Apple vs. FBI: Controversy Over Unlocking the iPhone

Denrique Preudhomme
writer@denrique.com

Introduction

Information Technology (IT) has become an integral part of criminal investigations. To verify the alibies of most criminal suspects, law enforcement and forensic professionals turn to data stored on telecommunication devices and computer hardware, as well as replay on information produced in “real-time” by embedded systems that could provide evidence to support alibies. Similarly, data from telecommunication devices, computer hardware, and embedded systems are commonly used as evidence in criminal investigations to convict criminal offenders. In the recent case of Apple, Inc. (Apple) vs. the Federal Bureau of Investigation (FBI); Apple’s refusal to unlock the iPhone of Syed Rizwan Farook, the San Bernardino gunman who shot and killed 14 people (Benner & Lichtblau, 2016), presented a matter of company ethics vs. law enforcement. The case incited a national debate, and while many believe Apple adhered to an ethical practice (to not compromise privacy to support a Federal investigation) most are left to wonder whether privacy or security is more important.

The Case of Apple vs. the FBI

In December 2015, shortly after the San Bernardino shooting, the FBI launched a federal investigation into Mr. Farook’s background to find a possible connection between Mr. Farook and another person who was investigated for terrorism a few years earlier. To retrieve possible data from Mr. Farook’s iPhone that could link him to a terrorist group, the FBI ordered Apple to unlock the iPhone. The FBI wanted to guard against lost data with Apple’s operating system (OS), which allows only 10 attempts to enter the right code to access the iPhone, and, “After 10 straight failures, Apple's auto-erase function kicks in, permanently wiping all information from the phone” (Botelho, Brascia, & Martinez, 2016). However, Apple refused to unlock the phone, citing that it would be a breach of customer privacy protection, and Apple would be forced to build

software, according to its CEO, Tim Cook, that "would have the potential to unlock any iPhone in someone's physical possession" (Pagliery, 2016).

The Issue of Apple's Privacy vs. the FBI's Security

Apple's commitment to Protecting Personal Information (PPI) against online and physical threats resulted in its stand against the government for democracy and freedom of speech. This was evident because, although the FBI exercised its authority over Apple to unlock Mr. Farook's iPhone, Apple exercised its legal obligation to protect their customers' privacy, and spoke freely to the media about their refusal to comply with the government.

With the enhancement of operating systems and software applications for smartphones, 43 percent of users (up by 9 percent from 2013) now believe that it is somewhat safe or very safe to access or store financial and personal data on smartphones (Economics Research and Data, 2016). This has forced smartphone manufacturers like Apple to safeguard against theft of Personally Identifiable Information (PII)[1], thus increasing their privacy policies.

In the case of the FBI's need to unlock Mr. Farook's iPhone for National security, it meant the government believed that the data on Mr. Farook's phone could compromise the safety of Americans. The government believed that the nation's *proverbial* PII had already been exposed, and the risk of further terrorist attacks was therefore probable.

Company Ethics and Law Enforcement

In general, companies are held to codes of ethics—specific business practices that govern their standards and behaviors. These are policies, procedures, and guidelines that define the way the organization is run. These codes of ethics are mainly in the best interest of getting and keeping clients/customers held by contractual agreements. The case of Apple vs. the FBI makes clients/consumers wonder whether

[1] PII is any piece of information that can potentially be used to identify, contact or locate a person. This includes a full name that is linked to social security number, bank account, credit card or driver's license number.

their contractual agreements can be overridden by law enforcement at any given time. Understandably, law enforcement has an obligation to protect the nation against criminal activities and terrorist attacks, but would they now be obligated to protect smartphones against hacking activities and cyber-attacks[2]—given their insistence to unlock private phones?

Conclusion

In March of this year, the California Justice Department announced that they found a way to successfully unlock Mr. Farook's iPhone (Benner & Lichtblau, 2016). It is unknown whether the data retrieved from the iPhone was useful to the FBI's investigation or whether the method used to unlock the phone was shared or would be ultimately shared with Apple. However, this raised new uncertainties about the strength of security in the iPhones, and moreover, concerns that the technique used to unlock the phone would be disclosed and made available to hackers.

Unfortunately, the government may have made things worse by unlocking Mr. Farook's iPhone, especially if whatever they created to hack the phone becomes available to hack millions of iPhones. Sadly, the FBI's order on Apple to unlock Mr. Farrok's iPhone may result in their being held responsible for compromising privacy while creating massive cyber-attack mayhem.

References

Benner, K., & Lichtblau, E. (2016, March 28). *Technology.* Retrieved from The New York Times: http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0

Botelho, G., Brascia, L., & Martinez, M. (2016, February 16). *Anger, praise for Apple for rebuffing FBI over San Bernardino killer's phone.* Retrieved from CNN: http://www.cnn.com/2016/02/18/us/san-bernardino-shooter-phone-apple-reaction/index.html

[2] Cyber-attacks are any type of aggressive attack carried out by an individual or organization that targets computer information systems, networks or personal computer devices by various means of malicious acts. These attacks are normally anonymous.

Economics Research and Data. (2016, May 19). Retrieved from Board of Governors of the Federal Reserve System: https://www.federalreserve.gov/econresdata/mobile-devices/2016-mobile-security-and-privacy.htm

Pagliery, J. (2016, February 19). *CNN Tech.* Retrieved from CNN Money: http://images.cnnmoney.com/2016/02/18/technology/apple-fbi-fight/index.html

