Class Directed Case Study (Group 1)

Members: Minhee Kwon, Deki Namgyal, Christina N Nwachukwu, Ihor Mulyarchuk, Qilan Lao, Nadrat Rafa

Overview:
Using the assigned case study:

- Summarize the case study and highlight the issues to be addressed
- Engage the class in a deconstruction of the case and a resolution
- Gain consensus of the class or delineate the alternatives and create a framework to evaluate alternatives

Objectives:

- To summarize a document with the intent of using it to persuade someone to take action
- To persuade by using summary as evidence that action should be taken

Deliverables:

- A set of notes and discussion questions that could be used to run a class about the case study
- A summary of the case and its alternatives with a best choice scenario

Notes:

- Submit all documents
- We will be using your notes, discussion questions and summaries in class

Discussion Question:

1. How can we get into one's phone without risking the privacy of everyone else?
2. Is this course of action benefiting Apple?
3. Is this course of action benefiting the US government?
4. How will this affect Apple's stance on consumer privacy?
5. How will it affect the right of the consumers to protect their privacy?
6. Is it a danger of National Security or Personal Privacy?
7. Should there be a point of compromise? Or no compromise at all?

Summary:

A shooting took place in San Bernandino where a married couple killed 14 and wounded 21 at the husband's work- holiday party. There were many versions of why the accident happened and if it was a thoroughly planned terror attack. It was believed that new details could have been revealed if the FBI had access to the attackers' iPhones.

The Federal Bureau of Investigation requested that Apple provide "appropriate technical assistance" to help them unlock the terrorist's iPhone 5. However, Apple's CEO Tim Cook refused to give even one-time access to the suspect's smartphones, claiming that sharing their customers' personal data violates the company's digital privacy policy. Apple asserts that giving login information to even one person will allow the government to create a system that automatically generates passcodes for every user. Therefore, it would have the power to reach into anyone's device to capture their data. In addition to this, the FBI requested Apple to create software (backdoor) that would decrypt any locked iPhone that is confiscated from terror crime suspects.

On one hand, it seems that the U.S. government's intent is to protect the citizens, on the other hand, Apple is also protecting the customers by giving them a sense of privacy and not sharing their personal information. Thus, the ethical dilemma of "right-versus-right" arises. The ethical dilemma from the case study is making a choice between public/ national safety and personal/ individual privacy.

Tim Cook chose to protect the Apple brand and uphold their policy to protect the customer's data. The backdoor request by the FBI involves Apple creating a new IOS to circumvent certain security features on the iPhone allowing the device to be unlocked by a 3rd party. Although there is a claim by the government that this backdoor access will be limited to this case, it is safe

to say that if the need arises to unlock another device, they will undoubtedly make use of this opportunity. If Apple allows access based on the FBI's request, it will not only question Apple's data privacy policy, but other companies may also face similar requests for data vulnerabilities and design flaws in their products in the future. It could also result in a series of civil cases on privacy infringements as we know it only takes probable cause for security institutions to get warrants for carrying out a search, it therefore begs to question if this access would not be abused and wrongly enforced.

At present, more and more consumers pay attention to personal privacy, as such devices and data security are regarded by Apple as one of the keys selling points of its products. Creating backdoor access would leave Apple devices with an immediate vulnerability that could be exploited and put the privacy of every user at risk. As Cook explained, "You can't have a back door that's only for the good guys."