Name: Atmik Ajoy SRN: PES1201800189

Assignment: Privacy Versus Safety? - Apply Case Study

Q1. If you were in Cook's shoes, would you comply with the court order to help the FBI access the data on the iPhone used in the San Bernardino shooting? Why or why not?

No, If I were in Cook's shoes I would not comply with the court order to help the FBI access data on the Iphone used in the SanBernardino shooting. While it is a sensitive subject and a very delicate and nuanced one, I believe that what Cook did was the best possible course of action. On surface level, it seems almost intuitive to provide all help and to comply with said court order, however if we were to think about it a little more, not only would that move compromise the whole business model apple bases itself and markets its products on, but it would also lead to catastrophic implications. I will be outlining why in the succeeding paragraph.

Firstly, Customers all around the globe would lose all faith in Apple as a company. Apple thrived itself on being one of the only tech companies that really respect people's privacy and didn't look at their data without their consent. We clearly see this from the launch of the iphone 6S (that had enhanced security features and encryption updates) and their continual development of security in their iOS rollouts. With continual iterations of them telling the world that there was no "Backdoor" to enter through , support for this court order would invalidate everything they claimed to be private about their phone, thereby putting them in a tough spot as an electronics provider.

Secondly and most importantly, the court order implied that apple was meant to "software engineer" the phone such that they should be able to not only increase the number of attempts (from to 10), reduce the waiting time between wrong passcodes but also develop new software from their end that helps the fbi break into the phone by force. This would be now possible with the 2 former features removed as while it is time consuming, it would be an iterative program trying 6^6 combinations. This is especially harmful as once a technology like that is developed, all Apple's security measures they implement till date are null and void. This is because their encryption was based off the fact that the user passcode is taken into consideration to generate the key along with a specific hardware component. The moment we know the passcode we know everything and have access to all the data of that user. This technology would break all apples security measures and would as tim cook said be "technological cancer". Hackers would relentlessly try to get this software and there is a slippery slope for where to apply it or not as currently at the time apple also had 13 other pending requests to open apple phones for other crimes in new york city. If they comply with this request for the san

Bernardino shooting, where does this end?. It is better to not have the technology exist in the first place than to have such harmful and detrimental technology exist and keep it at risk or being misused.

Hence i believe that as Cook i too would not comply with the court order.

Q2. What are Apple's responsibilities for public safety?

As a tech giant in the modern world, Apple has responsibilities in public safety. Usually when a law enforcement agency serves an order to a company to co-operate in retrieving data from a locked device, said company obliges, but this wasn't the case with apple. Apple created levels of encryption and security that pitted personal privacy against public safety at times forgoing its responsibility for public safety.

Accessing key data in ongoing police investigations became a major topic of contention in the matter of apples responsibility towards public safety as the new york police department had about 72 apple devices out of 97 that they couldn't get into as apple had not created a mechanism for government agencies to snoop data on citizens phone without the passcode. This is probably one major responsibility to public safety that apple does have, which is being able to allow government agencies to access data of perpetrators or accused criminals in cases, as since a lot of data of users is stored on their devices, it becomes crucial in differentiating between whether a person is accused, innocent or guilty. This hinders public safety as guilty criminals aren't getting what they deserve. Additionally in some extreme cases like the San Bernardino shooting it becomes of utmost public safety that Apple discloses/helps in disclosing the information on the shooters phone, but refusal to do so results in hindering public safety.

On the flip side, it does help in enforcing public safety as it gives users the utmost privacy. By doing this criminals also cannot access any user data and cannot take advantage of any citizen that way, cannot sell information on the black market (like in target cyber attack). This "Hyper Encryption" that Apple has to enforce privacy also helps as mentioned before in attacks from hackers in turn preventing the exploitation of user data. For example, it is this increased privacy that allows Apple to hold 800 million itunes accounts information and not have the risk of an information leak.

Q3: What are Apple's responsibilities for customer privacy? Does Cook have additional responsibilities to take into account in this situation? If so, what are they?

The first and foremost responsibility apple has in terms of customer privacy is that customer data should not be given out unless and until consented upon. This means that data that the customer has stored on their device / cloud should not be accessible by anyone apart from said customer unless and until they give specific permission stating otherwise. There are several implications of this including the fact that the government should not be able to spy on its citizens' data without consent, tech companies shouldnt and cannot have monopoly over users' most sensitive data.

