding on marketing to ensure that sells representatives and


consumers are aware that they still over a domain that the government does not have ownership of, as it is likely that those who are not in favor of “big government” may not want to do business with a company where there are questions as to if the government owns their data.

This policy has the potential to cut down the time and effort in which it takes to solve crimes—which would lead to lower costs for the government—and create an unprecedented partnership with a technology company that could change the way the government interacts with the private technology industry without excesses overreach. The FBI paid over $1.3 million alone to hack an encrypted Apple iPhone during its investigation of the San Bernardino shooting suspect.\textsuperscript{33} The FBI also spent weeks trying to find a legal avenue that would force Apple to cooperate with unlocking the phone.\textsuperscript{34} Even with the potential benefits, this policy is not without risks and drawbacks. In addition to the cost of potentially having to recover from a data breach, under this policy, funding would be incorporated into the federal budget, which would cost the government millions. If citizens do not choose to opt into the program, this policy will not be successful and instead will have costed the government money with no real return on investment. It is likely that there will be many factors that play a role in a citizen’s decision on opting into such a program, including views on privacy and income. Those who disagree with current governmental practices to secure citizen’s personal data from devices are not likely to trust a program that gives the government ownership of their data. Additionally, those who can afford the price of the device without a discount have

\textsuperscript{33} Alfred NG, “FBI paid more than $1.3 million to hack into the San Bernardino terrorist’s iPhone—found no links to ISIS,” \textit{Daily News}, April 21, 2016, \url{http://www.nydailynews.com/news/national/fbi-paid-1-3-million-unlock-san-bernardino-iphone-article-1.2610445}

only the incentive of additional storage space at no additional cost to them, which is not likely to persuade the wealthiest citizens to opt in. It is also unlikely that those with criminal intentions will knowingly opt into this service, thus, there is the risk that none of the data that the government will own will be useful in criminal investigations.

The government will also have a huge role in how many people opt into the service, as it will be their responsibility to market the program to the right population—perhaps college students and those in the low middle and lower socioeconomic statuses—and gather their feedback to continuously upkeep the program over the five year implementation.

Likewise, if the program is successful at attracting citizens to opt into using the government domain and the amount of cloud storage purchased by the government is not enough to meet the demand, there is the potential for a failed roll out, which can have long term impacts on how receptive citizens are to the overall policy. This was demonstrated during the botched roll out of the Affordable Care Act, commonly referred to as Obama Care.

Another downside of this policy is the difficulty associated with data ownership delineation. One of the main highlights of the policy is that the government will own all data that is kept on the government domain. Thus, the government does not have to wait for external companies to respond to subpoenas or go through extensive litigation when a company does not want to release certain information citing privacy concerns. However, with maintenance and vulnerability management being the responsibility of the technology company, there could be instances where a failure on the side of the technology company leads to a breach or loss of data. For instance, if a firewall is not
using the latest patches or a piece of technology is running on a software version that is no longer supported, the storage service could be under attack. If some adversary effectively breaks into the system and comprises data, the government may argue that the technology company should be responsible for remediation and costs associated with informing and protecting the public, since it was their lack of action that left the system at an increased vulnerability level.

Another potential issue for the policy is that the success of the policy relies heavily upon the technology company with which the government choose to partner with to establish a government domain. If the company that the government choose to partner with is already actively involved in any litigation with the government or does anything that would require any sort of federal investigation, the government’s partnership could pose conflict of interest issues. Also, depending upon a sole technology company for the partnership could be risky for the government; if the technology company does not perform well during the five year timespan of the proposed policy and chooses to go out of business or downsize, government officials would have to determine next steps.

Ultimately, there is the possibility that this policy will end up costing the government more money than it saves, mostly because of the unknown variable of citizen opt in. More specifically, criminal and victim opt in. In the event those who commit crimes or those who will end up becoming victims of crime are not a part of the demographic of people who decide to opt into the program, the government will have spent money to build an environment that is a convenience for lower income families to be able to enjoy technologies that they may not have otherwise been able to afford with the aid of the
government. All the while, the government will still have to spend funding to investigate crimes where a locked piece of technology could provide evidence.

