The FBI & Apple: Security vs. Privacy

In December 2015, the FBI attained the iPhone of one of the shooters in an ISIS-inspired terrorist attack that killed 14 people in San Bernardino, California. As part of the investigation, the FBI attempted to gain access to the data stored on the phone but was unable to penetrate its encryption software. Lawyers for the Obama administration approached Apple for assistance with unlocking the device, but negotiations soon broke down. The Justice Department then obtained a court order compelling Apple to help the FBI unlock the phone. Apple CEO, Timothy Cook, publicly challenged the court in an open letter, sparking an intense debate over the balance between maintaining national security and protecting user privacy.

Apple and its supporters, including top technology companies such as Google and Facebook, made the case on several fronts that the court order threatened the privacy of all individuals. First, according to Apple, the order effectively required the company to write code, violating its First Amendment right to free speech by forcing the company to "say" something it did not want to say. Previous court cases had already established computer code as legally protected speech. Second, such a backdoor, once created, could fall into the wrong hands and threaten the privacy of all iPhone owners. Finally, it would set a dangerous precedent; law enforcement could repeatedly require businesses such as Apple to assist in criminal investigations, effectively making technology companies an agent of government.

Representatives from both sides of the political aisle offered several arguments in favor of the Justice Department's efforts and against Apple's stance. Their central claim was that the U.S. legal system establishes constraints on the government's access to private information which prevent abuse of search and surveillance powers. At the same time, the law still allows authorities to gain access to information that facilitates prevention and prosecution of criminal activities, from terrorism to drug trafficking to child pornography. Critics of Apple also rejected the slippery slope argument on the grounds that, if Apple cooperated, it could safeguard the code it created and keep it out of the hands of others, including bad actors such as terrorists or criminal groups. Moreover, Apple was accused of being too interested in protecting its brand, and even unpatriotic for refusing to comply with the court order.

Ultimately, the FBI dropped the case because it was able to circumvent the encryption on the iPhone without Apple's help.

Discussion Questions:

1. What harms are potentially produced by the FBI's demand that Apple help it open an iPhone? What harms are potentially produced by Apple's refusal to help the FBI?

2. Do you think Apple had a moral obligation to help the FBI open the iPhone in this case because it involved terrorism and a mass shooting? What if the case involved a different type of criminal activity instead, such as drug trafficking? Explain your reasoning.

3. Apple argued that helping to open one iPhone would produce code that could be used to make private information on all iPhones vulnerable, not only to the American government but also to other foreign governments and criminal elements. Do you agree with Apple's "slippery slope" argument? Does avoiding these harms provide adequate justification for Apple's refusal to open the phone, even if it could reveal crucial information on the terrorist shooting?

4. Politicians from across the political spectrum, including President Obama and Senator Ted Cruz, argued that technology preventing government access to information should not exist. Do you agree with this limit on personal privacy? Why or why not?

5. Ultimately, the FBI gained access to the iPhone in question without the help of Apple. Does this development change your assessment of the ethical dimensions of Apple's refusal to help the FBI? Why or why not? Should the FBI share information on how it opened the iPhone with Apple so that it can patch the vulnerability? Explain your reasoning.

Resources:

Apple Fights Order to Unlock San Bernardino Gunman's iPhone
http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html

How they line up on Apple vs. the FBI
https://www.washingtonpost.com/graphics/business/fbi-apple/

Why Apple Is Right to Challenge an Order to Help the F.B.I.
http://www.nytimes.com/2016/02/19/opinion/why-apple-is-right-to-challenge-an-order-to-help-the-fbi.html

Apple's Rotten Core: CEO Tim Cook's Case for Not Aiding the FBI's Antiterror Effort Looks Worse than Ever
http://www.wsj.com/articles/apples-rotten-core-1456696736

Obama, at South by Southwest, Calls for Law Enforcement Access in Encryption Fight
http://www.nytimes.com/2016/03/12/us/politics/obama-heads-to-south-by-southwest-festival-to-talk-about-technology.html

U.S. Says It Has Unlocked iPhone Without Apple
http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news

Authors:
Robert Moser, Ph.D. and Patrick McDonald, Ph.D.
Department of Government
College of Liberal Arts
The University of Texas at Austin