James Small

CSE488

15 February 2014

Ethics Code Violations aren't always as they seem

When looking at the ever changing technological world around us, it is hard not to notice the different moral and ethical issues that arise from the progress. As the technology changes, so should the moral and ethical issues associated with them. With more and more of our lives being put onto computer systems, there are many security, privacy, and intellectual property issues that arise. The seemingly obvious benefits of an interconnected life can not go unnoticed, but there is a cost associated with it. In this paper, I will look at three separate articles that all relate in some way to the security, privacy, and intellectual property issues of our interconnected world. First, with the hugely popular social network Facebook, and the changing of their privacy policy without notice. Second, with the loss of 80 computers from a nuclear facility. Lastly, with the horrible Stuxnet worm and it's purpose. Through these articles, a common message appeared in that all of the players involved felt they were doing what was morally and ethically right while violating the different standard codes of ethics. Yet upon a closer inspection, these violations don't apply to all involved as certain situations change what is ethically good.

Trying to imagine a world without all the technological advances seems impossible. The value of these technological systems are beyond helpful and valuable in our lives. To the joy of seeing your friends' children's pictures on Facebook, to the advances in technology that allow us a species to make things that would have never

been possible without, all of which show how technology has enriched our lives. It is a choice we all make in embracing this technology that causes problems. Even though we choose to put our information online and reap the benefits of technology does not take away our basic right to privacy, security, and intellectual property protection. In all three articles, it is easy to see that the ACM Code of Ethics and IEEE Code of Ethics are clearly in violation by all parties involved, but there is more to the story.

In the first article in PC World magazine regarding Facebook, we see that Facebook mad a drastic change to their privacy policy. This subtile change was given without notice and was not even discovered immediately upon the change. This change was based on the removal of an important line from their privacy terms. The basis of the section in question stated that Facebook has an "irrevocable, perpetual" license to your "name, likeness, and image" in whatever way they see fit. There was another line, the one that was deleted, that came next that stated that this license to use our data would "automatically expire" if we removed our content. With this line removed, our data would essentially be available to use forever as Facebook sees fit (Raphael).

This privacy change, which the Facebook CEO Mark Zuckerberg defended, was eventually reversed back to its original form. Why would a company do such a thing? Making such a dramatic change without notifying users seems ethically and morally wrong. The power of Facebook is in their data. The amount of data they have on all of us is staggering. This data is the main source of their income in the form of advertising. The more data they have on you, the more targeted ads they can sell to you and people like you, and the more money Facebook makes. This is a straightforward process. Since Facebook is a public company, they have a fiduciary responsibility to their

shareholders to increase profits. By making these changes, and essentially keeping this data, they are doing right by their shareholders and adhering to their responsibility to their shareholders. These changes show that Facebook is using ethical concept known as Egoism, which states that the action taken by Facebook were done at the benefit of themselves, and with disregard for everyone else involved (Lander). The change was made purely for financial reasons, regardless of how it was perceived by everyone on the outside.

Facebook also violated the ACM Code of Ethics, particularly article 1.7, Respect Privacy of Others (ACM). Facebook is not respecting the privacy of its users. Even though we put our data up there for them to use, it was done based on an existing privacy policy, and by changing that policy without our notice our privacy is no longer being respected by them but being exploited by them. If I choose to be apart of the Facebook system, I would understand the consequences of my actions in regards to my intellectual property and privacy, but if I chose to leave that system, my data should come with me. This change removed that fundamental right. The use of my data in their system when I'm not in their system anymore particularly shows their lack of respect for the value I brought them when I was part of their system. They are also in violation of the IEEE Code of Ethics, particularly article 9 which states that they should avoid injury to others, their property, and their reputation (IEEE). This sudden un told change made by Facebook easily shows their non respect for our property, in this case, our intellectual property and privacy.

The second article discusses the lost, stolen, or "missing" computers from the Los Alamos National Laboratory in New Mexico. An internal letter describing the lose

was brought to public attention by the Project on Government Oversight organization. The letter discusses how 13 lab computers were lost or stolen during the past year, and another 67 computers were deemed "missing". The impact of this cannot be overlooked considering the location of these computers. The Los Alamos facility was created during World War II as a secret, and it was the site for the Manhattan project. The Manhattan project gave birth to the first nuclear weapons created by the United States Government (Lowy). The data contained on these computers should be of national security, as they have the potential to help other nations create nuclear weapons, a problem that can affect all of us.