**Political Analysis:**
There is somewhat of a political divide on the matter of encryption, personal data privacy, and how much reach and oversight the government should have on those matters. Democrats and Republicans generally have different ideals—Democrats often being accused of being liberal and advocates for policies that assist the poor and middle class, while Republicans are often accused of being conservative and in favor of the interests of big businesses. However, the divide is smaller than it is on most other issues, as Democrats and Republicans seem to be closer than they are divided when it comes to the issue of encryption, personal data privacy, and the government’s reach.

Former President Obama stated that Democrats will “reject the false choice between privacy interests and keeping Americans safe”. 35 This is only slightly different from the stance that Republicans were taking around the same time this statement was made. During the 2016 Republican National Convention, the Republican Party took the platform that government should not become a “meddlesome monitor” in the technology industry, but acknowledges the need to be able to access encrypted information. Both the most recent former President and the current President have acknowledged the need for government to partner with the technology industry more in order to create a safer tech savvy nation. Towards the end of his second term, President Obama introduced the

---

Cybersecurity National Action Plan. As a part of the plan, the President proposed investing $19 billion in cybersecurity for the FY 2017 budget, as well as empower Americans to secure their online accounts through multi-factor authentication. Also proposed as a part of the action plan was a partnership with leading technology companies such as Google and Facebook to make securing the accounts of Americans easier and with companies like Venmo and PayPal to make online purchases more secure. The plan also introduced a new Federal position; the Federal Chief Information Security Officer which is designed to drive cybersecurity planning, policy, and implementation.36

From this plan laid out by President Obama (Democrat) and the large meeting President Trump (Republican) had with top technology company leaders as President Elect, it is clear that both major political parties see the need for collaboration between the Federal government and the technology industry, which works in favor of the proposed policy. Implementing a policy that would put such a collaboration in place stands to be beneficial to both President Obama and President Trump; as the vision that President Obama laid out is partially the inspiration behind the partnership policy and if successful, President Trump would be credited with seeing at least part of a revised plan with similar goals through. Even if the policy is not successful/widely accepted by the public, President Trump would still be in a favorable position, as he could blame the failure as one that was inherited by the work that President Obama already started and could use the lessons learned as the basis for follow up policies. Likewise, even if the policy is not fully successful, Democrats and President Obama will still be in favorable positons, as

Democrats will likely blame the lack of success on how President Trump chose to carry out the policy and still credit President Obama with being the visionary for the real need for a government that is more aware of technological advances. President Obama, who has already served two terms does not have much at stake politically, which is why the failure of this policy is not likely to negatively impact him.

Implementing this policy would help the United State to catch up to the standard that has been set by other nations, who are thought to be leaders on cybersecurity issues. The European Union (EU) has been a long time leader on matters of data protection and privacy. Their government has had data protection directives in place as early as 1995.37 While government oversight is not always welcomed by citizens, the EU’s strict policies and regulations, even when dealing internationally for business purposes have been well received by its citizens and data protection experts.

Another factor that works in favor of the proposed policy is the fact that so many Americans have fallen victim to personal data theft that is it likely that at least some of the public would be willing to support measure that allows the government to play a more proactive role in managing and protecting their personal data. In January of 2014, a Pew survey found that 18 percent of respondents had had important personal information stolen from them.38 In another survey conducted by the Pew Internet & American Life Project in 2013, 66 percent of adults said current privacy laws are “not good enough” to protect Internet users’ privacy. Having a policy in place that gives people like the 66

percent of those surveyed who want the government to have more involvement with their
data would at least provide a group of early adaptors who could help to enhance future
policy. However, if the execution of the policy is not a success, this benefit could quickly
turn into a political downside.

If the government is able to convince members of the public to opt into using a
government owned environment, it must be secure and personal data cannot be misused.
Following the OPM data breach in 2015, a survey conducted by Accenture found that
almost 75 percent of American citizens do not trust the government’s ability to keep their
information private and secure.39 The Director of the National Background Investigations
Bureau Charles Phalen also stated that “…we need to renew the faith of the American
public that we can protect their information”.40 While the government is already in such a
fragile state with public trust, implementing a policy that takes on ownership of personal
data is not likely to go over well with all Americans, especially those impacted by the
OPM data breach.

