Jack Potter

CprE 234X Term Paper

2019-12-13

My Personal Code of Professional Ethics

While confronting many ethical dilemmas may require hours of deliberation and result in no obvious conclusion, this essay will examine several situations that I believe would require little to no consideration on my part before making a decision as well as the applicable tenets of my personal code of professional ethics. These tenets in particular are inflexible, demarcating the lines that I will not willingly cross; resigning or accepting termination from my job would be preferable to violating these portions of my code.

First and foremost, my personal code borrows from the most widely-known aspect of the Hippocratic Oath required of medical professionals - “do no harm”. Specifically, I refuse to be complicit in actions that will directly lead to directly endangering the health and safety of others. While this may seem like a general ethical principal that isn’t directly applicable to the field of cyber security, I maintain that it is an important starting point for one’s ethics to draw from, and while it may not be a frequent occurrence for cyber security engineers to find themselves in a situation where people may face physical harm, it is certainly possible.

In order to examine such a situation in which human health and safety is put at risk, let us imagine a cyber security engineer by the name of Alice. Alice has been tasked with securing a company’s critical infrastructure, primarily focusing on the servers that form the backbone of the company’s service. While analyzing all possible attack vectors against the servers, Alice walks through the company’s server room to search for weaknesses that could be exploited to gain physical access to the servers. To her dismay, Alice discovers that the emergency exits from the server room have been padlocked shut to prevent an attacker with an under-door tool from manipulating the internal crash bar from the outside and gaining access to the server room. By padlocking the door shut, the company has prevented anyone from entering the server room without authorization, but they have all but guaranteed that anyone working in the server room would not be able to quickly open the doors and escape in case of a fire. This, obviously, is a serious issue.

In my opinion, the path forward for Alice is fairly straightforward. First and foremost, she should remove the padlocks from the fire doors. This may involve tracking down the keys, utilizing a set of lock picks, taking a screwdriver to the mounting brackets the padlocks hold together, or simply finding a pair of bolt cutters and snipping right through the locks. After the locks have been removed, she should report directly to her supervisor and make it clear that these dangerous security measures cannot be tolerated, and if they insist on replacing the locks, she’ll report it directly to the county fire marshall. While they may threaten her job for doing so, it is her moral and ethical duty to take action to prevent people from being hurt or killed if she could have directly acted to prevent it. As we discussed in class, it is never easy to decide to become a whistleblower against one’s company, however, in situations where health and safety depend on it, I believe it is not only justified, but necessary.

Moving on, my code of ethics can be somewhat extrapolated from the “base case” of “do no harm”. I think that if a cyber security professional discovers a situation that could lead to the breach and release of critical personally identifiable information, they have an obligation to fight for it to be fixed immediately, accepting that they must fight hard enough that if they lose, they may be terminated from their position. Now, it is important that we qualify what constitutes critical PII. I believe that a database correlating customer names to email addresses isn’t important enough to warrant fighting with senior management in this matter. Obviously, there is a moral imperative to work towards the securing of this database, but the actual ramifications of it being released are relatively minor for the customers. However, a database that contains customer social security numbers correlated with customer names is absolutely important enough to warrant this type of response. Not fighting tooth and nail to ensure that this problem is remediated would be tantamount to allowing the inevitable theft of the identity of every individual in the database. As we’ve discussed in class, particularly regarding the Equifax breach, companies can recover from such events, and they typically do so by offering services such as credit monitoring to those affected by their negligence. However, I don’t believe that this is enough. Frankly, the financial solvency of the company in this case is one of my lower priorities, as I am much more concerned with the impact felt by the individual consumers that have to deal with the aftermath of the company’s mistakes. Note that while I have qualified what constitutes critical PII, I haven’t quantified the number of affected individuals necessary to warrant such a response, and this is intentional. I don’t believe that there is a number of people that I would be okay with harming by standing by and allowing their identities to be stolen. Furthermore, if a company’s processes allow one person’s data to be unlawfully accessed, they almost certainly allow access to the data of many others. Therefore, if my company actively refuses my requests to fix serious security issues that could lead to such catastrophic consequences, I would have no option but to resign or be fired.

Let us continue to extrapolate “do no harm” into additional ethical principles, this time by imagining a cyber security engineer named Bob. Bob has recently been tasked with setting up a secure channel between the application developed and maintained by his employer and an advertising service. As he works to the specifications given, he realizes that the primary purpose of this channel will be for transmitting customer data from his employer to this advertising service. While many applications have found great success by offering free services that are supported by advertisements, Bob’s company’s application isn’t one of them. Customers are charged a fee in order to use the application, and they believe that the data they give the application is kept completely confidential and never shared. In fact, the application terms of service indicate that at no point will the information leave the company’s servers.

