Simon Owens

Dr. Hwang Senior Seminar Ethics Essay

Apple Ordered to Unlock iPhone

The F.B.I. filed a lawsuit against Apple inc. for not helping them gain access to a terrorist's phone. This terrorist murdered several people and the contents of his phone could help arrest accomplices and possibly save future lives. Many have criticized Apple's actions in response to this horrific event. To understand why Apple is not helping the F.B.I., you must first understand what it takes to gain access to this phone and what would result to the software architecture, company, and users of Apple devices if they broke into the device or designed a backdoor.

There are two ways to gain access to the contents of the user's phone: break the device encryption or find a flaw in one of the interfaces. Apple devices running IOS 8.0 and later versions use AES 256-bit encryption. Apple does not have the key to this encryption system, so those wanting to break this must solve the discrete logarithm problem, which currently has no known vulnerabilities. Apple could get lucky, but it would likely take several years to break this encryption. So, the other option is to have Apple find a new vulnerability on its own system. Doing security testing on Apple's own products is completely legal and ethical, but not when the intent is to disclose personal data. Disclosing this user's data directly conflicts with Apple's Code of Conduct, "Supplier shall respect intellectual property rights and safeguard customer information."[1]. The Association for Computing Machinery (ACM)'s code of ethics, which many computer scientist follow, also clearly states, "2.03. Use the property of a client or employer

only in ways properly authorized, and with the client's or employer's knowledge and consent."[2]. I believe that the terrorist gave up their privacy rights when they decided to end another human's life. This opinion conflicts with these ethics, but these ethics were poorly developed because they are vague and don't cover many scenarios. The Apple software developers have a justifiable reason for refusing to help the F.B.I. because they've agreed and committed to these ethics. However, I believe that the Apple and the Software Engineers acted unethically. They should have realized their ethic's policies did not fit the situation. Helping preserve the murder's privacy did nothing for the average citizens privacy. Changing their ethics policies and testing for a vulnerability would have been more beneficial to the safety of the public. It would also be ethical for the F.B.I. to pay Apple for every hour they help, instead of just forcing this issue upon them. I believe it would be unethical for Apple to help the government break into any other devices unless there was conclusive evidence of them doing a harsh crime.

There is more to this lawsuit than just breaking into the phone. The U.S. government wants a way to gain access to Apple devices in the future for scenarios like this[4]. This is severely detrimental to the company and users. Creating a back door will not only will violate several user's privacy, but will also make the device much less secure, and cost Apple a large amount of development and sustainment money. Software Engineers are only supposed to "Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment"[2]. Leaving Apple's money aside, adding a backdoor increases the opportunities of other attackers. Attackers could attack the backdoor's interface, or the key management

system holding the user's private keys. Apple would have to implement some type of hardware or software SSH and key management system. The national vulnerability database reports there have been approximately 500 vulnerabilities that target or utilize this protocol, which shows there would be ongoing problems with Apple's backdoor solution[3]. Defense contractors, agencies, and allies also heavily use Apple devices for business/mission purposes so weakening their security could increase risk to the general public's safety. Implementing this solution would not be beneficial, ethical, or feasible at all.

Works Cited

[1] Supplier Code of Conduct [PDF]. (2015, January 1). Apple.

[2] Software Engineering Code. (2017, November 18). Retrieved from https://ethics.acm.org/code-of-ethics/software-engineering-code/

[3] Search Vulnerabilities. (n.d.). Retrieved September 21, 2018, from https://nvd.nist.gov/

[4] Markoff, J., Benner, K., & Chen, B. X. (2016, March 17). Apple Encryption Engineers, if Ordered to Unlock iPhone, Might Resist. Retrieved from https://www.nytimes.com/2016/03/18/technology/apple-encryption-engineers-if-ordered-to-unlock-iphone-might-resist.html