As previously mentioned, a major stakeholder in the technological partnership that would
make the proposed policy a reality is the technology company that would partner with the
government. While having an additional resource to share the burden of responsibility
with may be beneficial for technology companies, companies in Silicon Valley have
historically been against proposed government regulations that would enable the
government to have a say in how the company handles the data it collects. A prime

---

39 Joseph Marks, “OPM breach’s greatest damage was impact to US government’s reputation,” Nextgov, April 10, 2017,
http://www.nextgov.com/cybersecurity/2017/04/greatest-damage-opm-breach-was-governments-reputation/136902/

40 Joseph Marks, “OPM breach’s greatest damage was impact to US government’s reputation,” Nextgov, April 10, 2017,
http://www.nextgov.com/cybersecurity/2017/04/greatest-damage-opm-breach-was-governments-reputation/136902/
example of this would be Silicon Valley’s push back on The European Union’s proposed regulation called the Right to be Forgotten, which would require that certain personal information be wiped from the Internet and that companies not process or store a person’s personal data after a certain set of conditions have been met. Giving the government any control over what happens to data after it is collected using technologies developed under a specific business model for profit is not likely to be immediately adopted by the large technology companies who are key players in the market place the policy is attempting to gain footing in.

Even if technology executives are willing to take the risk of partnering with the government to implement such a policy, the failure of the policy could have huge implications on the American stock market and economy. According to an article released by Business Insider, the five most valuable public companies are all technology companies. If there was a decision to take on a partnership with the government which failed and resulted in public outrage, it is highly likely that stocks would drop, the company would lose money, and other technology companies would be impacted.

**Recommendation:**
Based on the constraints of the proposed policy and the analysis presented, it is my recommendation that the FBI Director present this policy to the President and push to have the legislation passed. Although the proposed policy would be costly to the government and present monetary risks should a data breach take place, it is important for the government to demonstrate its commitment to technology and progress the tools

---


42 Kif Leswing, “The 5 most valuable public companies are all tech companies,” Business Insider, August 1, 2016, [http://www.businessinsider.com/4-most-valuable-public-companies-all-tech-companies-2016-8](http://www.businessinsider.com/4-most-valuable-public-companies-all-tech-companies-2016-8)
available to law enforcement bodies such as the FBI to solve crimes. While the data 
shows that data breaches are on the rise, the data also shows an uptick in the use and 
purchase of smart devices. It is estimated that before 2020, more than 21.4 million smart 
speakers will have been sold in the United States.43 With so many cases already having 
evidence linked to technology, it is reasonable to anticipate that the number of cases that 
involve technology as evidence will increase in coming years.

Since a huge criticism from law enforcement of current laws is that they do not keep up 
with the change of technology, and the criticism from privacy advocates is that laws that 
are heavily relied upon to increase law enforcement’s chances of being able to obtain 
personal data from a technology device are outdated, vague, and being misinterpreted— 
such as the All Writs Act—it is in the best interest of the government to find common 
ground. Under this policy, the government would have another legal tool to lean on in 
order to expeditiously, fairly, and accurately investigate and solve crimes, which would 
address the concerns of both sides involved.

Furthermore, I believe the proper time to propose such a risky, yet much needed policy 
change is under a new administration, particularly the Trump Administration. President 
Trump has demonstrated interest in working closely with Technology companies and 
“draining the swamp”—or in other words moving away from traditional government 
decision makers and practices.44 With his strong private sector business acumen, I believe 
President Trump and his advisors will be in favor of such progressive legislation and will 
persuade members of Congress from the Republican Party to pass the bill.

44 Justin Worland, “Donald Trump Says he Still Wants to ‘Drain the Swamp’,” Time, December 22, 2016, 
http://time.com/4616679/donald-trump-drain-the-swamp/
Curriculum Vitae:
Chanel Outley was born on August 25th in the Washington, D.C. metropolitan area. After graduating from the Project Lead the Way pre engineering program at her high school, Chanel attended the Pennsylvania State University where she majored in Information Sciences and Technology with a concentration in design and development. After graduation, Chanel began work as a technology consultant with Deloitte working in the firm’s federal cybersecurity practice. Her passion for understanding the business/funding aspect of the policies that governed the decisions made by her federal clients lead her to pursue a Masters in Public Management from Johns Hopkins.