Apple's Conundrum: Liberty vs. Security and Modern Terrorism

Tamra Blakely, Krista Elam, David Langley, Will Morrison, David Robinson
Livingston, AL 35470

Abstract

Questions regarding the immutability of liberty and security present challenges for modern society. Recently, issues of liberty versus security were questioned during the scenario involving the Federal Bureau of Investigation (FBI) and Apple Computer regarding iPhone access. In this case, Apple faced a pivotal decision wherein constitutional issues of liberty versus security were salient considerations of national security and the deterring and countering of terrorism. This paper provides a brief commentary regarding this scenario.

Keywords: Apple, FBI, liberty, security, national security, iPhone, terrorism

Introduction

Commensurate with the all-hazards perspective of homeland security and emergency management that is advocated by the U.S. Department of Homeland Security and departments of public safety among the states, threats against American society represent both natural and man-made hazards and origins (Doss, et al., 2016; Gallant, 2008). Within this dichotomy, terrorism is a concern of societies globally. It ranges from the incidents of lone wolf operators to the sophistication of organized factions (Doss, Jones, & Sumrall, 2010). Since the events of 9-11, which catapulted the U.S. into war, periodic reminders of the dangerousness of terrorism have affected domestic society. Examples include the 2009 Fort Hood massacre, 2013 Boston Marathon bombing, and the 2015 San Bernardino shooting incident. Historically, examples range from the 1960s church bombings in Birmingham, Alabama to the deeds of the Ku Klux Klan (Doss, 2011). Although none of these events rivaled 9-11 with respect to similar, mass quantities of thousands of casualties, they involved some considerations of planning, coordinating, controlling, and organizing. They also involved some consideration of technology for perpetrating the attack. During the aftermath of the 2015 San Bernardino event, a dispute was instigated between Apple Computer and the Federal Bureau of Investigation (FBI). This disagreement underlies an ongoing saga that involves considerations of the FBI accessing an Apple iPhone. A philosophical and political cornerstone of this saga involves foundational concerns of societal liberty versus security.

In 2012, a worldbank.org survey found that 75% of the world's population has access to a cell phone (Russell & Cieslik, 2012). With a cell phone a person can make calls to anywhere on earth, they can write emails, surf the web, and much more. The cell phone, and the fact that 75% of the world now accesses one, brings about many new frontiers which were unheard of even five years ago. The access that a cell phone provides its user is a great step in safety and communication, but what are some drawbacks of having such access in the palm of one's hands? Certainly, such devices are used for communication regarding both legal and illegal purposes (Doss, Glover, Goza, & Wigginton, 2015). Within the context of illegality, the motivations that underlie physical crime are mimicked within virtual environments (Doss, Henley, & McElreath, 2013a; 2013b). Thus, mobile phones and their affiliated technologies are subject to the whims of humans when planning, facilitating, and perpetrating terrorist acts (Sharma, 2005).

With the rise of cell phone usage, criminals and those alike have found a new way to steal information and cause trouble. Not only do they use it for criminal activities, but they also organize using the cell phone. So how does law enforcement prevent such things from occurring, or better yet, how do they use the criminal's cell phone to against them? The next question would be: should the government have access to a personal phone even if the owner of the phone is a supposed criminal or terrorist? These are all questions that wouldn't have ever came up even five years ago, but they are very important questions which will shape the freedoms of future Americans to come. The FBI's hacking into one of Apple's cell phones without permission from Apple or a federal warrant raises many eyebrows across the country. The debate of Liberty versus Security has been a debate since the birth of The United States of America. The founding fathers themselves pondered which is more important, liberty or security? According to Volokh (2014), Benjamin Franklin once said, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." Do the founding fathers same views apply to this situation or are their views not applicable, given that cell phones were not around during the lifetime of Benjamin Franklin? The basic premises of liberty versus security are just as important today as they were during the origin of the nation (McElreath, et al., 2013). This paper considers the debate and sheds light on some of the pressing issues which surround the FBI's access into Apple phones.

