The controversy on the extent of government surveillance: fbi versus unlocking sy...

Government

There’s a very controversial technology battle taking place that potentially could impact close to half of the American population. The FBI took Apple to court so that they could sue for the right to Apple’s software in order to view what all was on the San Bernardino shooter’s iPhone. Apple took a strong stance against the FBI with their biggest argument being that, “…unlocking one phone amounts to unlocking them all, equivalent to creating a master key capable of opening hundreds of millions of locks”(Hodson). After Apple did not comply with the FBI they hired outsourced hackers to break into Apple’s software to launch what is known as a “ brute force” password attack on Syed Farook’s iPhone 5. While this seems like just a tech savvy strategy for law enforcement to gain information on this specific perpetrator, it could be the beginning of a very disturbing violation of privacy. With this access to Apple’s software the government has the ability to hack into any iPhone’s data without the user having a clue as to what was going on.

To give a little backstory as to what exactly happened to cause this debate on December 2, 2015, Tashfeen Malik and Syed Farook, who happened to be a married couple, attacked a public health building during a holiday party where Farook was employed. The couple opened fire on his co-workers, killing 14 and injuring 22. Four hours after the attack, the couple was being pursued by law enforcement and was eventually gunned down. It was later discovered that the couple was sheltering home made bombs and thousands of bullets in their San Bernardino home. The two suspects were believed to be tied to either al-Qaeda or ISIS but these allegations were never confirmed. One day after the attack foreign terrorist group, ISIS, claimed that the couple were supporters of their terrorism but denied that they were actually

affiliated with their organization. This is when the US government took a stronger approach to find out what exactly motivated this couple to pursue this act of terrorism.

This truly was a tragedy and a day that will never be forgotten by the American people but we cannot and should not allow the government to invade the privacy of millions for the actions of two.

Apple and the Department of Justice spent 43 days in a very public legal battle over an order from the FBI. This order stated that Apple must help the FBI unlock an iPhone belonging to the San Bernardino terrorists. The problem that the FBI was facing was disabling a security feature that is built into the latest generation of iPhones. This feature has locked investigators out, leaving them unable to access the iPhones data. The security function would potentially erase all the iPhones data if investigators unsuccessfully guessed the password ten times.

On February sixteenth, the same day as the court order, Apple CEO Tim Cook responded with a thousand word letter to Apples customers. In this letter, Cook states that " The United States government had demanded that Apple take an unprecedented step, which threatened the security of Apple customers"(Cook, Tim). This letter caused a public uproar, bringing to light many constitutional and privacy concerns. Apple denounces the court order, and gives the following explanation. " There is a need, almost a necessity, for encryption. Smartphones have become an essential part of nearly every Americans life (Cook, Tim). Smartphones contain personal information, from private conversations and pictures to financial information. We can even be

tracked through our smartphones. It is vital that this data is protected from hackers and criminals who want to access our knowledge and private information without our permission. Apple believes that it is their duty to their customers to provide them with protection from these hackers.

Apple continues on to denounce the San Bernardino terrorist attack. It is important to note that Apple has previously complied with other requests by the FBI, but believes that this request is just too dangerous to create. The FBI had asked Apple to build a backdoor to the iPhone. Specifically, “ The government is requesting Apple to write brand new code that eliminates key features of iPhone security that protect us all. Essentially, the government is asking Apple to create a master key so that it can open a single phone” (Neal, Dave). The government may argue that this technology would be limited to this one San Bernardino case, but there is no way to guarantee that.

Within days a number of organizations and companies came to Apples support. On February seventeenth, the day after the initial court order, Privacy Supports held a rally outside the downtown San Francisco Apple store to protest the FBI’s request. Within a few more days Google, Facebook, and Twitter announced their support of Apples stance. On February 19th, the Department of Justice filed an order that would force Apple to comply. Apple responded by filing an opposition to the court order, and eventually the judge ruled against the department of justice stating that their lawyers failed to establish a good reasoning to enforce the All Writs Act, written in 1911. The government attempted to enforce a law that dates back to 1911, which

was nearly 70 years before the first personal computer and over 80 years before the first smartphone. This law essentially states that a court may issue all writs necessary in aid of their respective jurisdiction.

A few days after that ruling, and within 24 hours before a hearing, the justice department requested a postponement. They had found an alternate way to hack into the phone, through a third party. It was initially believed that a firm based in Israel was hired for the job. However, within weeks it had become clear that this information was false. Instead, the government had hired freelance hackers to extort the data from the terrorist’s iPhone.

The most common way to get into a phone secured by a password it by just guessing an infinite amount of combinations of passwords until you gain access to the phone. The reason why the FBI couldn’t guess the phone’s password was because of a setting that can be enabled on the device. This setting makes it possible that if the incorrect pin is entered a certain amount of times, all critical data on the iPhone would be deleted. So the FBI wanted Apple to disable this feature so that they could guess any number of combinations they chose. This “ backdoor” would mean new code was written and would compromise the iPhone’s encryption security. Apple’s CEO Tim Cook opposed the ruling saying “ We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely companies like Apple to protect their data.” This doesn’t necessarily mean in future cases courts will be

compelled to follow the ruling. Digital rights experts say this scenario raises the question who can make this type of demand? If the U. S. Government can force Apple to do this, why can't other governments?

