Luke Albert

Case Analysis 2

I believe that the United States should adopt something like Europe’s General Data Protection Regulation (GDPR). User data is important and should be confidential no matter what. The results of a breach could affect someone greatly and they may be at risk of theft or even identity fraud. Big corporations such as Google and Facebook often use people’s data without them knowing. Usually, this use is for a good reason and is beneficial to the consumer. However sometimes data breaches can result in people’s information being stolen as well as sometimes the corporations use the data in a malicious way. There should be rules and guidelines for these corporations stealing and collecting data, so people can use the internet more safely and securely. In this Case Analysis I will argue that consequentialism shows us that the United States should follow Europe’s lead because it keeps the consumer safe, puts more responsibility on corporations, and allows the consumer and producer to meet each other’s needs.

One of Michael Zimmer’s central concepts is that there is an insignificant amount of privacy protection for consumers in the US. As time goes on and technology evolves and develops over time there needs to be new laws in place. I feel like that is one thing a lot of people miss out on. Technology is advancing so fast we do not exactly know of all the dangers yet. This is a reason of why there needs to be updated legislation especially dealing with personal data security online. There are many out-of-date legislations that need to be updated with current times. A lot of people are misinformed or not informed enough in general, so they can be taken advantage of very easily. Even if there is a user agreement before someone can use the platform most people just click accept without reading. That is partially the consumers fault for not reading about what they sign up for however corporations are just taking advantage of the lazy consumers or the consumers that do not care. Not to say that is a bad thing however, there needs to be laws in place, so the consumers do not get completely screwed over if a data breach happens. There is a set of security in place for the consumer, but like Michael Zimmer said, there are huge limitations on those rules and there needs to be more security. The T3 experiment was planned to have guidelines and to protect the data of the people being tested. It is good that they initially tried to protect user data however as their experiment went on they realized how many loopholes there were. The experimenters accessed data of students whether the students profile was private or public. This is unethical because if someone has their account on private then their data and information shouldn’t be available to the public. No matter what the organization does with the information they still obtained it and allowed there to be a possibility of a breach to happen. The T3 experiment caused peoples data to be vulnerable and uncontrollable by the user themselves. With their data pulled out, all of their information is in a new database which they do not have control over. The amount of data pulled out from the test subjects is wrong and should never had happened to the extent which it did. The T3 experimenters obtained data from over 1,500 people over the course of four years. The T3 project obtained user data in an improper way by not having consent of those who they were studying and even stealing data from those who had their profiles on private. They saw a loophole to obtain private data and abused it and allowed the private data be available to the world when it was never suppose to be available to the world in the first place. With new laws in place the producer is going to be forced to make that extra step to make sure that the consumer is safe along with their data. My selected ethical tool is consequentialism and I believe it fits this case quite well. There are consequences for each action any person takes, whether they are good or bad consequences there are consequences. The consumer uses the producer’s platform and the consequence for that is allowing them to use their user data, but the producer allows the consumer this platform but does not have any consequences for data breaches and losses other than maybe the consumer not using the platform anymore, but the consumer is still at a far greater loss. Therefore, there needs to be laws, rules, and regulations in place, so the producer must make sure this data is secure and protected. Without any laws then the producer can do virtually whatever they want with the data and not care about the consumer at all. In this case specifically the consumer did not lose anything. Rather they gained knowledge about how their data is used and available to the public. A utilitarian believes that consequences of an action are good when the consequences benefit others in the world. The consequences of the producer are bad in the case because they negatively affect the consumers. However, in Europe where the GDRP law is in place the producer can positively affect the consumers while keeping them and their data safe. I believe the researchers did this in good nature and to expose how much of a faulty system we live and use.

There were a few central concepts from Elizabeth Buchanan that I like and agree with. One of those concepts is using user data to seek out ISIS and other terrorist organizations. This is a good use of using people’s online user data. Seeking out ISIS or other terrorist organizations and finding out their plans and recruitment process can help prevent major terrorist events and major deaths. Shutting down their programs and accounts so they cannot recruit people for their future malicious acts is a great way of using what we have at hand. In this case police and FBI can track criminals on Twitter or Facebook and see what they are up to, what they are planning to do, and able to stop them from doing anything evil to the public. I never thought of user data being used like that and it is such a good example of using data for good and not evil. With this data the police can make a safer environment for people by eliminating a threat before it is shown in public. My ethic tool consequentialism is great for this example. The police are using data for good and therefore creating good consequences for the world. Another concept I gained from Buchanan is that one person may agree with someone else’s data being used for something however does not want their data to be used in the same way. I thought this was very interesting because it makes sense and makes the person contradict themselves. I want the police to be scanning for terrorist organizations and attacks however I do not want the police to be scanning my data either. This also falls into consequentialism because I allow the police to track terrorist’s data, but my consequence is they are also tracking my data as well. I am okay with this because if the terrorist’s data is being tracked then that is adding better to the world than if it was not tracked. Another concept from Buchanan that struck out to me is she mentioned that people often have their profiles open to the public. I have all my accounts on private and only allow people I know to be able to access them. Some people have their accounts wide open with all their information and photos accessible to the public. In this way I believe their data should be easily obtained and there should be no problem with it. Whatever someone posts online is online forever. It is up to that someone to figure out who they should allow to access their information. This falls into my ethical tool consequentialism because a person who posts on a public account so they can reach to more people is paying the consequence of all their information and photos to be seen to the public. If they did not want their information available to the public then they would make a private account instead, but since they want more interactions, they have to bear the risk of being watched and having their data analyzed.

I am a strong believer in that the United States need to implement some sort of law or system like Europe has. The GDRP is a great tool for consumers safety. As evolving technologies climb to higher heights, the security for these technologies also need to be increased. Big corporations can take advantage of ignorant consumers or consumers in general. Laws such as the GDRP should be in place in the United States to ensure the safety of the people. This would also force big companies to take a step forward and start protecting the people who support them. I believe the consequences of the consumer is to allow these companies to use and analyze their data for the good and not evil, and the consequences for the producer is to protect the data that they are using and analyzing. If the producer cannot come to these terms and protect the people, they should be penalized and fined heavily.