Liberty versus Security

In December of 2015 in San Bernardino, California, an attack led by Syed Rizwan Farook resulted in 14 deaths and huge controversy. The FBI demanded that Apple hack into the late terrorist's phone in hopes that unlocking it would reveal his associates or thwart future attacks. Apple refused claiming that this action would violate privacy; however, even Apple's top programmers were unable to crack the phone's password. The IPhone has a feature that allows it to permanently erase all data after only ten incorrect passwords. Knowing this, the FBI ordered Apple to create a new software to give them a backdoor into criminal's phones. Giving FBI a backdoor would also be giving highly experienced and potentially dangerous hackers a backdoor also. If a back-door exists among technological devices, then "all kinds of people can walk in. If the US government can demand access, the Chinese government can do so as well; Apple exercises a soft market power to resist authoritarian demands, but it won't have a leg to stand on if the government of its own country compels access" (Apple, 2016). The two parties resolved to take the case to court. The FBI hoped to win the case using the All Writs Act. Limer (2016) indicates that it allows federal judges to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." However, this was passed in 1789 and some might argue that this is too vague or outdated to apply to this case. Before this case even reached court, the FBI dropped the case and found a third party to unlock the phone on March 28, 2016. The controversy stems from the public feeling torn between security and privacy, but also because many people have iPhones that store their most personal information. They are also used as alarms, reminders, diaries, and more. For many people, it never leaves their side. Knowing that the FBI can easily hack the iPhone may deter quite a bit of Apple's customers. Apple might even resort to making new phones with tighter privacy measures because of this incident. When most people are asked whether they mind giving up some privacy to help catch terrorists, a Marcovici (2014) indicates that an analogous query is, "Do you want the government to engage in surveillance?" most people say yes. However, Marcovici (2013) indicates that "Do you want the government to engage in surveillance without a warrant or probable cause?" is really what is asked. Solove (2011) indicates that, "Rarely does protecting privacy involve totally banning a security measure," but somehow it seems that protecting security always involves losing privacy. Should we sacrifice privacy for security? No. The United States Constitution promises both liberty and justice for all.

Terrorism Threat

September 11th, 2011 could be known as the catalyst of modern terrorism in the United States. When two airplanes, American Airlines Boeing 767 flights 11 and 175, a third American Airlines flight 77 that crashed into the Pentagon, and the fourth plane, United flight 93, that crashed into a rural field in Western Pennsylvania, al-Qaeda committed one of the greatest acts of terrorism in the history of the United States. This single act took the lives of approximately 3,000 people, either directly or indirectly (McElreath, et al., 2014). However, within the U.S., terrorism can be dated back to the founding of the country. Terrorism is the use of violence and threats to intimidate or coerce, especially for political or religious purposes. Terrorism can come in many different forms. State, religious, pathological, nuclear, eco-, and narco-terrorism are just a few to name. During modern times, given the advent and proliferation of electronic technologies, cyberterrorism is a reality within society. Cyber terrorists use electronic resources and information technology to facilitate their attacks. Cyber terrorism is the use of computer-based attacks aimed at disabling vital computer systems so as to intimidate, coerce, or harm a government or section of the population.

Cyber terrorism is a massive threat to the nation and the world. For many people, common technology involves the use of a cell phone. Cell phones are the center of the Apple/FBI investigation. The FBI wanted Apple to create a "backdoor" entry into Apple's iPhone products. Of course, Apple refused, saying it was a threat to security and an infringement on our first and fourth amendment rights. From the perspective of the Fourth Amendment, various concerns of warrants and electronic boundaries are pertinent regarding digital devices (Yang, et al., 2016). The FBI wanted a way to break into a personal iPhone and see what information was inside. They wanted to see what possible terrorist affiliations may have been indicated by the data contained within the device.

Perspectives

Over the years, many questions have been raised by the actions of the government. The NSA and Snowden incident brought about the question of honesty from the supposed peace keepers of the United States citizens, whether or not to allow the government to allow access to our personal devices and information or not. The debate of security vs freedom is a very hot topic in American society right now. The recent case of Apple versus the FBI is one of the biggest debates trending right now. The FBI acquired an iPhone belonging to a terrorist that was connected with the San Bernardino terrorist attack on December 2, 2015. The FBI believed that it held valuable information that might lead to better understanding or deciphering further terrorist activities. This debate brings forth the idea of being able to gain access into anyone's personal devices on a whim. The underlying theme behind it all is: Should the government be allowed to "tap" into American citizen's personal devices and comb through their personal data, in the interest of national security? Or should privacy be held in higher importance over the possibility of stopping further attacks like the one in San Bernardino?

Generally, identifying and penetrating terrorist cells as well as obtaining organizational information are often challenging and daunting endeavors, and require much time, effort, and financial costs (Doss, Sumrall, McElreath, & Jones, 2013). The opportunity to examine and analyze the captured iPhone presents law enforcement organizations and the intelligence community with a potential treasure-trove of data that may contribute toward the successful identification and arrest of additional individuals. Potential benefits could be the sparing of human lives, thwarting of future incidents, and reduced time necessary for penetrating a terrorist network. Regardless of any considered benefits that may be derived from the captured cell phone, an age-old issue permeates the situation: liberty vs. security.

