Privacy and individual rights: the issue of apple and the fbi

Abstract

This paper discusses the mass shooting of Inland Regional Center in San Bernardino, California by a man name Syed Farook and his wife Tashfeen Malik. It also explains the intense investigation that followed this terrible event. Despite the criminal act of these two individuals, privacy and individual rights were upheld by his phone manufacturer. I will discuss in detail the request for access to Syed's iPhone by the FBI to Apple and the response that was received.

Apple V. The FBI

The United States of America has been called many things over the decades but the one that comes to mind is " The land of the free". This country holds true to that saying to an extent. All countries must have rules and regulations to keep people inline and to prevent complete and total chaos. With that being said, at some point there comes a time where there has to be a determination outside of the law of what is ethically right and what is ethically wrong. Throughout history many people have fought and died to preserve the many freedoms that people in the United States enjoy today. Though many battles have been won, there are still threats that exist that prove that we as a country must remain aware and on guard against these enemies. The terrorist attacks of 9/11 were monumental in showing the American people that our freedom is not something that should be taken lightly. Since the attacks that day, 18 years ago, there have been 479 different jihadist terrorist related crimes charged in the United States (Bergen, 2019). Although all of those events have helped sharpen the United

States anti-terrorism laws and defenses, one terrorist event in those numbers have made Americans question certain laws and rights on which this country was built upon.

Syed Farook was an American citizen born on June 14 th , 1987 to Pakistani parents in Chicago, Illinois. Even though he was born in Chicago to Pakistani parents, he grew up in California. Throughout his life he was raised Muslim. This includes wearing traditional dress and attended religious services regularly. He attended California State University, San Bernardino and graduated with an Environmental Health Degree in 2010 (Ahmed, 2015). Syed took a job at the Inland Regional Center (IRC) in San Bernardino as an Environmental Health Specialist. Not long thereafter in 2011, Syed decided to become a radicalized Muslim by listening to online lectures and broadcast from the Al-Qaeda leader Anwar al-Awlaki. These lectures motivated Syed to commit an act of terror in the name of Jihad. In 2013, Syed met a woman online named Tashfeen Malik. Malik was also of Pakistani decent. The two met in person in Saudi Arabia and would commit themselves to jihad and martyrdom (Counter Extremism Project, n. d.). In 2014, Malik and Syed got married in California. This would allow her to have a fiancée Visa and stay in country as a legal resident of the United States.

On December 2 nd 2015, at a mandatory employee training located at the Inland Regional Center, employees gathered inside of a festive conference room socializing and sharing the Christmas holiday spirit. Among those employees was Syed Farook. It was reported by witnesses at the party that Syed came in, placed a package on the table and left as if he was angry

(Ahmed, 2015). Syed was angry that as a Muslim he was forced to be around a Christmas party when he was a Muslim. This was believed to be the event that triggered the events to follow. Syed left in a black SUV to pick up his wife Malik from home. The couple returned to the party dressed in all black tactical gear and began unloading countless shots from a high-powered AR-15 at the IRC employees. The spraying of bullets caused massive amounts of terror, death and injuries. This is exactly what the couple wanted. After Syed and Malik were finished shooting at the IRC, they headed home where they were intercepted by a tipped off police officer. A stand off shoot out ensued leaving both Syed and Malik fatally wounded. The terrorist shooting left 14 people dead and 22 injured. This tragic terrorist attack was considered the deadliest attack since the 9/11 terrorist attack in 2001. Attorney General Loretta Lynch made a statement saying “[The attack was carried out] with a single, repugnant purpose: to harm, frighten and intimidate anyone who believes in open and tolerant societies; in free and democratic governments, and in the right of every human being to live in peace, security and freedom.” (Los Angele Times, 2015).

All across the United States and especially in San Bernardino County, Americans were swept with fear and sadness that something like this had happened so close to home. Through this terribly difficult time, the county made arrangements to support the families as best they could. Liaisons were set up to provide services such as babysitting to allow families to plan for funerals, visiting victims in the hospital, attending funerals, and coordinating survivor gatherings (Aguilera, 2016). As one could imagine a massive amount of anger would follow directed at the Muslim community. Shortly

after the shooting the Muslims United for San Bernardino raised more than $100, 000 from Muslims donors across the US (Watanabe, 2015). Muslims all across the country felt a need to apologize publicly for this event. Muslims as a whole are not all terrorists. It’s the radicalized ones that give the entire religion a bad reputation. Its unfortunate that this is the way that society has turned to view the Muslim faith.

