Intentional Weakening of Encryption: The Ethical Implications of Apple's Refusal to Create a "Backdoor"

Daniel Wong

Computer Science

May 2, 2018

CPE 300

Abstract

In December of 2015, two attackers killed 14 people in San Bernardino, California. The attackers destroyed their personal phones but their work iPhones were recovered by the FBI. However, the iPhone required a 4 digit pin to unlock it. The FBI requested data from Apple through valid subpoenas and search warrants. Then, the FBI requested Apple to engineer a version of the iPhone's operating system that would allow it to disable security features once installed. Apple declined this request stating that in the wrong hands, this software can have the potential to unlock any iPhone in someone's physical possesion. Was it ethical for Apple to refuse the FBI's request to create a "backdoor" to all iPhones? [**?**]

The United States goverment urged Apple to comply with the order after being opposed. The FBI stated they would allow Apple to destroy the software once the FBI was able to unlock and remove security features of the attacker's iPhone. Critics argued that Apple and technology companies alike should be held to the same provisions which made cellular encryption weak enough to allow officials to "tap" phone conversations as seen with A5/1. Others argue in defense of Apple stating that the intentional weakening of encrpytion will lead to easy access of the encrypted data. After A5/1 was used to encrypt phone conversations, security researchers were able to attack and easily decrpyt the conversations.

Contents

1 FACTS

In December 2015, Syed Rizwan Farook and another attacker killed 14 people and seriously injured 22 others. (CITE)After the attackers died, the FBI was able to recover Farook's work phone. The FBI had the National Security Agency attempt to unlock the iPhone. However, after a limited amount of incorrect attempts, the iPhone would automatically delete all of its data. With the NSA's absence of knowledge required to unlock the iPhone, the FBI turned to Apple and issued valid warrants and subpoenas to unlock the iPhone. Apple complied and gave all of the data and information available to them.[**?**]

The FBI needed Apple's help beecause the security settings on the iPhone lock may erase all of the phone's data if passwords are entered incorrectly ten times. The FBI requested Apple to engineer an operating system that could be installed onto the attacker's phone to disable critical safety features. This operating system would allow the FBI as many trials as necessary to break the 4 digit pin without erasing the phone's encrypted data. [**?**]

Apple refused the FBI's orders to create and install an operating system onto the San Bernardino shooter's iPhone to circumvent several important security features. Apple believes that building this operating system would create a backdoor and while the government may argue that its use would be limited to this case, there is no way to guarantee such control. [**?**]

In Apple's letter to their customers, they explain that the "'key' to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge." [**?**]

Apple and other technology companies alike believe that if Apple complied and created this "backdoor", it could set a very dangerous precedent. However, technology has become a crucial tool for some very dangerous individuals. Apple did not comply with the FBI's request to aid in unlocking the iPhone of the mass murderer and hundreds of other iPhones recovered during investigations of other serious crimes.

2 QUESTION

Was it ethically justifiable for Apple to refuse the FBI's request to create an operating system that would allow the FBI to unlock the attacker's iPhone?

3 SOCIAL IMPLICATIONS

Whether or not Apple's refusal to create a "backdoor" to unlock the phone of the San Bernardino shooter was ethical, there are numerous important considerations on its impact to the information able to be retrieved on personal phones.

When considering the implications of Apple's refusal, there are many concerns about public safety and preventing terrorism. Manhattan district attorney, Cyrus Vance, Jr., says he has 175 iPhones, with potential evidence from serious crimes, including murder, that he wants Apple to aid in opening.[3] Former FBI director, James Comey puts it, "Technology has become a tool of choice for some very dangerous people. Unfortunately, the law has not kept pace with technology and this disconnect has created significant public safety problems we have long described as 'going dark.'"[**?**] Thus, many people consider Apple's refusal to create this "backdoor" to be unjustifiable as it allows dangerous people to protect the information stored on their phone. As Republican Senator Lindsey Graham puts it during the GOP Debate in 2016, "Any system that would allow a terrorist to communicate with somebody inside our country and we can't find out what they're saying, is stupid."[**?**]

On the contrary, many argue that if this "backdoor" was built, it could lead to huge pri-

vacy concerns for the general public. John Oliver explains, "If you penetrate a safe, you have only penetrated that safe. But, a code to open one phone could be modified to work on many more phones."[?] Apple's CEO Tim Cook comments, "No one, I believe, would want a master-key built that would turn hundreds of millions of locks even if that key were in the possesion of the person that you trust the most; that key can be stolen... The only way we know to get additional information is to write a piece of software that is the software equivalent of cancer."[?] Thus, this order and compliance has many important implications regarding overall security of the public including their privacy and preventing terrorism.