FBI

The FBI's stand in this whole matter, is that national security is of the utmost importance, and having the ability to tap into a personal device would give them an all new edge when it comes to detecting and preventing further terrorist attacks. The government cites the previous case, *United States vs. New York Telephone Company*, as the basis for its argument for the information that Apple is withholding, stating that under the All Writs Act that any company is required to give reasonable technical assistance to any government agency that expresses and proves a substantial need for it. The FBI took Apple to court because they refused to open up the iPhone to the FBI so that they could retrieve the information from it under the stand of privacy over security. The FBI thought that they needed apple's help to unlock the phone without losing all the information on it, they later proved, to themselves and Apple, that they didn't actually need Apple's help. Shortly before the original trial date, the FBI altered the time on their request. The reason was because they found a third party that was able to, reportedly, unlock the phone. While this settled things between Apple and the FBI, it only fanned the flames to a fire. This allowed the FBI to show criminals and terrorists alike that there was no infallible or impermeable security system and that, given enough time and money, any defense could be broken and any information that was highly sought after could be obtained at any time.

Apple

Apple's stance in this entire debate has been privacy over security. They feel as though they have an obligation to protect their customer's privacy and politely refused the FBI's request for access to the phone. Tim Cook, Apple's CEO, is urging the FBI and other federal agencies to find other ways of combating terrorist threats so that Apple does not have to break its customer's trust. In this scenario, Apple will most likely be seen as defenders of privacy and be seen as a more moral company, one that will fight for its customers. However, regardless of what Apple chose to do, their phones have supposedly been broken into, lowing the overall reliability and implied security of Apple products. This will surely drop demand for Apple's products, especially their iPhone lines, and cause the company some financial grief that they will have to frantically try to overcome. The FBI demanded that Apple write new software that would allow them access into any device that Apple produces. Apple promptly claimed that this would be a violation of the First Amendment which guarantees the freedom of speech to all US citizens.

Conclusion

Having access to information that may contribute toward abating calamities or terrorist activities is a legitimate concern within society. Within the emergency management cycle, deterring, avoiding, or mitigating the negative effects of a cataclysm are concerns for all levels of society (McElreath, et al, 2014a). Avoiding incidents, such as the San Bernadino shooting, is often facilitated through some consideration of what is known about the situation. Thus, within the context of the emergency management cycle, pertinent information from the iPhone may contribute toward deterring or avoiding future calamities. Given such considerations, the potential of using data to avoid future harm is a notion that is relevant within the context of the liberty versus security argument. The tragedy of 9-11 shows the dangerousness of terrorists who maximize opportunities to generate mass harm within society (McElreath, et al, 2014b).

Technology, in and of itself, may be viewed as a neutral tool (Liu, et al., 2016). It may either be used beneficially or malevolently per the intention and motivation of the human user (Liu, et al., 2016). This notion certainly applies to the technologies that are used by terrorists. Examining the content of the iPhone associated with the San Bernardino terrorists may yield critical data that contributed toward thwarting future incidents. Examined data may reveal additional contacts who have terrorist inclinations. As such, the iPhone has the potential of being a strong investigative resource whereby societal order may be maintained and terrorism may be deterred.

Many people question what the U.S. needs in order to safely and effectively perform counter-terrorism operations. Any number of state and non-state entities desire to harm American interests via terrorism, both domestically and globally (Doss, McElreath, et al., 2014b; Wigginton, et al., 2015). By stating that Apple's security was broken, the government has effectively made a target out of Apple, allowing hackers, both blue collar and white collar types worldwide, the confidence they might need in order to increase the quantities and levels of sophistication of attacks against Apple. All the while, the FBI has shown that the U.S. has the capabilities to challenge any system in the world. This ability should deter many would-be hackers and should send a clear message to any terrorist organization that they can be found. However, this might also frighten the American people. Knowing that their personal devices can be hacked into at any time will not reassure the people of their government's intent to only protect them from terrorists. The conspiracy theories have flown for decades about the unethical and immoral aspects of government surveillance, and this recent bout between Apple and the FBI will do nothing to put people's minds at ease.

To conclude, Apple experienced a dismal lose-lose situation with the FBI. Either Apple helps them break into the phone or they force the FBI to take matters into their own hands. If Apple were to help the FBI break into the phone, millions of users would question Apple and the security of their phones as well as the security of the customers themselves. However, on the flip side, when the FBI was able to hack into the phone, users of Apple phones questioned how safe their own phones were. If no one was supposed to be able to get into Apple phones, and it took the FBI just a matter of weeks, how soon could more phones be hacked in to? This is a scare for Apple because the security that they offer is now at jeopardy. With all of the new and improved ways of communication and terrorism rapidly growing, Apple will have more of these choices in the future. Apple will need to be clear to their customer that they ensure everyone's privacy, and only under dire circumstances will they provide assistance in this this kind of situation. Apple will not be able to please everyone, but when it comes to terrorism and making sure no one is harmed, that should be a top priority.