In picking up the pieces from this horrifying event, the police discovered that Syed was issued an Apple iPhone 5c from the IRC. Little did anyone know this phone would stir up court orders, legal battles, encryption technology discussions, and cost the government millions of dollars. This phone was a target for the FBI because of the information the phone could possibly contain. The most significant information that the phone could contain would be a list of other people involved in this event and possible other planned terrorist attacks. The possibility of this information created a storm of attention and efforts to get to this data ASAP. There was one thing that put this wave of effort at a complete stand still, a passcode. Syed enabled a security feature on the phone where if the passcode was input incorrectly 10 times the device would automatically erase all data stored on the phone. One would imagine that due to the severity of the need for this information, the manufacturer would aide in unlocking this phone to prevent any more tragic events and aide in the investigation. Unfortunately, the assistance requested by the FBI was denied by Apple.

If Apple were to agree to just give access to my personal phone, I would feel completely violated. When you buy a cellphone, it should become your private property just like anything else you purchase. If you were to buy a

home, the contractor doesn’t just tell people they can go inside because they feel the need to look for something. The same should apply to technology devices. I wouldn’t want my cellphone unlocked by authorities for an investigation due to my privacy. With that being said there is nothing on my phone that would make me a criminal nor have I been the suspect of a mass shooting. The point is that just about everyone in the country has a cellphone that contains personal photos, text messages, and browser activity that should be considered personal property and not subject to viewing by just any authority that wants access. That is until a person has committed a crime so despicable and horrific that obtaining access to information on their phone could possibly prevent further harm. In that scenario, the phone could contain information on more crimes that are planned and the people involved. At that point the privacy protection of the person should be surrendered and all information on the device be accessible by law enforcement agencies.

In the United States, a policing authority or government agency cannot just go through your property for any reason they choose. For example, if you are pulled over in your car and they suspect you have drugs in the car they cannot just search it because they think there is something there. They need your permission or a probable cause such as visible drugs or an alert by a drug dog. Citizens are protected by what is called the Fourth Amendment of the U. S. Constitution. This amendment protects citizens from unlawful searches of an individual’s property. The same amendment applies to digital information technology as well. When it comes to the issue with accessing Syed Farook’s phone, police had a legitimate reason to search the phone.

The FBI proceeded to obtain a warrant to search the phone. The warrant was easily obtained due to the manner of the case. There was one major problem that existed, encryption. The data on the phone was protected by a passcode. Since the only person that knew the phone passcode was deceased, the FBI had to resort to other measures to try to gain access. The director of the FBI James Comey was quoted saying " It is a big problem for law enforcement armed with a search warrant when you find a device that can't be opened even when a judge says there's probable cause to open it" (Moog, 2016). The first obvious stop would be the manufacturer of the phone, Apple. The FBI contacted Apple with a search warrant in hand only to be denied access. Apple told the FBI that due to its encryption technology it was unable to unlock the phone. The FBI director continued to address the issue of accessing the locked iPhone, " It affects our counterterrorism work.... we still have one of those killers' phones that we have not been able to open, and it's been over two months and we're still working on it." (Moog, 2016).

The Apple iPhone is one of the top selling phones due to cutting edge technology and features. Most people are not aware of the intense level of security that lays behind the user-friendly interface. Syed Farook's phone had a passcode set. This passcode would allow 10 attempts before wiping all data on the phone. This security feature is extremely useful in the event your phone is stolen and someone tries to get access to your data on the phone. This battle between the FBI and Apple not only proves that the security feature is efficient but it also doesn't have the ability to be bypassed by anyone, not even Apple themselves. Syed's phone was an iPhone 5c with iOS

8 loaded onto it. The updated security feature in iOS 8 was that it encrypted more data on your phone that usual. Apple also updated the policy in which they state the level of security installed on Apple products. “ Apple has updated its privacy policy as part of the rollout of iOS 8, announcing that devices with the latest version of the operating system installed can no longer be accessed by the company itself.” (Farviar, 2014). Encryption has been around for a long time. Now more than ever, there are constant evolving threats to digital privacy. This includes acts of spying, hacking and any kind of theft of private information stored on digital media. “ Encryption is the process of helping protect personal data by using a “ secret code” to scramble it so that it cannot be read by anyone who doesn’t have the code key.” (Symantec, n. d.).

