A history of data encryption, terrorists case and different views on data privacy...

Technology, Information Technology

In very recent events, Apple Inc., one of the largest technology brands in the world, has become the center of a heated debate on consumer data encryption. Revolving around the iPhone of the terrorist who led an attack at the Inland Regional Center in San Bernardino, California, this controversy has sparked a newfound public interest in data privacy, government access to data, and whether or not Apple should be forced to build a “ back door” into its mobile operating system, iOS for the FBI to utilize. In the following report, I will provide a brief history of data encryption, quickly summarize the terrorist case, and then proceed to analyze critical viewpoints from both ends of the spectrum. Finally, I will conclude with my own stance on the matter and provide information to back up my beliefs. This is a situation that affects every person who uses an Internet-connected device and it is crucial to understand how it impacts/could impact our everyday lives.

Introduction

Data encryption is the process of converting digital data into another form, called ciphertext. After this is completed, it is impossible to decipher unless a user has a decryption key (Rouse, 2014). Encryption has many uses, however its primary ones include keeping confidential files secure and out of the wrong hands, protecting online currency exchanges through credit cards, and preventing cyber-attacks.

In spite of the recent events in San Bernardino, data encryption has become a hot button issue for many. While the technology has been around for ages, it was not until this tragic event that the topic moved into the public spotlight. Thanks to the media, this issue did become radicalized, however it is important for consumers to educate themselves on the matter. Before someone could blink an eye, the entire situation grew into a heated political debate.

The main issue at hand was that one of the men who executed the terrorist attacks used an iPhone as his personal device. After the tragedy, the FBI wanted to gain access to the personal information on the device; however, they encountered a huge issue whilst attempting to do so. iOS, Apple’s mobile operating system, is pre-equipped with data encryption, so the FBI was unable to simply extract the data and view it on another device. In addition, they locked themselves out of the phone by incorrectly guessing the device passcode too many times and even managed to reset the user’s Apple ID password. The situation escalated very quickly and gained plenty of media attention from both sides (liberal/conservative).

After failing, the FBI turned to Apple for support on the issue but were respectfully declined. In an open letter from Apple CEO, Tim Cook (2016), stated that customer information needs. To be protected from hackers and criminals and that by compromising the security of our personal information they could put our personal safety at risk. He then proceeded to explain how Apple, although outraged by the terrorism, simply could not proceed further with the requests of the FBI. The United States government was requesting that Apple create a special version of its mobile operating system so that they would have a “ back door” into the iPhone. This poses a huge security risk because if that software were to get into the wrong hands, it could act as a master key, allowing anyone access to anybody’s phone.

In the following, I will be examining the following questions:

1. How long has data encryption been around, and why should individuals care about it?
2. What exactly are the details of this whole debate and why has it received so much media attention?
3. What was the aftermath of the case and what does it say about the current and future states of privacy?

San Bernardino

On Wednesday, December 2, 2016, three individuals who are now labeled radicalized terrorists, shot up a local state-run facility that serves people with developmental disabilities. Forty injuries were reported, sixteen of them being fatal. There was a police standoff with the suspects that eventually led to their arrest. President Obama stated that an FBI investigation was being initiated for this case and that it was a national concern. After charges were made, the FBI truly began their investigation.

On February 16 of the next year, a federal judge, Sheri Pym, demanded that Apple help the FBI by disabling a feature of iOS that disabled the terrorist’s iPhone after ten failed passcode attempts. A few hours later, Tim Cook published his letter saying that the request was “ chilling.” Hundreds of supporters held rallies in support of Apple’s stance, but three days later, the Department of Justice escalated the case in an attempt to force Apple to follow the government’s orders. Later, Apple then informed the media that the terrorist’s Apple ID password had been reset; thus eliminating any possibility of backing up the data to an external server (Weise, 2016).

