Apple and FBI

Introduction

Assume that you have been appointed to a task force of 5 or 6 computing professionals within your organization. You have been asked to examine the current issue outlined in the article below. Your team has not been asked to make specific recommendations to solve the problem. Rather, you have been asked to make recommendations that will help the Government decide what next steps they should take.

Prompts

1. What is/are the problem/problems here? Is there an underlying fundamental problem?
2. Who are the major stakeholders and what are their perspectives?
3. What are the major ethical, legal, and security aspects associated with the problem?
4. What are the intended and unintended consequences of existing computing solutions? Consider the consequences on individuals, organizations and society within local and global contexts.
5. What recommendations do you propose that may lead to potential solutions?

If a crime happens in your home then personal possessions and information in your house could be accessed by police and become evidence. So why should a technological device be different? In 2015 there was a mass shooting in San Bernardino and government authorities wanted to access the iPhone of one of the killers, Syed Farook, to retrieve encrypted data. However, Apple refused to allow engineers to break into the phone as this might create an example whereby users would not own their own data. This led to a court case between Apple and the US government to extract data from the phone. Apple was ordered by the court to make an update that would make it easier to guess the password of this particular type of iPhone. Apple refused, so the FBI paid a security company for a hack to gain access to the phone. This case questions whether the owner should have total control and ownership over data in all circumstances.

While this court case related to a single device, this technique could be used again to get access to data. Although the FBI maintain that they were only interested in Farook's iPhone, the situation has led to a wider concern that governments could have the right to order private companies to get into encrypted products. Apple wonders where this could lead, perhaps "someday they will want [Apple] to turn on [a user's] camera or microphone. We can't do that now but what if we're forced to do that? Where will this stop? In a divorce case? In an immigration case?" said Apple's senior vice president of Internet Software and Services.

Regulations concerning ownership of user data vary around the world. In 2010 the UAE and Saudi banned functions such as instant messaging with Blackberry over security concerns, as the authorities were unable to monitor content. Saudi Telecom claimed that the decision was made to encourage Blackberry to release user data when needed. In the UAE encryption techniques are prohibited if it covers the meaning of content, and in 2012 laws against cybercrime were passed. Having a photo of someone without their consent on a mobile device is an offense, and people have been prosecuted for messages, such as insults, and photos communicated on WhatsApp and social media. The UAE monitors this data to protect morality and security.

The Apple case has led to an increase in super-secure phones that cannot be accessed by a third party or even engineers specialized in encryption. Phones that claim security as their main feature have been on the market for a while, such as BlackPhone and RedPhone. Blackberry has the Priv, which is an Android device offering corporate customers security and applications such as Signal and Wickr encrypt calls and text messages. Box is an online storage provider that allows customers sole custody of their data. The Security Officer of Box comments, "our goal is to achieve a 'zero-knowledge' state where our customers have total control over their data". Apple have cancelled passcodes on encryption, so phones are much harder to hack. Facebook and WhatsApp have also implemented new protocols so they can't access user communications.

This court battle is the first time big technology companies such as Google, Apple and Facebook have stood together against a government. Apple has decided to make the issue much larger than one phone and about data security generally. It has said that it will make encryption even stronger on Apple devices, and possibly even devices Apple engineers can't access. Facebook and Twitter are with Apple to "fight aggressively against requirements for companies to weaken the security of their systems. These demands would create a chilling precedent and obstruct companies' efforts to secure their products". Technology companies are against anything that could make encryption weaker, and so are reacting strongly because they are worried about consumer trust. They argue that if they can be ordered by the government to break encryption on a phone, their customers will no longer trust the security of their products. This includes software updates, which have been one of the best ways to address security flaws. Google and Facebook are frightened of the possibility that the law could force a tech company to put spyware on a

user's phone for the FBI. They could then be seen as acting for the government or law enforcement, and this would affect sales. Overseas sales of American products have decreased before in countries like China over user confidence in security.