One of the main issues that came about during this lose was in how it was handled. Instead of treating this lose on the basis of intellectual property theft like it should have been, it was treated as a "property management issue" (Lowy). It was essentially treated as the lose of a piece of equipment, like a stapler, instead of something that had national security implications. The decision makers at the Los Alamos facility were clearly not aware of the issues and impact surrounding these computers. The importance of the data contained on the computers seems very clear, yet not acted upon. What makes this even more appalling is the fact that the events that led to their lose, and their current location are not actively being pursued. How could that be? How could such a glaring problem be ignored? The Los Alamos facility seems to be employing the idea of Consequentialism which states that the consequences of a particular action are the basis for the moral decision (Sinnott-Armstrong). Essentially, the fear of getting in trouble and looking like a bunch of idiots helped them decide on their ultimate path. Instead of speaking up and making a strong

effort to figure out what happened, they essentially do nothing. In this case, Consequentialism employed by these people can have a catastrophic affect on everyone. If that data ended up in the wrong hands, nuclear weapons could be used on our country. This alone should drive their decision to do what they can to solve the problem, but still, it doesn't seem like anything is happening.

There are also many code violations in relation to this article. The Los Alamos facility is clearly in violation of the ACM Code of Ethics, particularly article 1.1 which states that an ACM member must contribute to society and the well being of others (ACM). They are in clear violation of this article because the potential for harm to others is prevalent in the loss of potential nuclear data. When it comes to the IEEE Code of Ethics, they are 100% in violation of article 1, which states that an IEEE member must "accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment" (IEEE). Their consequentialist decision to not 100% pursue the reasons behind the loss and the location of the highly sensitive data on those computers shows how they did not accept responsibility for for the welfare of the public. This loss has a potential to "endanger the public or environment" in a nuclear disaster. With the threat of nuclear disaster always on our minds, what can be done about it?

The final article was about a computer worm that was commonly referred to as Stuxnet. Stuxnet was a computer worm created by the United States and Israel as an attempt to prevent the creation of nuclear weapons by Iran. The stuxnet worm was highly sophisticated in how it operated, showing not just anyone could have created it. The stuxnet worm was intended to attack computers in a nuclear enrichment plant in

Iran. To accomplish this, the worm was put onto USB sticks and brought into the facility where it would infect computers running the Windows operating system. The worm was able to not be detected because of a certificate that made it look authentic. Next, the infected computer would search the network for the target machines it was looking for. In this case, it was Siemens Step 7 software running on other Windows based machines. This software was used to control centrifuges and the worm was made to attack the programable logic controllers of those centrifuges. Essentially, allowing the creator of the worm to break the centrifuges, thereby slowing down the production of nuclear weapons by Iran. The worm would compromise these systems using several zero day exploits in the Windows operating system. It would spy on the infected systems and network and report back its findings to its creators. In the final, yet brilliant step, as the machines were being controlled in a way that could cause damage them, the worm would report back to its operators that everything was going fine, thus preventing a fix until it was too late (Kushner). The power of this worm comes from the basic way a worm operates.

A virus is a way to compromise a computer system that takes advantages of vulnerabilities in a system. A virus operates by user interaction. Essentially meaning a virus needs a user to click on an affect program or run some piece of software in order for it to replicate. A worm on the other hand can spread without user interaction. It runs on its own and can infect other computers without any interaction. In this case, a worm was the best solution because it would spread on its own to the correct systems it was targeting.

Upon investigation of the stuxnet worm, it was concluded that it in fact was started by the United States and Israeli governments to stop Iran from obtaining nuclear weapons. Instead of bombing the nuclear facility, it developed this highly sophisticated worm to do the work for them in a much safer way. The US and Israeli governments are essentially hacking. Hacking has always been morally and ethically wrong, yet in this case, there can be arguments made that it's right. The creators of this worm employ situational ethics to help justify their decision to engage in this attack. Situational ethics states that the morality of an act is based upon the current situation the act was made in (Ethics Guide). Under the current threat of Iran having nuclear weapons, the creators took the best action they could to prevent the problem. Without the situation that was created by Iran seeking nuclear weapons, such an ethical and moral decision would not have been made. The unfortunate side effect of this ethical decision is that the worm, which was only intended for the specific Iranian facility, made its way out into the public, and in true worm fashion replicated itself to other computers automatically. In the end, this does not change the original ethical decision. The cost of such a worm getting out on the internet pales in comparison to Iran possessing nuclear weapons.

The creators of the stuxnet worm are in clear violation of the ACM Code of Ethics, particularly article 1.2, avoid harm to others (ACM). On first glance, they are in clear violation of this article because they are not preventing harm to others, particularly causing property damage in regards to the centrifuges that are being destroyed. They are also in violation of the IEEE Code of Ethics, particularly article 9 which states that they should avoid injury to others, their property, and their reputation (IEEE). Just like in the ACM Code of Ethics violation, the effect of this worm is the property damage of the

centrifuge. It seems straightforward in this violation, but upon closer inspection, they are also following certain articles of both codes that overshadow the violations.

