Case Analysis on User Data

In Danny Palmer's article on the digital privacy legislation in Europe, it explains how Europe regulates general data protection and gives European's more control over their data. The GDPR is a set of guidelines that make the privacy regulations of businesses and citizens easier. The general data protection regulations establish that the data is collected legally and under strict conditions. The people that manage the information protect it so it is not misused or exploited. The definition of personal data in Europe is exceptionally different from the United States because it includes your name, address, and photos. But with GDPR, it is expanded to include IP addresses, genetic data, and biometric data. In this Case Analysis, I will argue that deontology shows us that the United States should follow Europe's lead because they are making everyone's privacy their concern, so the citizens don't have to do so.

One concept Michael Zimmer's article, *"But the data is already public"* had was the idea of improper access to someone's data that the research team using in-network research assistants was an unacceptable way to go about collecting the data. What if most participants set their profiles up only to allow people in the Harvard network to view their profiles? To foster a sense of community against the people they go to school with and live nearby. Making it so that anyone outside of that community to view their profiles, something that outside research assistants would not be able to do. But by them using research assistants that went to Harvard or were already in that community took away those privacy efforts of those profiles that they collected. That because these students had accounts that the research assistants had access to does not make them public, their privacy settings could have blocked everyone but Harvard students making them private. But they disregarded those students' privacy and not giving them the respect to use out-of-network research assistants. Whether to bypass those problems intentionally, or they didn't care to honor those students' privacy.

The deontology concept, specifically Kantianism, says those 1700 students should be respected and valued as the end in themselves. Not as simply a data set to satisfy the need to study them because they can. Even though no harm came to them and ultimately none of them identified, it was still immoral to violate their privacy without their knowledge. Saying nothing used from their profiles wasn't already out in public for those to see should not be the argument. The ethical imperative should have been to respect their autonomy, and that should have been

motive enough to use outside research assistants. That should have been their duty to provide those who wanted independence and set their profiles to the security they wanted to be respected. Including them in the data set even though they might have had information that they did not wish to publish to the outside world.

I think that they should have let the 1700 students opt into the data set or at the very least tell the students that a research team was on campus and they might be in the study. Could that have changed the information they got, maybe? But the students would have been made aware that they would be giving up their privacy should they participate in the study. Because people post their information on social media sites doesn't mean the information is for the masses, nor should it be collected without their knowledge. We all treasure privacy, and the European Union has the right ideas for what is considered PII. Even with the research team's measures to deidentify their research subjects, it was still possible to determine where the data set came from without access to the actual data. But if the United States defined PII as the EU does, more than half of the information used to figure out what university it came from would not have been included in the data set.

Elizabeth Buchanan's journal about data mining to identify ISIS supporters displays an idea that the methods are valid and reliable. But saying that this process can tell who should deserve to be observed has nothing to do with it is a violation of their privacy. Producing an algorithm to look at patterns across a data collection, unbeknownst to the subjects, is sketchy at best. For example, Benigni et al's paper is trying to pass the concept mining public open accounts is not a violation of privacy. He is purposing that the end outweighs the means of a person's privacy and national security. Keeping our national security secure and safe is a great idea, and no one is trying to keep them from doing so, but at what cost. Europe's privacy laws aren't taking anything from their national security, but it ensures that their citizens' rights are intact. Kantianism says that the citizen's privacy should be respected no matter what, that they are not a means to an end; they are the end.

Doing what is suitable for people and treating them as human beings is the essential thing to Kantianism. They are not harming them by mining their data, but is it moral to do without their knowledge. Using the justification that the information in public doesn't mean there shouldn't be privacy concerns. In Europe, people's IP addresses are considered PII; even though they can be public, they can still identify them. If we had those privacy laws, they would not

mine the data the way they do now. No argument should start with the phrase, “It is public, so they lose their rights.” We are moving in the direction of a more online world. We can’t lose our sense of privacy just because we post on social media. If we were haven’t a conversation in public, would it not still be considered private if it was between two people. The police use social media posts in criminal cases, but where does the expectation of one's personal space on their Facebook or Twitter accounts.

I believe that we should follow Europe’s lead and define PII stricter, including pictures, IP addresses, and anything else that can infringe on individuality. Companies and law enforcement would probably have to work harder and change the way that they do business. But, with so many data breaches and so much personal data leaked online, people want to feel safe while on the internet. The need to do the right thing and either get the bad guys or collect data to better one’s understanding doesn’t mean you to do what you can to accomplish your goals. We could have the social media sites block posts or flag posts that pose a concern and let them know the entry and future posts will be looked at by the proper authorities because of content. Make people aware of a potential violation of privacy because next time, it might be your privacy next.

My position is that the United States would greatly benefit from adopting the European Union's policies. There would not be less confusion about what is allowable or what violates someone’s privacy. No one would have to watch what they say on social media because a program could accidentally mark you as being a terrorist. Protecting everyone’s privacy should be the primary goal of any program or data set. Because the information is out there and seemly accessible doesn’t make it private. It just means people are expressing their rights. You should be able to expect to have autonomy over the internet if you have expressly broken any laws. My social media is just that my right to say or write what I want without someone mining my data or likes and dislikes. People's privacy should never be a means to an end; the person should matter the most.