James Small

CSE488

18 January 2014

Data Theft and the Ethical Impact

In our world today, more and more of our lives are stored on computers as data. From where we shop and what we eat, to more personal things like financial information and our personal relationships. The power of this data has enhanced our lives, but at what cost? Most people do not think about this data until something happens to it. Employees turned “cyber moles” and crime syndicates all over the world are stealing this data from the very sources in which you put your faith in to protect it. Our reliance on data has turned it into something more valuable than even money. With data theft recently reported to have topped a trillion dollars, this is not some small problem, but a massive problem that can have huge impacts on our lives. Not only are large “cyber mafia gangs” breaking into corporate networks and stealing this data, but employees who are struggling financially because of the current economic conditions are utilizing the theft of this data to survive. Even though these people feel the need to steal data, there is no way to justify what they’re doing, as it is morally and ethically wrong to do so.

A lot of people think that they are safe if they don’t shop online because they are not putting their data out there to be stolen, but this data theft can happen anywhere. Over the holidays, an estimated 40 million credit card numbers were stolen from one of the nation's largest retailers, Target. We all put our faith in this company to protect our data from being stolen while shopping there, myself included, who used a credit card at Target over the holidays. The financial impact from this breach can’t go unnoticed.

Who is at fault here? Is it Target for trying to cut corners with the security in place to protect this data, or could it be our reliance on data that has formed over the last decade? We live in a connected world where we want everything available to us at the push of a button on our smart phones, so we need to all understand the possible consequences of that desire.

Data theft, like the credit card data stolen from Target, is most often stolen for personal gain. The power of data like this is staggering, so the incentive in stealing it is high. These “cyber mafias” employ the ethical idea of Egoism to justify the stealing of this data. Egoism tells us that the actions taken by an individual should be good for the individual, and that they should not be looking out for others (Lander, para 1). This data theft at Target exemplifies this point clearly as they do not care about what happens to the 40 million credit card owners, but what they will gain from this data. The cost to fix this breach in security goes beyond charges that are made on these stolen cards, but the cost to replace all the cards by the credit card companies, and also the loss in trust of Target as a company. Target’s bottom line will be affected by this stolen data as shoppers might decide to shop else where, as the trust is now gone. The financial burden from this breach cannot be measured, but in the end, these data thieves do not care about what happens to everyone, but only what happens to them. This transitions right into the idea that they feel they are doing the right thing because the result enhances their happiness.

These “cyber mafia” members also employ the idea of Hedonistic Utilitarianism to help justify the stealing of data. This ethical concept states that the right action comes from the idea of maximization of happiness (Stanford, para 2). These people know that the financial windfall they will achieve once they have all of these credit card numbers will enhance their lives. For whatever reason, their need for money drives them to feel that the right action is to steal the data and that the privacy of others is not important. Obviously money has the potential to make all of us happy, and in the case of Target, the hackers felt that the money would accomplish that, but at what cost.

We all desire a high level of privacy in our lives, yet we put all of our data out there to be looked upon and possibly stolen. Facebook is a perfect example of how we are looking the other way when it comes to privacy in order to gain the value that we feel a website like Facebook offers. With all the controversy over the privacy settings that Facebook changes without notice, the expected result would be for people to leave the site in droves, yet they stay. There is a reason Facebook is valued at such a large amount of money. The data they have on us is more valuable than most on the internet today. Yet, why do they change their privacy settings to make things more open without our knowledge? Facebook benefits from our data more than most people who use the site understand. The more data you give them, the more money they make off of you. Facebook has a moral and ethical obligation in regards to the data we give them, yet when they make things more open without our knowledge I feel they are employing, to some degree, a level of Utilitarianism. They are a public company, and they have a fiduciary responsibility to increase profits for its shareholders. Because of this, Facebook feels that by changing their privacy settings without notice, they are in fact doing well by their shareholders and their responsibility to them. Not all issues relating to privacy and data theft are caused by such large corporations and “cyber mafias”, but are caused by other things.

With the downturn of the economy since 2008, people have needed to make drastic decisions in order for them, and their families, to survive. These workers were turned into “cyber moles”, stealing data from the companies they work for. With drastic pay cuts, and the cutting of benefits, employees felt it was morally right to steal data from their own companies. This is a perfect example of Situational Ethics as these employees felt their decisions were morally right because of the situation they were put in by their employer (Ethics, para 1). When it comes down to it, if a decision had to be made to protect yourself and your own family, or protect the company you work for, all of us would make the same decision in order to survive. The fact that these employees work for the company, and know the ins and outs of how it works, it makes it a lot easier to steal the data. Take a look at the breach at Target and it has been confirmed that this hack came in from outside their network, but what was stopping this breach from coming from the inside. Employees turned “cyber moles” had the potential, and access, to steal such data.