The first article in the ACM Code of Ethics states that you should contribute to society and human well-being (ACM). The first article in the IEEE Code of Ethics states to accept responsibility in making decisions consistent with the safety, health and welfare of the public (IEEE). I believe these two codes to stand above the rest. They both state the same basic principal that you should do what is necessary to protect human well-being and the welfare of the public. By attempting to prevent Iran from obtaining nuclear weapons using the stuxnet worm, they are doing what is necessary to stop what could be a threat of global proportions. They could just bomb Iran and destroy any chance of the creation of nuclear weapons, but they are preventing innocent casualties in the process, there by continuing to apply the first articles of both codes of ethics.

When looking at the 80 computers stolen from the Los Alamos nuclear facility and the potential threat created by Iran attempting to obtain nuclear weapons, we can see that they are related. What if the 80 missing computers were in fact stolen by Iran to help them create nuclear weapons? With our government going through as much work as it is to help prevent Iran form gaining these weapons, yet the Los Alamos facility not treating this as a big of problem as it is seems to go against the norm. This just adds to the problems created by the actions taken by the Los Alamos facility in treating the loss as a property management issue instead a national security issue. The basic idea of computes being stolen on their own is not that big of a deal, but the idea that the person or group that ended up with it can have catastrophic results.

An interesting quote in an article by Ian Thomson titled "Security Experts Split on Cyberwar", Mikko Hypponen is quoted as saying, "Ultimately the ethics of this don't really matter - the decision has been made and this kind of stuff is going to be unavoidable" (Thomson). In the end, of course the decision has been made. The stuxnet worm was created and it did what it was intended to do. Ethical conversations can of course be avoided, but that does not mean they shouldn't happen. There is an ethical discussion to be had here because hacking is deemed ethically wrong, yet in this case, there is a strong argument for it's value. In this case, the end result of the creation of the stuxnet worm was inherently intended to be good and to prevent Iran from gaining nuclear weapons, which is universally deemed as a bad idea. The discussion should still be had, even at the same time as the practicalities of the situation are also being discussed.

In the end, the violations of the ACM Code of Ethics and the IEEE Code of Ethics are valid. Each party involved had their own ethical reasoning to justify their actions. With Facebook changing it's policy, it employed the use of egoism to justify their decision, in the end violating both codes of ethics in the process. This decision on their part was wrong based on their violations. With the computers stolen from the Los Alamos facility, they employed the ethical idea of consequentialism in their decision to not pursue the stolen computers and treat the issue like the big issue it actually was. The decision on their part was wrong based on their violations. Lastly we looked at the stuxnet worm created by the US and Israeli governments in order to stop Iran from obtaining nuclear weapons. They employed the idea of situational ethics to justify their decisions. The decision on their part can be viewed as wrong based on their violations

at first glance, but upon inspection, their true reasoning comes forth and even though there were violations, they can be justified and are morally and ethically right. The take away here is that violations of the ACM and IEEE Code of Ethics do not necessarily mean that what was done is ethically wrong. Each situation needs to be evaluated on its own merit. With security, privacy, and intellectual property involved in all transactions and ethical discussions related to things online, it is imperative to evaluate them not on from the outside making a simple assumption, but to go deeper and see that ethical intentions may look bad in the beginning, but can be good in the end.

References

ACM Council. “ACM Code of Ethics and Professional Conduct.” Association for Computing Machinery. 16, Oct. 1992. Web. 15 Feb. 2014 http://www.acm.org/about/code-of-ethics

IEEE. “IEEE Code of Ethics.” IEEE – The Worlds Largest Professional Association for the Advancement of Technology. IEEE, 1 Jan. 2013. Web. 15 Feb 2014. http://www.ieee.org/about/corporate/governance/p7-8.html

Ethics Guide. “Situation Ethics.” BBC – Ethics Guide. Web. 15 Feb 2014. http://www.bbc.co.uk/ethics/introduction/situation_1.shtml

Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum*. IEEE Spectrum, 26 Feb 2013. Web. 15 Feb 2014. <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>

Lander Education. "Ethical Egoism." Philosophy Home Page. Philosophy Lander, 26 June 2011. Web. 15 Feb 2014. http://philosophy.lander.edu/ethics/ethical_ego.html

Lowy, Joan. "67 Computers Missing From Nuclear Weapons Lab" The Huffington Post. 11 Feb. 2009. Web. 15 Feb. 2015. http://www.huffingtonpost.com/2009/02/11/67-computers-missing-from_n_166189.html

Raphael, JR. "Facebook Privacy Change Sparks Federal Complaint." *PC Magazine*. PC Magazine, 17 Feb 2009. Web. 15 Feb 2014. http://www.pcworld.com/article/159703/facebook.html

Sinnott-Armstrong, Walter, "Consequentialism", The Stanford Encyclopedia of Philosophy (Spring 2014 Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/spr2014/entries/consequentialism

Thomson, Ian. "Stuxnet: 'Moral crime' or proportionate response?." The UK Register. The UK Register, 27 Jul 2012. Web. 15 Feb 2014. http://www.theregister.co.uk/2012/07/26/stuxnet_moral_crime