Updates to iOS are released periodically with a package of performance enhancements, new features and security protection. Although these updates will keep your phone up to date with the latest and greatest software Apple has to offer, users may not want changes to their current user experience. In line with this, users have the option of automatic updates downloaded and installed without their knowing or only install updates when they want the new features and improvements. Many users have become suspicious of automatic updates since Apple was accused of slowing down older phones with its iOS updates. “ Apple’s admission caused some outrage online and raised a lot of questions. People have long believed the company hinders older devices to get customers to buy new models (something Apple has denied), and the criticism got fierce over Apple’s lack of transparency around its battery policies.” (Tibken, 2017). The purpose was to enhance

performance while the battery of older phones declined. Some could point this to a sales strategy to get users to purchase new phones. Regardless of the backlash of the updates, the main purpose is to keep devices protected from new security threats and vulnerabilities.

In response to Apple being ordered to unlock phones by the government, the company has aimed their security posture at making it absolutely impossible to break into the phones. The iOS Security is something that Apple has been very serious about over the years. It continues to advance as the entertainment features of the phone advance as well. Apple states that “ Only Apple can provide this comprehensive approach to security, because we create products with integrated hardware, software, and services.” (Apple, 2018). The security architecture can be broken down into three categories: System Security, Data Security, and App Security. Each of these areas of security have been developed to protect the user from many different angles. System Security starts at the hardware and iOS level. To make it secure, the device is verified each time the device is turned on. Safeguards such as strong passcode policies and other access features have been tightened up to ensure that only the owner of the phone has access to the phone. App Security uses a security model that verifies each application through a development program. Only apps that have passed through this development testing are allowed to be installed on the Apple devices. Lastly, the Data Security has been targeted by providing methods to protect data stored on the device at all times. The device has dedicated hardware to process performance and is locked down with AES-256 encryption right out of the box (Apple, 2018). With the combination of all these levels of security,

Apple has created an environment that has the user’s privacy and security at the forefront.

Apple has been a leader of user privacy security developed into their phones but there are other mobile providers that put security measures into their devices. The top two competitors to Apple in the arena of mobile phones are Samsung and Google. Samsung is a technology giant producing a full line of electronics. Their phones specifically run the Android OS which is created by Google. Samsung has stated that their device security posture is at the forefront of development just like Apple. “ At Samsung, we take security and privacy issues very seriously and we are doing our best to respond as quickly as possible. Securing your device and maintaining the trust you place in us is our top priority.” (Samsung, 2017). One difference between Apple and Samsung phones is the OS comes from another company. Apple creates the iOS and the phones that run it while Samsung makes phones and uses Android OS. Androids creator, Google, has implemented many security features to keep their OS secure as well. This includes regular security updates, vulnerability management, and encryption that goes down to the hardware level. One difference that stands out between the two is that one relies on open source code. “ Android devices are the opposite, relying on an open-source code, meaning that the owners of these devices can tinker with their phone’s and tablet’s operating systems.” (Rafter, n. d.). While this is a feature that makes Android so widely used, users have the ability to install and modify their phones out of this secure environment. The apps that can be download into the phone have not been put through an intense screening process like that of Apple. Users also have the ability to do their own

development within the device and create applications. With that being said, Android remains to be a secure OS by incorporating always running analysis and scanning, enforcement policies, platform security, and dedicated secure hardware elements (Android, n. d.). Chrome OS is also created by Google. This OS closely resembles Apple by providing a closed environment where not all applications can run on the device. Chrome comes with encryption, process sandboxing, automatic updates, and a non-optional security posture. Like both Android and iOS, Chrome OS has all the security features that make it difficult to compromise the privacy of the data on the phone. The difference that stood out to me about Chrome OS from the rest is that their updates are mandatory. There is no option to stop the update or prevent the download of the new OS once it has been pushed by Google.

All three of the operating systems are very secure and significantly reduce the chances of unauthorized access to the private data. From looking at all the specs of these three operating systems they all have their advantages and disadvantages. Focusing strictly on security, I would say that the safest operating system is iOS. The reason I believe it is the safest is because of the inability to change the root of the device. The phone is built to be locked down by design and to allow only know applications to be installed on the phone. This feature alone greatly reduces the possible threats to the phone. Customization of the phone is almost nonexistent due to the strict security policies. By blocking access to the root operation of the device, threats such as viruses and backdoors can’t open up the phone to make it vulnerable. “ Apple’s unprecedented control of the iPhone and iOS experience has meant

that most people receive and install software updates and security fixes. That’s critical, and it’s a major differentiator from Android.” (Eddy, 2019).