References

Apple. (2016). *Apple is right to challenge the FBI: But its case should only be the beginning of protecting our devices.* Retrieved from: http://www.thenation.com/article/apple-is-right-to-challenge-the-fbi/

Doss, D. (2011). *The Alabama anthology: Readings and commentaries in criminal justice*. Acton, MA: Copley Publishing.

Doss, D., Henley, R., McElreath, D., Lackey, H., Jones, D., Gokaraju, B., & Sumrall, W. (2016). Homeland security education: Managerial versus nonmanagerial market perspectives of an academic program. *Journal of Education for Business, 91*(4), 203-210.

Doss, D., Henley, R., & McElreath, D. (2013a). The Arizona border with Mexico: A Pearson correlation coefficient analysis of US border crossing data versus US reported cybercrime incidents for the period of 2001-2011. *International Journal of Social Science Research*, *1*(2013), 17.

Doss, D., Henley, R., & McElreath, D. (2013b). The California-Mexican border: Investigating Pearson correlation coefficient outcomes representing U.S. border crossing data versus U.S. reported cybercrime incidents during 2001-2011. *Mustang Journal of Law and Legal Studies, 4(*2013), 17-28.

Doss, D., Glover, W., Goza, R., & Wigginton, M. (2015). *The foundations of communication in criminal justice systems*. Boca Raton, FL: CRC Press.

Doss, D., Jones, D., & Sumrall, W. (2010, September). *A quantitative analysis of Animal Liberation Front incidents versus Earth Liberation Front incidents*. Paper presented to the annual meeting of the Southern Criminal Justice Association. Clearwater Beach, FL.

Doss, D., Sumrall, W., McElreath, D., & Jones, D. (2013). *Economic and financial analysis for criminal justice organizations*. Boca Raton, FL: CRC Press.

Gallant, B. (2008). *Essentials in emergency management: Including the all-hazards approach*. Lanham, MD: Rowman & Littlefield.

Limer, E. (2016). *Most useful podcast ever: Why is the FBI using a 227-year-old law against Apple?* Retrieved from: http://www.popularmechanics.com/technology/a19483/what-is-the-all-writs-act-of-1789-the-225-year-old-law-the-fbi-is-using-on-apple/

Liu, M., Yang, D., He, F., Li, M., & Doss, D. (2016). *Perspectives of technology and the instrumentalist paradigm. Proceedings of the Academy of Organizational Culture, Communications, and Conflict*, *21*(1), 34-38.

Marcovici, M. (2014). *You are the target: Or do you believe your government always watches the others?* Verlag: Books on Demand.

Marcovici, M. (2013). *The surveillance society: The security vs. privacy debate*. Verlag: Books on Demand.

McElreath, D., Doss, D., Jensen, C., Wigginton, M., Kennedy, R., Winter, K., Mongue, R., Bounds, J., & Estis-Sumerel, J. (2013). *Introduction to law enforcement*. Boca Raton, FL: CRC Press.

McElreath, D., Doss, D., Jensen, C., Wigginton, M., Nations, R., Van Slyke, J., & Nations, J. (2014a). *Foundations of emergency management*. Dubuque, IA: Kendall-Hunt.

McElreath, D., Jensen, C., Wigginton, M., Doss, D., Nations, R., & Van Slyke, J. (2014b). *Introduction to homeland security.* (2nd ed.). Boca Raton, FL: CRC Press.

Russell, C. & Cieslik N. (2012). *Mobile phone access reaches three quarters of the planet's population*. Retrieved from: http://www.worldbank.org/en/news/press-release/2012/07/17/mobile-phone-access-reaches-three-quarters-planets-population

Sharma, D.P. (2005). *The new terrorism: Islamist international*. New Delhi, India: APH Publishing.

Solove, D. (2011). *Why "security" keeps winning out over privacy*. Retrieved from: http://archives.californiaaviation.org/airport/msg47540.html

Volokh, E. (2014). *Liberty, safety, and Benjamin Franklin*. Retrieved from: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/11/liberty-safety-and-benjamin-franklin/

Wigginton, M., Burton, R., Jensen, C., McElreath, D., Mallory, S., & Doss, D. (2015). Al-Qods force: Iran's weapon of choice to export terrorism. *Journal of Policing, Intelligence, and Counter Terrorism*, *10*(2), 153-165.

Yang, D., He, F., Li, M., Liu, M., & Doss, D. (2016). Do you have anything to declare? Considerations of the Fourth Amendment and border searches. *Proceedings of the Academy of Organizational Culture, Communications, and Conflict*, *21*(1), 66-69.