The FBI argues that they are disadvantaged from doing their work because of encryption, and that encryption allows a way for terrorists to communicate. Some law enforcement officials say that the technology companies are being unreasonable, and are using the issue as a marketing tool. They maintain that the hack to access the information applied only to one type of phone, and that they were requesting access to only one phone. The underlying issue has an impact on privacy in a technological age when personal information is increasingly protected on encrypted devices. In the Arab world, some users believe information on social media and instant messaging can harm local cultures and traditions, and they support the close monitoring of data.

In the UAE the misuse of messaging services is punishable by law, and a man was prosecuted for swearing on WhatsApp. The law punishes detrimental statements and materials in an effort to protect the reputation, privacy and security of individuals and the country.

Some hope the technology companies and governments can find a compromise. Apple could have found a way to provide the data to the FBI without compromising user privacy and data security. Possibly there might be times when it's necessary to compromise user and data privacy for a greater cause. The government now has information on where the flaw is in the iPhone 5 system, and they could share this with Apple. The Apple philosophy that no one can access an iPhone except the user holds true for the moment.

Bibliography

Al Taher, N. (2014, June 24). *Man jailed for posting video of sleeping friend*. Retrieved June 2, 2015, from Gulf News : http://gulfnews.com/news/uae/crime/man-jailed-for-posting-video-of-sleeping-friend1.1351592

Brandon, J. (2016, 02 23). *In Apple's Fight with the FBI, Edward Snowden Has Already Won the Encryption War.* Retrieved 03 23, 2016, from Inc.: http://www.inc.com/john-brandon/in-apples-fightwith-the-fbi-edward-snowden-has-already-won-the-encryption-war.html

Dajani, H. (2015, July 19). *Tough UAE social media law could see expats deported for saving someone's photo.* Retrieved May 29, 2016, from The National : http://www.thenational.ae/uae/tough-uae-socialmedia-law-could-see-expats-deported-for-saving-someones-photo

Johnson, A., & Blankstein, A. (2016, 02 22). *FBI Fires Back at Apple: 'We Don't Want To Break Anyone's Encryption'.* Retrieved 03 23, 2016, from NBC News : http://www.nbcnews.com/storyline/sanbernardino-shooting/we-don-t-want-break-anyone-s-encryption-fbi-fires-n523186

Menn, J., & Love, J. (2016, 02 24). *Apple's fight with U.S. could speed development of government-proof devices.* Retrieved 03 22, 2016, from Reuters: http://www.reuters.com/article/us-apple-encryption-falloutidUSKCN0VX09N

Ochs, S. (2016, 03 10). *Justice Department slams Apple's 'corrosive' rhetoric in its latest court filing.* Retrieved 03 22, 2016, from PC World : http://www.pcworld.com/article/3042904/security/justicedepartment-slams-apples-corrosive-rhetoric-in-its-latest-court-filing.html

RIM reassures customers as Gulf woes multiply. (2010, August 3). Retrieved May 29, 2016, from Emirates 24/7: http://www.emirates247.com/business/technology/rim-reassures-customers-as-gulf-woesmultiply-2010-08-03-1.274238

Thielman, S. (2016, 02 20). *Apple's encryption battle with the FBI has implications well past the iPhone.* Retrieved 03 23, 2016, from The Guardian : http://www.theguardian.com/technology/2016/feb/19/applefbi-privacy-encryption-fight-san-bernardino-shooting-syed-farook-iphone

Two Gulf states to ban some Blackberry functions. (2010, August 1). Retrieved May 29, 2016, from BBC: http://www.bbc.com/news/world-middle-east-10830485

Williams, K. (2016, 03 10). *Apple: FBI could force us to turn on iPhone cameras, microphones.* Retrieved 03 21, 2016, from The Hill : http://thehill.com/policy/cybersecurity/272518-apple-exec-fbicould-force-us-to-turn-on-iphone-cameras

Williams, K. (n.d.). http://thehill.com/policy/cybersecurity/272518-apple-exec-fbi-could-force-us-to-turnon-iphone-cameras. *The Hill* .

Yadron, D. (2016, 02 19). *Facebook and Twitter back Apple in phone encryption battle with FBI.* Retrieved 03 23, 2016, from The Guardian : http://www.theguardian.com/technology/2016/feb/18/applefbi-encryption-battle-iphone-facebook-twitter-san-bernardino-shooting