Tim Cook, Chief Executive Officer of Apple, is the target of the warrant from the FBI. The FBI took the legal route to present its case to Apple. They obtained a warrant along with stating that the All Writs Act (AWA) of 1789 forces Apple to assist in helping with the investigation. Basically, what the AWA does is use a judge’s court order to force actions within the scope of the law. In this case the AWA is used loosely due to there not being any specific law in place that would make Apple help the FBI. Apple said that the FBI is just using the AWA to justify the expansion of the department’s authority (Cook, 2016). A Justice department spokesperson responded by saying that “ The Constitution and the three branches of the federal government should be entrusted to strike the balance between each citizen’s right to privacy,” (Benner, 2016). This could be interpreted that the power of the government should choose whether or not a person has the right to privacy. I completely agree with the term that Apple used to classify this statement, “ Chilling”. Making these kinds of statements show that when it comes to something the government wants, they feel they are the ultimate power to make the decision with what is fair or not. Apple came back with a barrage of legal ammo to protect why they don’t have to assist in the investigation. For one, Apple stated that complying with the order would “ inflict significant harm — to civil liberties, society and national security — and would pre-empt decisions that should be left to the will of the people through laws passed by Congress and signed by the president.” (Benner, 2016). Another claim by Apple is that forcing the company to create software, writing code, is

violating the 1 st amendment of free speech. However, another report gave an opinion of what might be met with Apples free speech argument. “ A speech-rights argument from Apple, though, could be met with skepticism by the courts because computer code has become ubiquitous and underpins much of the U. S. economy.” (Ingram, 2016).

Tim Cook penned a letter to Apples customers explaining the situation of what exactly the FBI wanted and Apple’s clear stance on the situation. “ The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.” (Cook, 2016). This quote by Apples CEO sums up the letter in two sentences. Mr. Cook proceeds to explain how encryption of the iPhone was meant to protect the user’s information against hacking and criminal data theft. Encryption is extremely effective at doing its job. To make this point more effective Apple has claimed that the iPhone is so secure that not even Apple themselves have access. To many of the iPhone users this statement supports the huge need for privacy that so many people seek in this day in age. Just about everything that is done on a daily basis including banking, mobile payments and online shopping are done from a mobile device. “ M-commerce sales are predicted to make up 44. 7% of total US ecommerce sales in 2019, up from 39. 6% in 2018.” (Johnson, 2018). Those numbers are huge when you consider that people have the option to go the actual store or use many other methods to purchase items. I use my phone for over 50% of all of my purchases. Every time I make a purchase, I am concerned about send my credit card number out to the internet world. I think it is fantastic that big

companies such as Apple, Google, and Samsung are actively trying to make devices as safe as possible. Mr. Cook continues to the speak of how the company has already helped the FBI in this case and many others. “ When the FBI has requested data that’s in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we’ve offered our best ideas on a number of investigative options at their disposal.” (Cook, 2016). If I were a customer of Apple and I read this part of the letter, I would think that Apple has done as much as they possibly could to support the FBI. Since Apple at this time made it so clear that they are not opening the iPhone of Syed, this sentence says that they have indeed tried to help. The letter continues to explain how the little fix that the FBI is suggesting is way bigger than it seems when weighed against the consequences. “ The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals.” (Cook, 2016). Personally, I completely understand what Apple is saying to everyone. Yes, if Apple created an isolated hack just for this one instance of breaking into this terrorist’s phone, the FBI’s problem would be solved. But the bigger question would be, what about the millions of other users that use the same phone? Are they now at risk to have their phone opened by this tool once the FBI finds another phone they want opened? Where is the limit to how much or who uses the tool once it is created? All of these questions begin to unravel the very architecture that Apple has spent years to build. When tools of this nature are built, the value of them become extremely high. The value is so

high that I can’t think of how much a super power government would pay to have access to every single phone in their country. By the value of the tool being so high, the company would become a target for hacking thieves. Since technology has become so advance to protect us, it has also become advanced enough to steal from us. The National Security Agency (NSA) which is an agency in the Department of Defense that is responsible for protecting the absolute highest level of classified intelligence in the country has once been hacked. “ Chinese intelligence agents acquired National Security Agency hacking tools and repurposed them in 2016 to attack American allies and private companies in Europe and Asia, a leading cybersecurity firm has discovered.” (Perlroth, 2019). If the NSA is able to get hacked by China and have their hacking tools stolen, Apple would be a sitting duck in cyber space and surely be next in line for an attack. This event took place a few months ago and Tim Cook made a statement about this years ago in 2016. This proves that Mr. Cook was right on point when he said, “ And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.”. “ Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.” (Cook, 2016).