The reason why it is so hard to decrypt an Apple iPhone is because when a new file is created on an iPhone, an app creates a new two hundred and fifty-six-bit key (per-file) and then hands it off to the hardware to encrypt while it is being written to memory. Then on top of that the " per-file" key is " wrapped" in one of several different class keys, depending on what type of file it is. To retrieve the file, the metadata is decrypted with the system key, which allows the per-file key to be seen wrapped and a notation on how it is protected. Then the per-file key is unwrapped with the class key. At this point the file can be handed off to the hardware engine to be decrypted to become a readable file again.

The two hundred and fifty-six-bit encryption is called Advanced Encryption Standard. This encryption is used by the United States government and worldwide. This type of encryption is not just a substitution or permutation, but rather, a combination of both. The block key for AES is at multiple of thirty two bits, being at least one hundred and twenty eight and at most two hundred and fifty six. AES works by using a matrix of bytes, which means the bites are organized by row and column for computation. The size represents how many cycles of transfer of plaintext (the regular input) into ciphertext (the encrypted ouput). It ranges from ten cycles for one hundred and twenty-eight bit keys to fourteen cycles for two hundred and fifty six bit keys. The way the encryption works is by deriving keys from the cipher key, then each

byte of the state is combined with a black of the key. Then bytes are substituted with each other non-linearly. Then the last three rows of the matrix are shifted a certain number of steps. The last round of movement is a mixing operation which mixes the columns by combining the bytes in each column. Lastly, it repeats the steps of substituting and shifting again, but not the mixing a second time. You can see how trying to get back to the original data would be hard, without knowing how many times the key tells you what bits are substituted with what, how much the rows are shifted, and what the four bytes were in each column combined to equal the mixed columns. It’s even more impossible, because this happens twice!

The first method the government took to try to crack the iPhone via a third party, because Apple wasn’t assisting them was to look for help from Cellebrite, an Isreali technology firm specializing in data extraction. The “ Universal Forensic Extraction Device” or UFED that they manufacture comes with various adapters and can force it’s way in to mobile phones. The device takes the data from computers or phones bit by bit and copies the whole data structure on to an usb memory stick or SD card.

It turns out though, that recent media is reporting that it wasn’t Cellebrite who cracked the phone, it was gray hat hackers. “ Gray hat” is the term to describe hackers who sell their discoveries and expertise, typically to government agencies and businesses. They consider their work to be a “ public service” The hired hackers apparently used a two-step process which involved first writing code that defeated the PIN number security features,

and then using at least one previously discovered software flaw to create hardware that cracked the phone

Just as we thought this case was over and the Apple vs. FBI debate would finally be at rest, another ruling comes up. This debate is not close to being over after Apple says that the FBI and other agencies have many other phones they would like to get unlocked including the latest hot topic in New York. This case is a now in the courts where the FBI is asking Apple for help, again, in unlocking an IPhone that belonged to someone who was arrested for drug trafficking. This is a case about an IPhone 5S as opposed to the IPhone 5C in the case with the terrorist. The IPhone 5S is a nicer phone that came out later and has a much stronger encryption so the hack that the FBI found earlier will not work on this phone.

For the FBI this means that they never really got any closer to finishing what they set out to do. (get a magic key to unlock every IPhone) They won the battle by cracking into the IPhone 5C, but lost the war because this hack only works on that one specific type of phone and will most likely be fixed soon since Apple seems confident that they can find out how their phone was hacked and patch it so that it cannot happen again. The FBI is just trying to do their job trying to protect us, but this is a battle between safety and privacy. How much privacy are we willing to give up to protect our safety?

Ultimately Apple is still going to have the FBI pressuring them and taking them to court to do something that they do not have the capability of doing. But they already “ won” the first case by not giving in and having the case dropped so it should get easier for them now. Also they make a good point

by saying that the FBI has already hacked into an IPhone without Apple's help so they do not need them. This is a debate that will war on with Apple and other companies claiming that the only way to keep people and their privacy safe would be to keep a strong unbreakable encryption.

What this argument means for other companies is that they need to start looking into their own encryptions. One example of this a app owned by Facebook called " Whatsapp". It is used by over a billion people sending messages, pictures, and videos. They saw what happened to Apple and decided to take their own action on encryptions. They hired a Coder and cryptographer to make their own securities where even their employees could not access the messages if they wanted to.

We have spent most of the time looking at the small scale of this debate, one single phone, but this case can have a huge effect in other ways. As already stated, a few celebrities had information hacked, what if apple creates a master key and it gets in the wrong hands. Hackers could get into the phones of the Senate, the Treasurer, or even the President. This makes the debate a national risk. As technology progresses, what if they could access our phones remotely, a lot of phones have personal or financial information such as banking information embedded in them, this could pose as a major threat to everyone.

What this whole argument means to us, as IPhone users, is that, for now, our private information is still safe. Even if someone here is involved in bad stuff Apple says that they couldn't do a wiretap on iMessage or even Facetime. This should make everyone feel confident that our phones and all the

information on them are still strongly encrypted and safe from everyone. Although we are now protected, we should still try to find additional preventive measures to take to keep our phones safe.