Christine Jimenez

Mr. Montoya

Phil 355E

9 January 2022

User Data

Should the United States adopt something like Europe's new privacy laws? In 2016, Europe decided to implement a new privacy law known as the General Data Protection Regulation or GDPR. In simple terms, the General Data Protection Regulation according to Danny Palmer, the author of the article "What is GDPR? Everything you need to know about the new general data protection regulations," is a set of rules that helps in giving citizens more regulation over their personal data/information. It brings focus to things such as personal data, privacy, and consent all pertaining to the day in age we live in today, where everything around us is simply technology-filled. The things that could be protected are one's name, address, photos and go so far as to also keep the individual's IP address personal also. Palmer suggests that everything around us has some sort of our personal data, whether it be social media, bank companies, retailers, or even the government. The upside to this new way of privacy protection is that it obliges organizations to ensure that anyone person's personal information has been gathered legally and under all the right circumstances. So, yes, the United States could benefit from the implementation of GDPR, but there are also many setbacks that could be the reason we have not chosen to pass on to new ways of privacy laws.

In a study written by Michael Zimmer titled "But the data is already public": on the ethics of research in Facebook, Zimmer discusses access to data through Facebook. He says,

"Recognizing the privacy concerns inherent with the collection and release of social networking data" (Zimmer 2010). The study focused on college university students' Facebook accounts and the release of their profile data. While it is never ethically right to breach an individual's personal data, Zimmer addresses the many ethical concerns relating to any other future studies on social networking sites. Research on social media security issues has been an ongoing issue for several years now, we especially see this through all the about Facebook. Facebook has had constant problems with security breaches and having access to people's personal information. Individuals often put a lot of trust into social networking sites, such as Facebook, Snapchat, Instagram, and so on, for the purpose of keeping in touch with friends, family, and many other reasons. When a company is not able to have control over their systems and is allowing for these security breaches to occur, they lose their clientele's trust.

So, how can this relate to deontology or Kantianism? First, we must focus on what deontology is: "the focus on people's reasons for acting in considering whether a particular action right or wrong." An example of this is killing someone to save your family. If a robber or murderer comes into your house and you kill them to save your family, Kant believes that this action is ethically just. Immanuel Kant's view on deontology suggests that an individual can perform an action that could eventually result in a good thing, even though the action could have or might have been motivated by bad reasons. In this specific case, social networking companies are ignoring the principle and are not focusing on the main result at hand. Simply put, if an individual downloads a social media app and signs up for it, they are putting trust into the app to manage and keep secure their data. In any case, it can become occurrent that the social media loses access to the individual's data or tampers with it purposely. Another way we see that social

media networks can sometimes use user data to their advantage and be the upper hand is when they take people's information and give it to third parties. In the end, these media apps are obliged and have the job of keeping information safe as opposed to using it against people. While Facebook has made a reputation for breaching privacy, it is their moral obligation to do as they say in their privacy terms and conditions. That is why it is always so important to read the terms and conditions of any applications or websites you are going to use because, in the end, you are the only person who can truly protect your own information and keep it secret. On another note, in relation to Europe's new privacy law, GDPR could be useful in the lawful guarantee that no one's data or information can be leaked or tampered with, but this guarantee can be quite difficult to deal with because new ways of hacking occur every day in our lives.

In a research article titled "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL" by Elizabeth Buchanan, she reflects on social media research and the ethics of data mining methodologies. A strong point she wrote was "Thus, one may implicitly agree to one's data sources being used for marketing purposes while that same person would not want their data used in intelligence gathering" (Buchanan 2). She makes a very strong point and it is something that is definitely worth discussing, different individuals are always agreeing to what they are okay and comfortable with being exposed to. That is why specifying specific terms is very important. She also takes into perspective, Benigni et al's paper and incorporates that data can be held by researchers, law enforcement, and others. When using social media the users should always be able to know who has access to their data and why. By implementing the use of GDPR, this again is pointing out the fact that having it really could be beneficial. Veering back to the article by Palmer, he says, "There are two different types of data-handlers the legislation

applies to: ‘processors’ and ‘controllers.’ A controller is a “person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing personal data,” while the processor is a “person, public authority, agency or other body which processes personal data on behalf of the controller.” That being said, applying these laws that are already being used in Europe can help many Americans.

How exactly does deontology relate to this research project? Buchanan writes, “The last time the United States federal regulations around human research protections were revised was 1991, and were not reflective of the emerging technological changes just beginning to affect the research enterprise” (Buchanan 3). This again agrees with the point that Immanuel Kant makes. One way to look at is it by understanding that collecting social media data or profile data is a means to an end. No one’s privacy should ever be compromised and that is why privacy conditions are made, so no person can use their personal data against another person. While I previously mentioned that social media companies have access to user data and can use it in ways such as handing it over to third parties, they are not choosing to do so with malicious intent. The only case in which an individual should ever have information out about them is if they have committed any sort of illegal activity, but even in that case there is still information that should and can be kept private.

In conclusion, I believe that incorporating the use of General Data Protection Regulation is useful and would be a great way to maintain security in America. It is not only good for the individuals using social media apps or other websites alike, but also very beneficial to businesses. It essentially maintains control over who has access to data and why. While Europe first started to implement GDPR in 2016, the United States still has yet to decide whether or not

they would like to implement it as well. Although it is not yet here with us today, there are a few regulations that come close or use similar ways that GDPR does. All in all, one of the most important things to remember in today's world is to keep secure your data as best as possible.