Mr. Cook finalizes his letter to the customers by stating how Apple has helped the FBI but they are now approaching an abuse of power and overstepping their authority. “ The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone’s microphone or camera without your

knowledge.” (Cook, 2016). This in my opinion is what drives home the reason Apple is denying to build the software that the FBI is requesting. As I mentioned before, if this one incident can make this secure tech company break protocols to build something to access data that they seek, what’s to say they will not use this as an opening to ask for more privacy invading tools. There is nothing stopping that from happening. However, if this incident was refused, it would erase the option of having Apple in the back pocket of the FBI. I completely agree that Mr. Cook is making the right move in regards to not obliging the FBI in their request.

This letter was absolutely necessary to be released to the public. The public opinion of Apple at the time concerning opening the phone was a common sense decision. Donald Trump, a presidential elect at the time, made the statement about Apple. “ Who do they think they are? They have to open it up,” Trump said. “ I think security, overall, we have to open it up and we have to use our heads. We have to use common sense.” (Matyszczyk, 2016). A terrorist used this iPhone to possibly put his associates that help with the planning of the San Bernardino shooting. Also, there could be information in there to possibly stop other mass murder events in the works. With a retaliation mind frame, this way of thinking seems fitting. If one of the victims were my family member, I would definitely want Apple to open the phone to prevent other people from feeling the hurt and pain that could come from such a loss. To truly access the situation one would need to take a large step back. Tim Cook did that in this case. It could be taken that Apple doesn’t care about the victims and are only thinking about their business. Whether that is true or not, the following quote shows that Mr. Cook did

express feelings toward the situation. “ We mourn the loss of life and want justice for all those whose lives were affected.”. “ We have no sympathy for terrorists.” (Cook, 2016). Overall the letter to the customers was written to show that they aren’t just being an unempathetic company just not wanting to help the US Government pursue terrorists and stop horrific events such as San Bernardino. In my opinion the message was well written and proved that there was more to Apples decision than met the eye.

There are many factors at hand here that make both sides of the argument make sense. It essentially boils down to which decision affects the most people. To be in favor of Mr. Cook’s side, I can think of many reasons to support that point of view. For one Mr. Cook said that unlocking this one phone could put many people at risk. This statement is proven to be true. Making a tool that put a backdoor into the Apple iPhone could be stolen and used to completely destroy the privacy of all the users of those phones. Secondly, the FBI tried to bully the company into doing what they wanted by using an act from 300 years ago. If this was to work that act could be used over and over until nothing is private when the FBI is concerned. Those two arguments in my opinion lead me to believe Mr. Cook made the right decision.

Looking at this decision from another angle, it makes perfect sense why none of that coding and privacy issues matter when people have died and many more lives are possibly at stake. Loss of life and public fear seem to be a legitimate reason to just create a backdoor, unlock the phone, and destroy the code that made the backdoor possible. The worst-case scenario could be that Apple codes the backdoor to be broken by an update if it was ever to

get out. This seems logical to a person that is not 100% savvy on how deep coding a program of this nature could go. As Mr. Cook pointed out in his letter to the customer, Apple had no idea how long it would take to reverse engineer their encryption techniques.

If Apple wins this back and forth with the FBI, it means a lot for all tech companies. Not only would it prevent the FBI from having technology companies at their disposal, it would give digital privacy a new name. It would show that the privacy of the people is valued. The FBI would likely go to another person outside of Apple to hack the device. Apple devices and clouds have been hacked before. A few years ago, a hacker was able to get into the clouds of celebrities and release their private pictures to the world. That proves the devices coming from Apple are not impenetrable. Apples response to this kind of blatant hacking of a device by the US Government could cause huge problems. It could actually make Apples argument completely useless. If Apple fought so hard to keep the software safe and then some third party just breaks in, that would be extremely embarrassing to Apple. Apple was the one that originally made this issue so big by outing the government. With that being said, they still made a statement about how large tech companies do hold their customers privacy very important.