4 LITERATURE REVIEW

4.1 Encryption: Last Week Tonight with John Oliver (HBO)

In an influential piece by John Oliver, he argues that whatever happens in this case will have huge rammifications. "Because, the FBI ultimately wants Apple and the entire technology industry to have an encryption always be weak enough that the company can access customer's data if law enforcement needs it." [?].

4.2 Matt Blaze: A key under the doormat isn't safe. Neither is an encryption backdoor.

Matt Blaze, an associate professor in the Computer Science Department at the University of Pennsylvania, "studies secure systems cryptography and the impact of technology on public policy." In 1993, the "Clipper Chip" was invented by the NSA and was as a device that would encrypt consumer computer's data but allow officials to access the data if needed. However, Matt Blaze was able to exploit the security flaws in the system. "Clipper's failure starkly demonstrated that cryptographic backdoors must be understood first as a technical problem... Clipper failed not because the NSA was incompetent, but because desigining a system with a backdoor was - and still is - fundamentally in conflict with basic security principles." [1]

4.3 Manhattan District Attorney: Smartphone Encryption and Public Safety

The Manhattan District Attorney's office believes that Apple and technology companies alike are making encryption decisions based on their business interests rather than considering the public's safety interests. "Without legislative action, these corporations will 'continue' to focus on customer and shareholder value,' while government entities 'will try to demonstrate the critical public safety price they (meaning we) pay for 'warrant-proof' platforms'." [3]

5 HOW THE SOFTWARE ENGINEERING CODE OF ETHICS APPLIES

The IEEE/ACM Softwar Engineering Code of Ethics considers software engineers to be those who "contribute by direct participation ... to the analysis, specification, design, development, ... and testing of software systems." [?] The operating system is the essential piece of software which interfaces between the user and hardware. "An operating system is a software which performs all the basic tasks like file management, (and) memory management" [?]

Thus, the employees at Apple whom are tasked with creating and maintaining critical safety features on the operating system are considered Software Engineers. These employees "shall adhere to the [Software Engineering] Code of Ethics and Professional Practice" [?] Software Engineers at Apple are the ones responsible for creating the operating system that fully encrypts

and protects the data stored on iPhones from becoming breached. The IEE/ACM Software Engineering Code of Ethics states that "Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm." [?] Is Apple instructing their software engineers to do good or cause harm?

6 ANALYSIS

6.1 Tenet 3.12: Respecting Privacy

Tenet 3.12 of the Software Engineering Code of Ethics requires software engineers to "Develop software ... that respect the privacy of those who will be affected by that software" [?]

6.1.1 Definitions

6.1.1.1 Respecting Privacy

To "respect" privacy is to protect the user's data from being authorized by other individuals. [?]

6.1.1.2 Actual or Potential Danger

6.1.1.3 Affected by Software

Those who will be affected by the software are generally the users or persons whom have their information stored by that software. Thus, if the information stored by the software became available, it would be a breach of personal privacy of those people.

6.1.2 Domain Specific Rule

In the domain of software operating systems, tenet 3.12 requires Apple software engineers to "Develop software that incorporates significant security measures to protect their users' information and data from being stolen." In regards to this case, the operating system that Apple developed uses encryption to protect the information of their iPhone users.

6.1.3 Discussion

6.1.3.1 Potential Risks

Encryption is the essential way of protecting data from being accessed without consent. In the letter to customers from Apple, "Smartphones ... have become an essential part of our lives. People use them to store an incredible amount of personal information ... All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission." [2] Apple engineers have a security system in place which encrypts the data on their phones. Thus, the information can not be accessed without entering the correct pin number to unlock the phone. In fact, Apple's security is so strong, in Manhattan District Attorney's office alone, 1445 out of 2000 total Apple iPhones obtained through court-ordered warrants are still locked. [?]

Apple argues that obliging with the FBI and creating an operating system to weaken the encryption only to be opened by certain individuals would never work. They believe that if this "backdoor" were to be built, then others will find ways to exploit and decrypt private information. "The government suggest this tool could only be used once ... Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge." [2]

In the 1990s, the Clipper Chip was introduced by the National Security Agency. "Clipper Chip, could be used in computers and other devices that needed to encrypt data. But there was a catch: Clipper-encoded data would include a copy of the key used to decrypt it ... If Clipper-encrypted data were encountered during an investigation, the key could be taken out of escrow and the data decrypted." [?] However, Matt Blaze, along with other security researchers were able to exploit the system. "Clipper failed not

because the NSA was incompetent, but because designing a system with a backdoor was - and still is - fundamentally in conflict with basic security principles." [?] Matt Blaze uses his knowledge with this particular case to argue that creating the "backdoor" requested by the FBI would compromise the safety and integrity of the data. "There is overwhelming consensus in the technical community that even ostensibly 'secure' backdoors put the systems into which they are incorporated at increased risk of outside attack and compromise." [?]