For the next several days, Apple and the FBI went back and forth throwing hateful comments at one another. The FBI claimed that Apple was merely trying to pull a publicity stunt while the tech giant claimed that the government was putting customer’s privacy at risk with their requests. On February 25th, Apple filed an opposition to the court order and were given even more support by other tech companies such as Google and Twitter. A few more days pass and another request for an iPhone unlock emerges; naturally Apple denies it. On March 24th, a mere twenty-four hours before the official court hearing, the FBI asks for a postponement. In a dramatic turn of events, the FBI sought assistance from a third party who claimed that they had the ability to unlock the iPhone. Shortly after, the FBI dropped the case and said that they no longer needed assistance from Apple. (Weise, 2016)

“ It is hard to accept that secured systems could ever remain secured, since they are designed by us and therefore must be breakable by one of us, given enough time. Every human-engineered system must have a flaw, and it is only a matter of time before someone finds it (Vacca, 2013).

History of Data Encryption

The foundation for encryption, cryptography dates back around 3, 000 years ago in India and China. They would write messages using alphanumeric symbols and shift characters within the string of the message in a defined manner, known as shift cipher (Vacca, 2013). This paved the way for the encryption standards we have today. The Data Encryption Standard was developed by IBM in the early 1970s. It was once widely used by many and became a federal standard in 1976, but has since been retired due to its 56-bit key size being too small (Denning and Denning, 1998).

Whenever mobile devices became extremely popular, a new concern for privacy emerged. Worry over who has access to user data and what kind of data is being collected became part of everyday life. Perhaps one of the biggest concerns is that of location privacy. According to Wicker (2012), it has been confirmed that iPhones collect user location data in an effort to measure signal strength and availability of Wi-Fi hotspots. While this does contribute towards the advancement of mobile technologies, it does pose the issue of making users feel uncomfortable.

In September of 2014, Apple and Google stirred up some waves by enabling data encryption by default in the latest versions of iOS and Android. The two tech giants realized that this was a necessary step in making their customers feel secure in using their products and services. This was the first time a major change caused such controversy with the officials. According to Timberg and Miller (2014), FBI director James Comey heavily slammed Apple and Google for enabling a feature that made it nearly impossible for the government to easily access user data when they deemed necessary. Other comments made were extremely radicalized and known to cause a moral panic. John Escalante, the Chief of Detectives in Chicago, said that the average pedophile now cannot wait to get an iPhone. This was a cliché statement in the sense that the general public begins to protest at the slightest hint of child endangerment. Apple and Google have clearly not backed down on their beliefs since this occurrence and I highly doubt they will.

The Concern Surrounding the Debate

Many connected this case with the controversial Patriot Act that was passed in 2001. As Barney (2007) stated, the Patriot Act was often viewed as the end of civil liberties and started an era of unprecedented fear. There is a fine line between privacy and safety, and many felt that the FBI crossed it. On the opposing side of the government's actions, people's main argument was that by creating a backdoor to the iPhone would bring with it a whole slew of potential data threats. As stated by popular technology news source, Technobuffalo (2016) https://www. youtube. com/watch? v= QCZGqVyWbZE, the threat of an exploit and the possibility of a leak of the special version of iOS made for the FBI became very frightening. The government claimed that it would only be used for one case, but they already proved themselves wrong. According to Johnson (2016), hundreds of requests for iPhone unlocks flooded the FBI just weeks after Apple denied their request. Perhaps even more ironic is that after this whole scandal, according to Perez and Prokupecz (2016), the FBI did not recover any relevant information from the phone. The fact that the government is relying on a the All Writs Act, a law signed in around 300 years ago, for their main argument, is disturbing (Gross, 2016).