If another person was to open up the Apple software what then? Well Apple has a few choices in the situation. One they could pay someone to come forward with the code used to break the iPhone open. I’m almost certain that this could turn to a bidder war between the US Government and Apple. The creator of the tool could cash in big. Once the tool is received Apple could break this tool with a patch pushed to all phones. Another option for Apple

could be to go back to the drawing board on a completely new hardened iOS. New chipsets and devices could be loaded with this software and sold to the public. However, both of these options would only be a temporary fix. Technology is something that is always evolving. There is no software that exists that cannot be hacked.

Just weeks after the FBI went around and round with trying to get Apple to assist with opening Syed Farook's iPhone, a third-party vendor was able to unlock the phone. As one could imagine the table had drastically turned on Apple. Now Apple needed the FBI's help to fix this vulnerability. Of course, the FBI had no interest in helping Apple. This flaw could be very useful to investigations to come because now the FBI could open any iPhone they wanted. Apple has continued to focus their development of future phones to have more advanced encryption. As time goes on, Apple has tried to be proactive at being cooperative in FBI investigations. On November 12, 2017 Devin Patrick Kelley killed 26 people inside of a Baptist Church in Texas. The shooter of this incident once again had a locked iPhone. Apple reached out to the FBI before being asked to show that they are not for terrorism. The FBI did not accept Apple's help. It is said that the FBI is using this situation to show how encryption is affecting police investigations and is an attempt to tear down the reputation of tech companies. " In other words, the FBI appears to be using this situation as another opportunity to paint the iPhone as antagonist to law enforcement procedures, in an apparent effort to drum up support for weakening tech industry encryption." (Statt, 2017).

The debate of privacy and Apple has spread to China. Apple iPhone users are now using an iCloud data server owned by the state. What this means is that

Apple partner Guizhou-Cloud Big Data (GCBD), which is known to have ties to the Chinese government, is now the keeper of the servers that hold users text messages, emails, and encryption keys (Hardwick, 2018). This sounds like some iCloud users in China will have less privacy on their accounts. However, users were given the option to switch to servers outside of China to avoid this issue of government possibly seeing their data. This move by the Chinese government is to grab ahold of data servers and hold them accountable to Chinese laws. At this point Apple can remain a secure company with their devices but must also warn customers that they have no control over the data on the Chinese servers.

This entire case involving the deadly mass shooting that killed 14 people has taught me a lot about being aware to signs of temperament changes in employees and people around me. The two terrorists, though painted as monster in the media and in my research paper, they were regular people. They had family, children, and friends. There is no common face for a terrorist now. I learned that Apple is more than a tech company. I personally don’t use Apple due to the customization available in Android OS. After doing the research on Apple, I am considering switching phones. My privacy, when it comes to my data, is very important. Not only do hackers want to get at your information, my own government finds it right to take away civil liberties when they see it to be fit. Of course there are scenarios where the reason can walk the line of invasion of privacy and public safety. As a community we can stay knowledgeable of our rights. Throughout all the information I presented, I feel that I am not surprised by any of it. It seems like every week there is another shooting spree from a distraught American

on other Americans. Terrorism lives locally and not just a foreign threat any more. I pray that some how we are able to reduce these shootings through providing the appropriate help to people with mental illnesses and better gun control through applicant screenings.

In conclusion, the United States is a country where many liberties and freedoms are enjoyed but at times are consistently threatened by different beliefs of a free world. Syed Farook and his wife Malik made a scar in the community of San Bernardino. In killing people to show allegiance to an Isis member, lives were destroyed and American policies were tested. One of the largest tech companies in the world was pulled into this situation because of the killer owning an iPhone. Although this devastating event was meant to tear apart American beliefs and spread fear, it failed at accomplishing its goal. San Bernardino remains strong today and the country has continued to try to better technology to intercept these plans before they can be put into action. This issue of mass shootings and digital privacy is far from over. My only hope is that as a country we continue to stand united against terrorist agendas and fight to keep our civil liberties of digital privacy throughout technical advancements that affect our everyday lives.