6.1.3.2 Respect of Privacy

The FBI is asking Apple to create a version of the iPhone operating system which would bypass critical security features to aid in recovering the encrypted data on the attacker's phone. "Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation."[?] The FBI is asking Apple to create a "key" that could unlock the specific iPhone. Apple states that it could be modified to open potentially every phone. Apple cites that it could set a dangerous precedent if they complied. "In the wrong hands, this software - which does not exist today - would have the potential to unluock any iPhone in someone's physical possession." [2] The Manhattan District Attorney states that if Apple created this software "backdoor", he would immediately ask Apple to aid his office in unlocking 175 iPhones. Thus, Apple's refusal to the order is due to their concern for users' privacy.

6.1.4 Conclusion

Tenet 3.12 of the Software Engineering Code Ethics requires software engineers to respect the privacy of those who will be affected by that software. As such, Apple's operating system encrypts users' information and protects it from becoming breached. As such, Apple was complying with Tenet 3.12. If Apple were to comply with the FBI and create an operating system to allow officials entry to encrypted iPhones, they would in direct conflict with Tenet 3.12. The domain specific rule, as derived from tenet 3.12 of the Software Engineering Code of Ethics, states that Apple should develop software that incorporates significant security measures to protect their users' information and data from being stolen. Because Apple did not build the system requested by the FBI, this rule was satisfied.

6.2 Tenet 1.03: Potential Danger

Tenet 1.03 of the Software Engineering Code of Ethics requires software engineers to approve software only if they have a well-founded belief that it is safe and does not ... diminish privacy." [?]

6.2.1 Definitions

6.2.1.1 Safe

"Safe" is defined as secure from danger, harm, or loss. [?] "Safe" is also defined as dependable or trustworthy [?]. These two definitions regards software to be safe if it is dependable and free from loss, danger, harm.

6.2.1.2 Software Privacy

"Privacy" is referred to as the freedom from unathorized disclosure of one's personal data or information; specifically as by a government, corporation or individual." [?]" This definition regards privacy as a matter to conceal one's information and to avoid revelation of such information to any particular organization or persons.

6.2.1.3 Diminishment

"Diminish" is defined as "to make or become less" [?]. We can simply define "not to diminish" as to "uphold".

To "disclose" is to "make known, reveal, or uncover" [?]. In the context of research, disclosure is closely related to informed consent,

which the Institutional Review Board Guidebook claims "assures that prospective human subjects will understand the nature of the research and can knowledgeably and voluntarily decide whether or not to participate" [**?**]. This definition regards prospective human subjects as the appropriate persons to which disclosure is directed. According to these definitions, to "disclose to appropriate persons" in research means to "make known to prospective human subjects (users)", and disclosure should include an opportunity to decide whether or not to participate in the research.

6.2.1.4 Actual or Potential Danger

"Danger" is defined as "liability or exposure to harm or injury; risk; peril" [**?**]. According to the Research Ethics Guidebook, "harm in social science research includes quite subjective evaluations like distress, embarrassment, and anxiety" [**?**]. This definition is relevant because social science is "the study of society and social behavior" [**?**], and Facebook's "emotional contagion" study "tested whether exposure to emotions led people to change their own posting behaviors" [**?**]. Therefore, "actual or potential danger" may be defined as "potential risk of distress, embarrassment, or anxiety".

6.2.1.5 Reasonable Belief

Reasonable belief may be defined as "hav[ing] knowledge of facts which, although not amounting to direct knowledge, would cause a reasonable person, knowing the same facts, to reasonably conclude the same thing" [**?**]. In other words, reasonable belief requires evidence, but not necessarily proof. To "reasonably believe", then, means to "have evidence to believe".

6.2.2 Domain Specific Rule

In the domain of internet research, tenet 1.04 requires Facebook's software engineers to "make known to users ... any potential risk of distress, embarrassment, or anxiety to the user ... that they have evidence to believe is associated with the Facebook news feed algorithm."