On the supporting side of the argument, the main arguments are those of Apple cooperating before in the past and people calling this is huge publicity stunt from the company. According to Harris (2016), Apple has unlocked iPhones for the government over seventy times in the past. What made this case different? Some individuals are upset more so because Apple has commented that it has the ability to extract data from the phone; they are just choosing not to do so for reasons that many believe to be unjustified. In addition, many feel that Apple is abusing this tragedy as a marketing scheme. According to Wyld (2009), " Prior research has shown that more trans- parent firms have higher growth rates, greater investment efficiency, and lower costs of capital." Many argue that Apple was merely trying to make itself seem more transparent in an effort to gain more customers and to make a heftier profit. Many believe that it is Apple's patriotic duty to stop the terrorists by revealing information possibly relating to future attacks. One has to ask the question of, " Would a terrorist really be that careless about leaving footprints?"

The Future of Our Data

Just days before writing this, new information and events have occurred relating to this case. After what seemed to be a huge loss for data encryption, there has been some good to come out of it all. According to Lecher (2016), the House of Representatives has approved a bill requiring emails for search warrants. This is a huge step in the right direction because the government is starting to treat people's online property the same as their physical property. With the majority of our information being digital nowadays, this is a crucial victory for the public.

Another great finding to emerge after this event was that fact that Apple has already patched the security hole used by the third party hired by the FBI to gain access to the terrorist's iPhone. Apparently the iPhone 5C in question was running iOS 7. 0 and therefore did not have data encryption enabled and also contained a glitch allowing anyone to bypass the lock screen. The FBI then tipped Apple of this security flaw. Thankfully Apple released a statement later acknowledging that this issue is no longer present in later versions of iOS and that users should not be worried.

Unfortunately, this case has also sparked some negative happenings as well. First, according to Lovejoy (2016), the FBI was recently issued a warrant that forced an iPhone user to unlock her device with her fingerprint. This is the first time this has ever happened in a federal case, and it certainty will not be the last. The law currently views fingerprints as real and physical evidence and therefore the authorities do not technically need a search warrant in order to request one (Lovejoy, 2016). This poses the concern of how much ownership of our data we truly have.

My Opinion on the Matter

While I realize that this assignment was not necessarily an opinion piece, I feel the need to state my beliefs regarding the whole case. After all, why else do people read articles surrounding these topics? I can summarize my opinions in three statements. Apple was in the right. The FBI does not understand the severity of the issue. People need to be aware of the information they are storing.

I will go down swinging, so to speak, defending Apple’s decision to not create a backdoor for the FBI. Apple is absolutely right, the unforeseeable future is too much of a risk surrounding these types of security breach requests. If this “ governmentOS” were to be leaked or stolen, it would essentially act as a master key in the real world. Anybody could gain access to any iPhone regardless of the security precautions they have taken. Even worse, imagine the horror if this operating system got transformed into a malicious software. Innocent users could have their entire data set compromised.

The FBI is not aware of the threat they posed to the American people. While they were simply trying to bring closure to the victims’ families and prevent future terrorist attacks, they wanted to do so in a way that completely violated privacy ethics and made many people lose even more faith in their government. Furthermore, the events that took place after the court ruling was dismissed further weakened the ties between big government and citizens.

Lastly, I would like to say that consumers need to be aware of the personal information that they are storing on their devices. Unless turned off, wireless backup is enabled by default on my smartphones. That data is stored in huge data centers and while they are under tight security and are encrypted, the personal data is still out there. People need to realize that every post, tweet, and picture is stored someone other than their local device and it may not necessarily be safe from prying eyes.

Final Thoughts and Conclusions

The Apple Vs. FBI case was one of the biggest controversies in the technology industry in quite some time. Breaching on ethically-questionable actions, the FBI asked the tech giant to perform a task that many viewed as a violation of civil liberties. There have been hours of debate over the topic, but the fact remains that just because we secure something with a password or pin number does not make it secure. Thankfully, data encryption standards have come into play and have enabled a lot of data protection that many take for granted. While I believe that Apple made the right decision in denying the government unauthorized access into the iPhone, there are surely those who disagree. I, for one, applaud Apple for taking a stance and preventing what could have become a grave danger to consumers’ data. A master key should never be made for cellular devices, no matter how severe the circumstances.