Bob must make a choice at this point. He can continue with his work and move on with his life, with customer data quietly being siphoned and sold to an advertising service with the customers remaining unaware of this intrusion. He can also refuse to complete his task, insisting that customers be notified well in advance of any changes to the service that would lead to the compromise of their information. I believe strongly that the ethically correct option is the second choice, with Bob willing to walk out and take this story to the media if his company refuses to back down, as he will never agree to violate the inherent right to privacy enjoyed by his company’s customers.

A more extreme, though less direct, case of privacy invasion should also be considered. Companies such as Hacking Team[1] discover zero day exploits, create malware, and develop surveillance technologies, all of which they sell to various law enforcement bodies and nation states. It can be argued that they are nothing more than black market weapons dealers, selling weapons to the highest bidder with no regard for who they will be used on. My personal moral code leads me to condemn companies of this sort in the strongest possible terms. I believe it is very difficult for anyone to argue that equipping government bodies with the tools necessary to spy on their own citizens or the citizens and governments of other countries is ethically correct. I furthermore believe it is impossible to argue in favor of equipping law enforcement bodies with such tools, as they will doubtlessly be used without justification on innocent individuals. As Quinn writes in Ethics for the Information Age[2], opponents to mass public surveillance systems point out both their cost and ineffectiveness. His

[1] www.hackingteam.com

[2] Michael J. Quinn, “Ethics for the Information Age” 7th edition, copyright 2017 Pearson Education

examples revolve primarily around surveillance cameras, pointing out that the one camera in in Britain for every 14.2 citizens did nothing to prevent the London Subway Bombing of 2005. In an unintentionally darkly humorous comparison, he includes CCTV images of the suspects of the Boston Marathon bombing, explaining that the CCTV in Boston was a crucial part of apprehending the suspects. However, CCTV, the USA PATRIOT Act, the OneDOJ database, and many other such potential safeguards against terrorism did nothing to prevent the attack from being carried out in the first place. Due to the nature of these ineffective yet still privacy-infringing law enforcement measures, I must conclude that my personal ethical code prohibits me from ever working for a company such as Hacking Team, producing and monetizing tools for this use.

I believe that the prior examples speak to a major part of my own personal sense of morality that extends beyond professional ethics. In class discussions, I've spoken ill of the corporate greed and profit-above-all-else mentality that incentivizes companies and their employees to cut legal and ethical corners in order to provide value to their stockholders. I personally believe that capitalism's relentless pursuit of "more" - more customers, more products, and ultimately more profits – is directly responsible for a number of the ethical dilemmas that we have spent the semester debating. From selling customer data without their consent to injecting advertisements into website content, from keeping critically important software closed-source to not securing customer data and calling it an "acceptable risk", all of these decisions are rooted in the simple cost-benefit analysis that always decides in favor of profit. Unfortunately, proposing a solution to this issue doesn't fall within the scope of this class, and certainly not within the length of this paper, so we will simply have to proceed with the understanding that my personal code of ethics will always prioritize the health, safety, and comfort of the individual above that of the corporation.

I don’t believe that this fundamental tenet of my personal moral philosophy is likely to change, so I logically don’t foresee my personal code of professional ethics changing as a result. If anything, I feel that after some time in industry, I may expand my list of situations that fall beyond the boundaries I’m somewhat outlining in this paper. Due to the unceasing need for people to work in the field of cyber security, it is fairly assured that qualified individuals will retain a high degree of job security throughout their careers. I believe that this gives us, the next generation of cyber security analysts and engineers, enormous bargaining power over the corporations that we work for. If we as an industry are able to come together and identify a code of ethics that we can stand by, we can make it clear to the world that we’re all going to do everything we can to ensure that companies continue to operate legally and ethically in cyberspace. If it is made obvious that the vast majority of cyber security professionals are not willing to violate the rights of the general public, companies won’t be able to simply fire their cyber security staff for taking an ethical stand and replace them with people who will be complacent. While I understand the difficulty of developing a unifying set of ethics that people can all abide by, I feel that this idyllic future is one worth fighting for. I realize that most of the ethical debates we had in class ended with the class rather divided on the issues in question, but I maintain that we should strive to band together as an industry and take a stand against blatantly unethical, flagrantly corrupt, and generally harmful behaviors.

In short, I understand that I’m just one person with my own ethical code, but I trust it to help me navigate through the complex and murky world of cyber security, and I hope that I may serve to be a positive force for change throughout my career.