While there are ethical ways to justify the decisions and actions of these “cyber mafias” and “cyber moles”, these people are clearly in violation of the ACM Code of Ethics. ACM is the world’s largest educational and scientific computing society and they have developed a set of imperatives to help show the fundamental ethical considerations of professionals. There are many violations of the ACM Code of Ethics, but one of the clearest violations comes from imperative 1.2 “Avoid harm to others”. The idea of “harm” can be interrupted differently depending on the persons involved. In this case, and according to the ACM Code of Ethics, harm refers to “negative consequences, such as undesirable loss of information” (ACM, 1.2). This is the basis of what these attackers are doing. They are in violation of this imperative on the basis of the data they're stealing results in an "undesirable loss of information", not only to the company for which the data was stolen from, but to the people who's data is actually stolen. Another major area of violation is in reference to imperative 1.7 "Respect the privacy of others" (ACM, 1.7). With the amount of data being stored currently, there is an increased responsibility of all to respect it. These attackers are in violation of this imperative because they don't care about the others involved. This goes back to the idea of egoism and the fact that they don't care about others and only themselves. It's not just the ACM Code of Ethics that these attackers are in violation of.

A member of the IEEE has a moral obligation to adhere by the IEE Code of Ethics. These "cyber moles" and "cyber mafias" are clearly not members of this organization based on their actions. Article 9 states "to avoid inuring others, their property, reputation, or employment by false or malicious action" (IEEE, para 9). The obvious take away from the article is the idea of property. These attackers are clearly not avoiding injuring the property of the individuals around them. Property, in this case, is the data about them that is being taken by these criminals. One area this article does reference is also reputation. With the data stolen by these attackers, they have the ability to devastate the reputation of the people whose data they stole. With all the personal information we put out on the internet today, the potential for damage to your reputation is high. Image someone stealing the data from Facebook, and all of your personal messages that you thought were private are now readily available to others. If you chose to engage in an extra martial affair, this data could cause lots of problems with your reputation. These "cyber moles" are also in violation of Article 2 as well, which states “to avoid real or perceived conflicts of interest whenever possible” (IEEE, para 2). By working for a company, you are given access to all types of data that could be useful outside the company. Your moral obligation while employed there is to protect this data. Clearly you would have huge conflict of interest in this case, as you would be using the data you have been entrusted with while an employee of the company. These violations still violate the basic idea that stealing is wrong.

When it comes down to it, regardless of what you deem morally right based on your own ethical beliefs, the idea of stealing data is wrong. These “cyber moles” and “cyber mafias” are clearly in violation of basic common sense that most of the people on this planet follow. Yes, there are all sorts of people, who feel for whatever reason, that their decisions are warranted. Most people believe in the basic concept that stealing is wrong. Respect for the privacy of those around us is a fundamental right that needs to be, and for the most part, is followed. If we lived in a world where the majority of people violated this basic concept of privacy, our society would fall apart. This brings about the idea of Ethical Nihilism. These people completely reject the basic ideas of privacy that most of us live by. The do not care about following the morals and social customs around them that most of us have been raised to follow, but chose to act in their own way (Pratt, para 1). An own way that they feel is right.

The concept of data security is more important now than ever. I think we, as technology professionals, need to put a huge focus on the protection of the data that is entrusted to us. We have moral and ethical obligation, as defined by the ACM Code of Ethics and the IEEE Code of Ethics, to protect this data. With potential attacks coming from internal and external means, the focus should be on defending what you know to be right. As more and more data is put out there, more and more people will try to steal it. This leads to a back and forth game of cat and mouse that unfortunately has no end. Every time a new vulnerability is discovered and exploited, it is blocked. This causes the attackers to find more and better vulnerabilities. Also, with the emergence of new technologies, the ethical and moral rules that we follow must change as well. Just because something makes sense in today's technological world, doesn't mean it will make sense in 20 years.

The importance of keeping data secure in our society today cannot be overlooked. From the use of credit cards at your local store, to the personal and financial information you give out on a regular basis, all of this data is out there and just waiting to be stolen by these "cyber moles" and "cyber mafias". The power that this data holds is not even close to the power these hackers have in controlling things. All it takes is one huge breach of trust from a company to signal its downfall. This cannot only ruin the company and the lives of its employees, but also can affect the economy as a whole. Most all of us have decided to put our data out there in many ways. The benefits of having our data out there can be vast, but it comes at a cost, a cost that you as an individual must weigh before deciding to put your information out there. In the end, we shouldn't have to worry about the privacy of our data if everyone in the world was honest and forthright. We all have the right to believe what we want and use whatever reasoning we'd like to justify those beliefs. Based on what I think is morally and ethically right, the stealing of data, and stealing in general, is wrong and should not be tolerated.

References

ACM Council. “ACM Code of Ethics and Professional Conduct.” Association for Computing Machinery. 16, Oct. 1992. Web. 18, Jan. 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. 18 Jan 2014. http://www.ieee.org/about/corporate/governance/p7-8.html

Ethics Guide. “Situation Ethics.” BBC – Ethics Guide. Web. 18 Jan 2014. http://www.bbc.co.uk/ethics/introduction/situation_1.shtml

Lander Education. "Ethical Egoism." Philosophy Home Page. Philosophy Lander, 26 June 2011. Web. 18 Jan 2014. http://philosophy.lander.edu/ethics/ethical_ego.html

Pratt, Alan. "Nihilism [Internet Encyclopedia of Philosophy]." Internet Encyclopedia of Philosophy. Internet Encyclopedia of Philosophy, 23 Apr. 2001. Web. 18 Jan 2014. http://www.iep.utm.edu/nihilism/

Stanford Encyclopedia of Philosophy. “The History of Utilitarianism.” Stanford Philosophy, 27 Mar 2009. Web. 18 Jan 2014. http://plato.stanford.edu/entries/utilitarianism-history/