The Right to Withhold Services to the US Government for Protection of Civil Liberties

Josh Simon

On December 2nd, 2015, Syed Rizwan Farook and Tashfeen Malik coordinated a terrorist attack in San Bernardino which killed 14 people and injured 22. The iPhone belonging to Syed Farook, who died in a shootout after the attack, was recovered and the FBI obtained a search warrant for the phone as long as they could unlock it. However, without the passcode, they only had a limited number of attempts to access it before the phone became completely useless, prompting the FBI to request that Apple create a backdoor code so they could use the phone. Tim Cook refused to create this backdoor code despite the pressure from the government. In an email to his employees, Cook stated "This case is about much more than a single phone or a single investigation...At stake is the data security of hundreds of millions of law-abiding people and setting a dangerous precedent that threatens everyone's civil liberties." Sparking outrage from the victims and further pressure from the FBI, Cook continued to refuse to make the code in order to make sure it does not inevitably become a target for hackers.

The FBI did not have malicious intent with creating the backdoor code and simply want to provide the victims with a complete investigation *the guardian article*. Apple did initially comply and actively assisted the FBI by giving "unsolicited advice" such as trying to back up the phone or changing the iCloud password so the FBI then insisted on making a modified iOS without the password guess limit so the phone could be accessed with brute force: Apple dubbed this program GovtOS. Cook foresaw a request like this and had a meeting about the idea months before the request and decided it was something that should never be made. After the FBI obtained a court order from a federal judge requiring Apple to create this GovtOS under the All

Writs Act, Cook became enraged at how this could set a dangerous precedent for the act and would also create additional questions concerning existing privacy laws.

This case brings up the ethical dilemma of what constraints the government can have with the increasing amount of digital information that can be used and abused. Both sides of the case have an argument on why the backdoor code should or should not be created, but at what point is the FBI's request considered overreaching and what sort of precedent would this set for the existing data privacy laws and the future use of the All Writs Act? At what point is it considered an unreasonable withhold of information from the government? Is there a way to both protect civil liberties of the innocent users who could become collateral damage in the creation of GovtOS while also providing the victims of this attack and future attacks that hinge on data collection with a full investigation?

Data Privacy Problems

A dangerous repercussion of creating GovtOS would be the effect it would have on every Apple user since such a universal backdoor could be abused by the government or hackers who manage to get their hands on this software. Apple knows that this is a potential consequence of this action, which would make them worry about the privacy of the users and also make them knowingly have the potential of violating privacy laws.

Article 12 of the U.N Declaration of Human Rights (UDHU) which was proclaimed by the United Nations on December 10, 1948 states "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence… Everyone has the right to the protection of the law against such interference or attacks" *Michigan Law Review*. This builds on the existing Fourth Amendment of the constitution which protects from unlawful search and seizure *Constitution Citation* which was later expanded upon in Katz v. United States (1967)

to protect citizens from unlawful search and seizures anywhere a person has a reasonable expectation of privacy; such as their cell phone in which Apple has promised protection for*Michigan Law Review*.

Apple would not be able to ethically create this backdoor program due to the privacy agreement in their Privacy Impact Assessment (PIA). The PIA states "... we design our products and services according to the principle of privacy by default and collect only the minimum amount of data necessary to provide our users with a product or service… ensuring that data collected is used only for the intended lawful purposes" *Apple's PIA*. Creating the code means the government has control over the data and Apple will not have a say in what they do with it. Despite how the FBI assures that the data and program would never be misused, it is a risk that could not be taken within good conscience.

Chief Privacy Counselor of Apple Jane Horvath stated that the company does not support allowing law enforcement having elevated access to private data to solve crimes, not only because of the risk it poses to other Apple users, but because of the gratuitous nature of the evidence on the phone. She supports this argument by claiming that having this data is not going to be critical in solving issues such as terrorism *CNBC article*; although having the data in the phone would provide a more thorough investigation, it ultimately would not change the outcome of the case and simply having the program would present greater risks in the future. As the precedents and current privacy laws stand, it is not possible to create a backdoor code while knowing the potential risks this poses to any and all Apple product users.

Applying the All Writs Act of 1789

One of the most important factors in this case is the FBI's use of the All Writs Act of 1789. This act states "courts may issue all writs necessary or appropriate in aid of their

respective jurisdictions and agreeable to the usages and principles of law" *All writs citation*. The purpose of this act is to "provide federal courts with the 'power to issue appropriate writs in aid of their respective jurisdictions as conferred by other provisions of law'" *Nassau UBar Citation*. As Ahmed Ghappour of the University of California Hastings College of Law puts it, "if there isn't already a law or statute that deals with a specific issue, judges can evoke the All Writs Act of 1789. A writ… is a court order" *NPR citation*. In a customer letter following the ruling, Tim Cook stated that this use of the AWA would set a "dangerous precedent" as the definition of "agreeable to the usages and principles of law" could be read very loosely while also abusing the current absence of a specific law concerning universal backdoor codes. It brings up the question of why the request of the backdoor code was approved when the code violates the previously mentioned Article 12 of the UDHU, putting Apple users at risk of a data breach.

Ability to deny access to information

Apple did not have the code that the government was asking for but still had the means to make it to attain their desired evidence which is why the dilemma of creating a backdoor became controversial because those affected by the terrorist attack would desire any closure to the case that they can. Many considered it unreasonable to not provide the FBI with this information, but this creates the question of to what extent can a company withhold information and at what point is it truly an unethical decision to deny these requests?

