Thatcher Lane

CITS 371

15 September 2017

Assignment 2: Cyber Ethics Issues

There are a lot of concepts that are associated with cyber ethics, among these are cyberbullying, intellectual property laws, and freedom of information, just to name a few. One thing that generally does not come to mind when thinking about cyber ethics is encryption. After the shooting that killed 14 people in California in December of 2016, the Federal Bureau of Investigation (FBI) demanded that Apple decrypt the information encoded on the iPhone 6 that belonged to the shooter (Nakashima, 2016). This event brought the ethical conflict of encryption to the forefront of most American's minds for the first time in their lives. While the idea of privacy has been around since the dawn of time, encryption is a new way of thinking about this. The ethical idea that arises here is if very strong encryption jeopardizes the security of the public, rather than protecting it.

While encryption may seem like a cut and dry issue, this is actually very far from the truth! Recently the University of Santa Clara held a discussion panel with leading experts in the field of cyber security. During the panel, FBI agent David Johnson said this:

“[Encryption is] a great, valuable tool. Without question, it should be used by individuals and businesses to protect their data, and by the government to protect its data. However, there have to be some limits on it, and it gets pretty complicated pretty quickly.” (University, S. C, 2017)

The major concern within the major branches of the government is that very advanced encryption that cannot be cracked can damage the safety of people in a crisis situation, in which the is not enough time to go through the proper channels and acquire a warrant. The FBI argues that while encryption may seem like a personal freedom or security, there are certain situations in which it becomes very public.

The largest problem that comes with this particular ethical issue is the large gray area over to whom the issue belongs. Is encryption of my hard drive a matter of personal security, or is it one of the public or even national securities? This is a large muddle in our particular issues. I personally believe that encryption is a matter of personal security and that the idea of encryption that is too good does not exist. Encryption of one's personal information, not only provides increased security in the case of a security breach, but it also provides peace of mind. If we view this conflict using the concept of utility, we can easily see that personal encryption is on the correct side of the "moral fence" so to speak. According to Ethics and Technology "Social utility is superior to alternative criteria for evaluating moral systems" (Tavani, 2013). The increase in peace of mind that one receives from encrypting their data well is observed as an increase in utility, which according to Act Utilitarianism is the only criteria that are of any importance when evaluating a moral issue.

Nakashima, E. (2016, February 17). Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks. Retrieved September 15, 2017, from http://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99\_story.html?utm\_term=.67882073bb5f.

Tavani, H. T. (2013). *Ethics and technology: controversies, questions, and strategies for ethical computing*(4th ed.). Hoboken, NJ: Wiley.

University, S. C. (n.d.). The Ethics of Encryption. Retrieved September 15, 2017, from http://www.scu.edu/ethics/focus-areas/business-ethics/resources/the-ethics-of-encryption/.