2.4. Case Analysis on User Data

Cybersecurity threats, attacks, and data breaches have increased in recent years, and everyone wants to ensure they are not victims of unseen/known attacks. With products like Life-Lock now a part or an additional feature to antivirus, I think the United States should adopt something like Europe's new privacy Law. The European Union's (EU) General Data Protection Regulation (GDPR) policy has been in effect since 25 May 2018. It is a privacy protection plan that applies to any organization operating in the EU or providing a service. The GDPR protection goes beyond typical data protection, including IP addresses, genetic data, and biometric data. Any company that violates the policy will be fine. Additionally, organizations must report data breaches and inform the individuals affected. The EU's GDPR is a good policy template for the US to model because the EU is holding organizations accountable for violating privacy laws. Also, they ensure that the victim gets notified instead of finding out when they try to buy a house or car. In this Case Analysis, I will argue that contractarianism shows that the United States should follow Europe's lead because that would benefit everyone. They hold organizations accountable and instill trust in the public that their data is protected. The United States would be morally entering into an unspoken social contract between the members of society to demonstrate their willingness to protect their private data. Both Zimmerman and Buchanan's articles are concepts of contractarianism however, Zimmerman's shows how the contract was violated while Buchanan's identifies with the concepts of contractarianism.

In Zimmer's article, he explains how the ''Tastes, Ties, and Time'' (T3) research group publicly released the Facebook profiles of college students after their research was completed. The T3 research group implemented what they thought were enough measures to protect the personal information of the students in the study. By conducting this research, T3 entered a contractarianism social contract with the individuals of their examination and had a moral obligation to ensure their privacy data was maintained. T3 failed to uphold their social agreement when the Facebook profile became public, and they began to deny any fault on their part. A series of systemic errors resulted in the information being public knowledge due to their research violating the social contract. Although they ensured the removal of names and identification numbers from the data occurred, they released a codebook with distinguishing features and data like the number of personnel in the study, the general location of the University involved, and all publicly available. Another failure was that Tastes, Ties, and Time did not remove or add additional or multiple individuals to the unique majors in the codebook such as Near Eastern Languages and Civilizations, Studies of Women, Gender and Sexuality, and Organismic and Evolutionary Biology. It is commonly known that an individual can aggregate enough information to identify someone if they have enough sources or data to pull from and that is exactly what happens. Danny DeVito stated in *Batman Returns* "a lot of tapes and patience makes all the difference", nowadays you can use programs and algorithms to piece together the information you need much faster than the tapes and patience method of the past. T3's failure to maintain the anonymity of the subject of their researcher resulted in a breach of the moral social contract and to make matters worse they denied any wrongdoing on their part after the data was public.

Tastes, Ties, and Time research group publicly released the Facebook profiles and instead of taking accountability for their actions, they played the veil of ignorance card. They claimed that they sociologists, not technologists, a hacker could do the same thing via Facebook and that none of the data they have isn't already on Facebook. Hidden behind the veil of ignorance is unethical and shows the utter disregard for contractarianism in this case. It's finger-pointing to take away the

focus from T3's mistake, which ultimately was caused by their research. The contractarianism social contract was violated by 3T because they did not ensure that their research and the anonymity of the profiles were maintained, which would have mutually benefited both by allowing the anonymity of the subject and allowing a successful multi-year research project. The United States should use this information to aid in creating a policy like the EU on the basis of contractarianism, which would benefit both parties. You can learn much from the mistake you made, just as much as your successes, and in this case, the United States could use this as an example of what not to do and to help get their police approval. If they had had a privacy law, the Government would have held the TE accountable, and the affected would be aware of their privacy breach, or this might not happen.

Buchanan provides an article that identifies with the concepts of contractarianism. If the United States were to create a privacy law like the EU, I think the underlining contractarianism social contract of Buchanan's article is a reason to follow. The ethical issue in question is whether or not the method of big data mining is for online extremism and supporting the communities of ISIS on Twitter. This is a justification for contractarianism because it benefits the protection of the people of the United States and assists law enforcement and intelligence agencies working to become technologically knowledgeable with social media. In this situation, there is a moral responsibility to use big data mining to ensure the United States protects its people, resources, and critical infrastructure from terrorism. The article states that data accessible to researchers, law enforcement, and other agencies are mined from public accounts. Additionally, there are exceptions, policies, and laws to supersede the normal policy/guidance when it comes to terrorism. We have seen it in movies all the time when a government agency takes someone, a document, or a piece of equipment, all in the name of national security. This would be a situation like that and the United States' social contract to protect the country would be the reason for big data mining to identify terrorist and their supporters.

There is going to be pushback on the opposite side of the United States social contract because of the ethics involved in a situation like that. For example, the question was brought up about individual privacy and informed consent. If all the information is public knowledge, there shouldn't be an issue of privacy. There should be a balance to identify what is public and private information, which has been difficult with the amount of information accessible on the internet these days, but that is why I think the United States should follow the EU's policy and develop its own privacy policy to aid issues like this. Another ethical issue that was concerning was the impact of not reporting on the data. The impact could lead to significant harm to the United States if the data identified a terrorist cell or sympathizers and they were planning a large-scale attack that could have been prevented. The use of technology is increasing by the adversaries of the United States, some are state-supported and some non-state-supported, and we need to keep up with them just to state ahead the facts of Buchanan's article to support the contractarianism ideal because it benefits the country and its people. The government should follow EU privacy law example.

In conclusion, cyber threats are on the rise and will continue as the world becomes more dependent on technology. The EU has developed a privacy law that affects organizations within and those outside organizations that support and conduct business with the EU. This law holds organizations accountable for their violations and requires those affected to be notified. The EU's privacy law is a good policy for the United States to follow in developing its own because it demonstrates contractarianism morality by showing the mutual benefit of enforcement of the policy and accountability. Additionally, the article by Zimmer and Buchanan shines a light on a social

contract in opposite ways. Zimmerman is an example of the violation of contractarianism and how the T3 group uses the veil of ignorance instead of being accountable for what they cause. Buchanan's article shows the underlining concept of contractarianism by using big data mining for law enforcement and agencies to identify terrorist organizations and supporters. Both articles demonstrate a social contract and can be used in efforts for the United States to model its privacy policy after the EU's.