A precedent for this dilemma can be seen in *New York Times Co. v. United States (1971)* revolving around the Pentagon Papers leak during the Nixon administration. Daniel Ellsberg largely opposed the Vietnam War and leaked the Pentagon Papers to the New York Times and the Washington Post who would go on to publish them. The government filed a lawsuit against both companies in the U.S district courts to halt the publication of the papers but the judges in both

cases ruled against the request and the case would eventually go to the Supreme Court where the majority voted that the government failed to meet the “heavy burden” of proof required for these restraints *Mtsu citation*.

This case shows the government trying to deny the First Amendment of the US Constitution by censoring the press, an abuse of power that was not approved by the courts. Louis Henkin of the University of Pennsylvania stated that this goes against the thinking of the authors of the Declaration of Independence and the Constitutional Fathers who saw sovereignty in the people and that “government governed with the consent of the governed” *UPenn citation*.

Despite all the controversy in this case, the leaking of the papers did very little to change public opinion on the war as it was already very unpopular by the time the papers were published. The damage of this case centers around the distrust and worsening public opinion of the US government. This can be seen in the sales of books documenting the Vietnam War with the New York Times selling millions of copies while the government official version only sold around 500 copies *mtsu*.

This all relates back to the necessity of information arguments of the Apple case and exposes unethical truths of practices from the US government. The New York Times case can be related to Jane Horvath’s claims that GovtOS would not help to solve terrorist attacks like the San Bernadino case or change the outcome or opinion on the attack, the same way that the Pentagon Papers would not change the trajectory of the war or drastically change the opinion of the war. Both cases show that the government is willing to compromise freedoms in order to protect their image in the public eye and do not follow the same principles of withholding information as companies. The government tried to withhold military information that would

have been eligible for public disclosure yet expects Apple to use their workers to create an unethical code to access information that has a privacy guarantee under US Law and Apple's promises to customers.

The Current State of the Law

Information being stored on electronic devices was very new going into the 21st century and has only become more advanced within the past two decades. The Internet of Things has made data much more accessible to companies and the US government, so there must be some sort of regulation on the use of this information in order to protect individual safety.

As it currently stands, there is no law concerning the creation of backdoor codes or the government having special permission to have 100% transparent access to any device. This was the basis of being able to use the All Writs Act despite the existing privacy laws which have seldom adapted to the advances in technology within the past decade. The conflict of interest between Apple, the FBI and victims of the San Bernardino attack, and general Apple product users shows a great need for the expansion of privacy laws to include restraints on what the government can ethically have access to while also incorporating the guidelines for all information-storing companies on what data is eligible for the government to request and at what point their refusal to cooperate is considered unethical.

Current privacy laws that have begun to incorporate technology include the E-Government Act of 2002, State Data Breach Notification Laws (beginning in 2003 with California), and the California Consumer Privacy Act (CCPA) of 2020. The E-Government Act's primary purpose is to "require federal agencies to conduct a 'privacy impact statement' (PIA)" *BJA*, The State Data Breach Notification Laws require businesses and state agencies to disclose when personal information is exposed in a data breach, and the CCPA is a state statute

intended to regulate how businesses handle the personal information of residents of the state of California *Michigan Law Review*. With the exception of the CCPA, these laws would leave the power of disseminating collected information in the hands of the companies that own the information. It is up to them to act ethically with this data and be able to report a well-received PIA; however it does not offer any protection from data requests from the US government. This absence of regulation would allow companies to abuse the data they collect unless they want to retain users, but also provides no protection from the requests of the US government if they choose to enact the All Writs Act where they deem necessary.

Creating Guidelines and Regulations

The CCPA is a good beginning to setting guidelines on the data that companies are able to collect which could also be expanded upon to include how this data can be distributed to other companies or the US government. The data collected can be both valuable and dangerous for the users, and it is important to make sure that this data is not abused by any source. The idea of the CCPA has begun to spread to states aside from California, such as the Consumer Data Protection Act (CDPA) which will go into effect in Virginia on January 1st, 2023.

The data collection restrictions expanding to the rest of the United States would be a start to solving the problem of what data can be ethically collected and disseminated to the government. This development of consumer privacy would include regulations against backdoor codes as they would be considered unethical and cannot be obtained via use of the All Writs Act, provide limits on what would be considered withholding evidence and information from the government that should be shared, and provide universal transparency to the users of certain technological devices on what is and is not collected and when it is or is not.

Conclusion

Despite both sides of the San Bernardino case having evidence to support their claims of either needing to create a dangerous code or refusing the code because it puts civil liberties at risk, the case overall showed the US government's need to adapt to more advanced data collection and provide transparent regulations on what is eligible for data collection and usage in the eyes of the law. The need for a Universal Consumer Privacy Act tackles the need of a specific privacy lat dealing with data. It eliminates the gray-area on what should or should not be requested by the government and prevents an abuse of power from the lack of regulation while also banning a company or the US government from having unfair or unlimited access to any person's devices without proper authorization, within the limits of universal technological limits. If technology one day advances to create a unique backdoor code for a specific device that cannot be used universally, then maybe the law could be expanded upon to allow the US government to access data on a device if they can provide a heavy burden of evidence that it is necessary to a case. As it stands currently, such a technological feat does not exist so a more pertinent regulation would have to ban the making of the backdoor code and only allow eligible evidence to be incorporated into cases.