On their website they state that they do not provide any information to any law enforcement agency unless and until it is absolutely necessary and even so they provide the narrowest amount possible. Similarly as stated in the case study, Apple encrypts messages and data stored on device/cloud using a key that is specific to each device depending on the passcode used and the hardware unique number of the device, hence apple themselves cannot read the data unless they know the passcode.

Aforementioned are the main responsibilities that apple has for customer privacy, but while taking into account these responsibilities during this situation (assuming the situation is the san berdinano shooting), there are not additional responsibilities that cook needs to take into account, a hard stance is the best stance in this case. As mentioned in a previous answer, development of such software that acts like a master key into all apple devices is very detrimental to mankind and any malicious source could use it to bring any government to its knees. The thought of development of such a resource only comes into picture of there are additional responsibilities tied in , situation based. The reason additionally is because statistically only a fraction of users are criminals using this for malicious purposes, so skimping on user privacy for that small fraction is not ideal and additionally skimping on user privacy as mentioned in previous answer could lead to worse public safety hazards.

Hence a hard stance is the best one, and the responsibilities are non fluctuational and neither are they situation based.

Q4: Does your answer to providing access vary with the government agency or national government requesting the data? Why or why not?

No, providing information about Apple users to a third party does not depend on the party at all, it is morally and ethically incorrect to provide private user information to any third party. Mostly because this distinction is a very grey area and there is not a clear line between who to give and who not to provide a date.

For example, in the case of robberies and crimes providing crucial data to law enforcement agencies sounds like a good idea however if this data is being provided to those agencies, then the CIA, intelligence agencies of other countries, other governments come knocking on the door asking for access citing seemingly valid reasons to have access to said data. There is no end to the requests and no clear distinction as to who to give the data to and who not to give the data to. This is one of the major reasons why providing access to data does not vary with government agencies.

In addition to this, it is also imperative to note that in oppressive regimes and failing states, this privacy acts like a safety blanket against voices of dissent. It is imperative that government agencies in said areas do not get access to this data, especially in the case of areas where wild violations of humanitarian rights happen. This privacy provided in these regions is the simple help between life and death for many of the citizens hence providing the information to anyone at all would be very harmful and not ideal.

Hence providing access to citizen information is not remotely dependent on what government agency is requesting it.

Q5: Is there a way for Cook to resolve the apparent tension among these various responsibilities?

The responsibilities of Cook are very varied and go across a wide spectrum mainly related to topics of public safety and customer privacy, and mostly having to balance the two. And as expected there is high tension between these facets of his responsibilities and relieving them is presented as something harder to achieve than individually satisfying the responsibilities. Let's summarize the responsibilities individually as mentioned in the previous answers and then try to find methods to relieve the tension of the both colliding.

In terms of public safety, the responsibility mainly rests on the ability to provide information crucial in criminal cases or matters of national security (like in the San Bernardino shooting) . We have discussed in detail what this entails in a previous answer. In addition to this pov we also talk about how increased privacy has indeed helped with public safety in a way that hackers can now not hack user data and exploit

users for it. It becomes imperative that this is noted as an important side-effect as Apple holds over 800 million iTunes accounts and each has very sensitive user information.

In the realm of customer privacy we discussed that main responsibilities lie in being able to not give out or access customer data unless and until explicitly consented upon. This ties in very closely with the idea that customer data should be protected at all costs and should not be exploited in any way, shape or form be it by the government or any other third party. This includes restricting access to all government agencies ant not being selective.

The balance of both customer privacy and public safety is this problem in this scenario, it is the one causing tension. On one hand, preserving customer privacy can prove to be detrimental to public safety (As in the San Bernardino Shooting) and on the other hand operation PRISM solidified the idea that sometimes rather more or less all the time, public safety can be used as a scapegoat to spy on citizens, causing a major invasion to their privacy considering that most sensitive information nowadays is stored on our devices. It hence proves to be a challenging task to resolve these tensions.

Talking about methods to resolve said tension, One way could be saying that customer privacy implies public safety as criminals cannot hack into other users data and citizens cannot be exploited. This is a major win. Whatever said and done, as long as Apple caters to customer privacy there is always going to be backlash from the government or law enforcing agencies talking about its determinants to public safety. On the other hand, Cook cannot compromise on customer privacy as it is Apple's major business model and it goes against everything Apple stands for. In reality, there can never be a sweet spot between the two where decisions just make sense and all tension is resolved. There will always be tension between these different facets and that's okay. If there was a way to reach an equilibrium there would be no progress in any of these facets, the raging tension between the two helps in making each responsibility better and execute more effeciently.