6.2.3 Discussion

6.2.3.1 Potential Risks

One major defense of Facebook is Tal Yarkoni's "In Defense of Facebook" article, which questions whether the "emotional contagion" experiment was any different from routine updates to Facebook. Yarkoni argues that "every single change Facebook makes to the site alters the user experience", and that these updates are made in the interest of improving the user experience [**?**]. Michelle Meyer agrees, arguing that the "emotional contagion" experiment was ultimately designed to improve the user experience, and that it did not "mess with people's minds" any more than Facebook usually does [**?**].

It is important to note, however, that the "emotional contagion" experiment was not conducted as a routine update to the system; it was designed to test "whether emotional contagion occurs outside of in-person interaction between individuals" [**?**]. Adam Kramer, one of the study's authors, stated that the researchers' "goal was never to upset anyone" [**?**]. The intentions of the study, however, are irrelevant to the potential for harm, which may have been necessary for the experiment to yield beneficial results. Kramer goes on to acknowledge that the study resulted in harm to the subjects: "the research benefits of the paper may not have justified all of [the] *anxiety*" [emphasis added]. Did the researchers have evidence to believe that the changes made for the experiment might cause anxiety before the study was conducted?

The paper on the study makes references to previous studies on "emotional contagion": "Emotional contagion is well established in laboratory experiments, with people transferring positive and *negative emotions* to others. Data from a large real-world social network, collected over a 20-y period suggests that longer-lasting moods (e.g., *depression*, happiness) can be transferred through networks" [emphasis added] [**?**]. These

references are clear acknowledgments that the phenomenon of "emotional contagion" has been demonstrated to include the spreading of negative emotions (including the anxiety that Kramer acknowledged). As the study was designed to examine "emotional contagion" via Facebook News Feeds, the researchers must have considered the possibility that negative emotions could be successfully spread during the experiment. Therefore, the studies cited in the paper constitute sufficient evidence for the potential risk of negative emotions, including anxiety, associated with the software relevant to the experiment.

6.2.3.2 Making Risks Known

If the researchers had sufficient evidence for potential risk, did they make these risks known to the subjects of the experiment?

As previously mentioned, disclosure is an important component of informed consent [**?**]. The researchers state that because they did not personally see any user data, the experiment "was consistent with Facebooks Data Use Policy, to which all users agree prior to creating an account on Facebook, constituting informed consent" [**?**]. James Grimmelmann agrees that this is "a meaningful way of avoiding privacy harms", which is a "principle risk" in observational studies [**?**]. However, he goes on to point out that the "emotional contagion" study was an experimental study, which carries more potential risks than just privacy risks. Indeed, the paper does not directly address other potential risks associated with informed consent, including the risk of distress, embarrassment, or anxiety.

If the researchers claim that Facebook's Data Use Policy constitutes informed consent, does it also address these risks? The policy states that Facebook "may use the information [it] receive about [users]: ... for internal operations, including troubleshooting, data analysis, testing, *research* and service improvement" [emphasis added] [**?**]. However, Kashmir Hill points out that the term "research" was added four months after the study was conducted [**?**]. This means that the Data Use Policy could not have been considered notification of participation in the study at the time it was conducted. As many critics point out, Facebook did not provide any explicit notification of participation in the study, and it was conducted without the subjects' knowledge [**?**] [**?**] [**?**] [**?**]. Therefore, the subjects could not have been aware of any potential risks associated with the experiment, since they were not even aware that they were subjects of an experiment in the first place.

6.2.4 Conclusion

The researchers behind Facebook's "emotional contagion" study had evidence to believe in potential risks of anxiety to human subjects associated with the software used in the experiment. The domain specific rule above, derived from tenet 1.04 of the Software Engineering Code of Ethics, states that they were required to make these risks known to the participants of the experiment. Because participation in the study was not made known to the subjects, they could not have been aware of these potential risks, and this rule was not satisfied.

References

[1] A key under the doormat isn't safe. neither is an encryption backdoor. https : / / www . washingtonpost . com / news / in-theory / wp / 2015 / 12 / 15 / how-the-nsa-tried-to-build-safe-encryption-but-failed/?utm_term=.1632699b8130.

[2] Cook, T. A message to our customers. https://www.apple.com/customer-letter/, Feb 2016. Letter to Apple customers about what the FBI wants from Apple and what they have and will do.

[3] Office, M. D. A. Manhattan district attorney's office on : Smartphone encryption and public safety. https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf, Nov 2017. Manhattan District Attorney's Office in regards to the current state of smartphone encryption.