References

- Bergen, P. (2019). Terrorism in America after 9/11. Part I. Terrorism Cases: 2001-Today. Retrieved fromhttps://www. newamerica. org/in-depth/terrorism-in-america/part-i-overview-terrorism-cases-2001-today/

- Counter Terrorism Project. (n. d.). Syed Rizwan Farook – Overview. Retrieved fromhttps://www. counterextremism. com/extremists/syed-rizwan-farook
- Ahmed, S. (2015, December 4 th). Who were Syed Rizwan Farook and Tashfeen Malik? Retrieved fromhttps://www. cnn. com/2015/12/03/us/syed-farook-tashfeen-malik-mass-shooting-profile/index. html
- Los Angeles Times (2015, December 9 th). San Bernardino Shooting Updates. Retrieved fromhttps://www. latimes. com/local/lanow/la-me-ln-san-bernardino-shooting-live-updates-htmlstory. html
- Watanabe, T (2015, December 9 th). San Bernardino Shooting Updates. Retrieved fromhttps://www. latimes. com/local/lanow/la-me-ln-san-bernardino-shooting-live-updates-htmlstory. html
- Aguilera E. (2016, March 9 th). San Bernardino shooting: How the county helped victims move forward. Retrieved fromhttps://www. scpr. org/news/2016/03/09/58197/san-bernardino-shooting-how-the-county-helped-vict/
- Moog, T. (2016, February 17 th). Tim Cook denounces ‘ chilling’ FBI demands. Retrieved fromhttps://www. digitaltrends. com/mobile/judge-orders-apple-to-unlock-phone-of-san-bernardino-shooter/
- Symantec Corporation. (n. d.). Encryption: What it is and why it’s important. Retrieved fromhttps://us. norton. com/internetsecurity-privacy-what-is-encryption. html
- Farivar, C. (2014, September 17 th). Apple expands data encryption under iOS 8, making handover to cops moot. Retrieved

fromhttps://arstechnica. com/gadgets/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/

- Tibken, S. (2017, December 30 th). Apple’s iPhone slowdown: Your questions answered. Retrieved fromhttps://www. cnet. com/news/apple-is-slowing-down-older-iphones-batteries-faq/
- Apple. (2018). Overview – iOS Security. Retrieved fromhttps://www. apple. com/business/docs/resources/iOS_Security_Overview. pdf
- Samsung. (2017). Android Security Updates. Retrieved fromhttps://security. samsungmobile. com/workScope. smsb
- Rafter, D. (n. d.). Android vs. iOS: Which is more secure? Retrieved fromhttps://us. norton. com/internetsecurity-mobile-android-vs-ios-which-is-more-secure. html
- Android. (n. d.). Powerful security, built-in. Retrieved fromhttps://www. android. com/enterprise/security/
- Eddy, M. (2019, April 24 th). Security Watch: Android vs. iOS, Which Is More Secure? Retrieved fromhttps://www. pcmag. com/commentary/367918/securitywatch-android-vs-ios-which-is-more-secure
- Cook, T. (2016, February 16 th). A Message to Our Customers. Retrieved fromhttps://www. apple. com/customer-letter/
- Benner, K. Lichtblau, E. (2016, March 15 th). Apple and Justice Dept. Trade Barbs in iPhone Privacy Case. Retrieved fromhttps://www. nytimes. com/2016/03/16/technology/apple-court-filing-iphone-case. html

- Ingram, D. Levine, D. (2016, February 18th). Apple likely to invoke free-speech rights in encryption fight. Retrieved fromhttps://www. reuters. com/article/us-apple-encryption-freespeech-idUSKCN0VS025
- Johnson, T. (2018, November 26 th). M-commerce Statistics and Trends in 2019. Retrieved fromhttps://www. cpcstrategy. com/blog/2018/11/mcommerce-statistics/
- Matyszczyk, C. (2016, February 17 th). Donald Trump on Apple: ‘ Who do they think they are?’. Retrieved fromhttps://www. cnet. com/news/trump-apple-iphone-san-bernardino-encryption-fbi-terrorist/
- Statt, N. (2017, November 8 th). Apple says it immediately contacted FBI about unlocking Texas shooter’s iPhone. Retrieved fromhttps://www. theverge. com/2017/11/8/16626452/apple-fbi-texas-shooter-iphone-unlock-encryption-debate
- Hardwick, T. (2018, July 18 th). Apple’s Chinese iCloud Data Moved to Servers Managed by State-Owned Mobile Operator. Retrieved fromhttps://www. macrumors. com/2018/07/18/chinese-icloud-data-managed-by-telco/