Questioning Constitutionality: FBI vs. Apple Inc.

Gabriela M. Niemczyk,
Political Science, Level III,
McMaster University

"Questioning Constitutionality: FBI vs. Apple Inc." was originally published on MUJLP Forum on March 4, 2016.

MUJLP Forum is our flagship, bi-weekly, opinion editorial section showcasing the work of hired, undergraduate students at McMaster University.

A politically fuelled 'digital divide' has ignited as result of a recent ruling in which a federal judge in the US ordered Apple to help create a software that would allow the FBI to unlock one of the San Bernardino California shooters' iPhone.[1] The shooter, Farook Malik, attacked and killed 14 people at the Inland Regional Centre in San Bernardino, California in December, leaving behind an iPhone that the FBI claimed could provide valuable information surrounding the attack.[2] The case has sparked debate over the dichotomy of privacy and security, leading the US federal court to call into question the role of corporations as 'citizens,' with a moral responsibility in a new age of security. The divide in the debate surrounding corporate responsibility is evident as a recent Pew Research poll found that 51 percent of Americans think Apple, "Should unlock the iPhone to assist the ongoing FBI investigation," while 38 percent say Apple should not.[3]

Although the severity of the San Bernardo case should not be undermined, the selection of a politically charged circumstance by the FBI bears asking the questions: how does this case differentiate itself from past governmental encryption requests and is it a way for the executive branch to evoke a greater vulnerability of citizens in security measures? Apple CEO Tim Cook took to the internet to publish a strong statement on the matter, saying "The only way to get information — at least currently, the only way we know — would be to write a piece of software that we view as sort of the equivalent of cancer." Cook's main concern is the potential creation of a 'back door' that would allow governments, organizations, or any individuals with the software to gain access to Apple devices. In addition, if the court rules in favor of the FBI, the case would potentially grant law enforcement officials the authority to apply

[1]Lichtblau, E., & Benner, K. (2016, February 17). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. Retrieved February, 2016, from http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0
[2]Lichtblau, E., & Benner, K. (2016, February 17). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. Retrieved February, 2016, from http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0
[3]More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone. (2016, February 22). Retrieved February, 2016, from http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/

the ruling to similar cases in which encryption access has been requested.

The director of the FBI, James Coney, spoke out with a countervailing opinion, stating that. "That tension should not be resolved by corporations that sell stuff for a living. It also should not be resolved by the FBI, which investigates for a living." However, the arbitrary nature of the case has spurred further speculation about whether a legal precedent will be set. The right to judicial review in the case of privacy concerns has been maintained, yet, the issue of how much power the public is willing to give the executive branch in order to ensure public security continues.

Even if you do not agree with Apple's refusal to cooperate with the requests of law enforcement, Cook's instigation of a public debate has substantial value for recognizing that encryption law issues continue to emerge in the United States due to outdated legislation. The government currently holds the power to order corporations to aid in investigations if probable cause exists via a law that is over 200 years old (The All Rights Act). In a modern age with developing security threats, a temporal issue in the constitution is impeding much needed legislative changes.

As a result, Apple responded to a federal court order with a legal brief claiming that these outdated laws, coupled with law enforcement pressures have created an "unprecedented threat to constitutional rights." The US legal system needs to consider the realm of consumer privacy in order to bridge the existing dichotomy of personal privacy and state security. In this FBI-Apple dispute, the government's fight to maintain security should not be a means for constitutional rights to be violated. Although there is no doubt a value in corporate accountability in cases of state security, the executive branch should not be unrestricted in the judiciary steps it takes to monitor safety and security. Overall, no matter what side you stand on, Cook's encouragement of public opinion demonstrates the value of democratic engagement on a pressing political-technological issue.

On March 28th 2016, the day before Apple and FBI were set to meet in court, the US government filed a reading saying that they found a contractor to access the data "and therefore no longer require assistance from Apple."[4] Even more shockingly, the FBI did not outline what method was used to hack the device. The only indication of the technicality of this device was a claim by the FBI that this hacking method is only functional for the model of iPhone (iPhone 5C models running iOS 9), that belonged to the San Bernardino shooters. However, Apple's concern over personal privacy prevails, as the corporation wants to challenge the FBI to see if this device would work in a similar case they were asked to assist with that entailed unlocking a Brooklyn criminal's iPhone 6.

Two main issues remain following the case's conclusion. First, the ability of the government to find a method to get into the device – after claiming Apple was the only organ able to do so – leaves citizens vulnerable to how the government may use the device in the future. Next, as the FBI dropped their case against Apple, after finding a contractor to hack the device, the constitutional system did not have to settle the dispute.[5] The century old All Writes Act that allows the department of justice to authorize legal action in settling encryption cases such as FBI vs Apple will remain. An ambiguous end to the FBI and Apple dispute means that future legal action for encrypted devices and the adaptability of the All Rights Act will depend on subsequent cases. For now, outdated legislation will continue to teeter the line between personal privacy and national security.

[4]Brandom, Russell. "Apple's San Bernardino Fight Is Officially over as Government Confirms Working Attack." Http://www.theverge.com. March 28, 2016. Accessed April 29, 2016. http://www.theverge.com/2016/3/28/11317396/apple-fbi-encryption-vacate-iphone-order-san-bernardino.
[5]Zapotosky, Matt. "FBI Has Accessed San Bernardino Shooter's Phone without Apple's Help." Https://www.washingtonpost.com, March 28, 2016. Accessed April 29, 2016. https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html.