Alex Bonhomme
User Data Case Analysis
PHIL355E

Should the United States adopt something like Europe's new Privacy Laws?

This case presented by senior reporter Danny Palmer was an informational article on what GDPR is exactly. After giving context as to what GDPR is, Palmer went on to explain what it means as well as how it impacts individuals and businesses. As a main reflective point, Palmer discussed how to ensure compliance with GDPR among the countries in the EU. GDPR stands for the General Data Protection Regulation and is the standards of the European Union (EU) that came into effect on May 25, 2018. The GDPR was implemented in place of the 1995 Data Protection Directive. Some main points that we should consider about the implementation of GDPR in relation to User Data Privacy should be what it means for businesses, what it means for consumers, and what comes next for GDPR. While explaining central concepts from both Zimmer and Buchanan, I will analyze this case through the lens of deontology. Through deontology, I will argue that the United States should follow Europe's lead to widen the scope of user data safety through the delineation of case studies and examples.

In the excerpt of Michael Zimmer's article, we cover the ethics of research in Facebook. He specifically discusses a previous social research project in 2008 entitled "Tastes, Ties, and Time" (T3). The dataset recorded for "Tastes, Ties, and Time" is comprised of 1,700 college students and their 4 year career at a university in the United States. More specifically, the data recorded pertains to what the entire cohort of students had posted on Facebook throughout those 4 years. Now they made the students' names and ID numbers anonymous, while implementing a terms and conditions for other researchers to use their studies to account for privacy. These measures ended up being futile in that the data and the identity of the school was exploited. This study reveals various gaps in T3's researchers' understanding of privacy risks related to their project. Through analysis of these precautions, Zimmer portrays the insufficiency of the 5 privacy protections in the T3 project. In relation to these precautions, the GDPR case presented by Palmer included what GDPR means for consumers and citizens in the EU. A method that should have been taken from GDPR and used in T3 is that citizens (or in their case the students) should have been reported when information about them was exploited. However, one ethical point that they missed was letting the students know they were being surveyed in the first place. The students' information was gathered through Facebook posts and mutuals after getting the initial information from RA's (Resident Assistants).

Problems with the initial data from Facebook profiles arise in the use of in-network RA's. Before I discuss the problems, lets include its correlation to Deontology. Deontology focuses on people's reasons for acting in considering whether a particular action is right or wrong. Specifically, what one should do in any given situation is the action that is based on the best reasons. Now although this is a project in research for social science, and there are precautions regarding the privacy of the students, the way that the data was obtained was unethical and deviate from a Deontological perspective. I have already delineated how the student's

information was gathered through university Residential Assistants. The main privacy and ethical downfall regarding the RA's ability to see students' profiles lied in the fact that some people might have their privacy settings to only be viewable to others in the network, and say the network classified as the university that student went to. In this case using the profile, posts, and information from students who keep their information private are ethically and inherently bad, thus differing from the deontological manner of being ethical in everything you do, and every action taken. The researchers with T3 should have gotten a survey of consent from the students and acquired their data that way. As mentioned before, students should have been notified when information about them was exploited, since the data collected contained identifying characteristics, whether the researchers noticed or not. Now this would be hard pill to swallow considering the fact that they didn't let the subjects know they were being researched and observed in the first place, but there definitely should have been more communication between the subjects and the researchers.

Elizabeth Buchanan discussed the ethics of big data research – but through a case study on supporting communities of ISIS or ISIL on Twitter. Buchanan delineated how researchers Matthew Curran Benigni, Kenneth Joseph, and Kathleen Carley presented an Iterative Vertex Clustering and Classification (IVCC) model to identify supporters of ISIS or ISIL throughout Twitter Users. Here, we discuss the morality of data mining vs the efficiency of the methods of finding these people as data has become so readily available. The GDPR is directly mentioned in this excerpt and how these methods may come into question when the GDPR is established. One part of this piece that directly corresponds to Deontology is where they emphasize a respect for those under observation in research. With traditional ways of research, information is gathered from human subjects with individual consent, but with technology, it is easy (but not right or ethically correct) to bypass this. A main issue that Buchanan discusses is the complexity of the domain of research and how data subjects are viewed currently. Are data subjects considered people? Or just subjects? And if so, do they have rights / are they subject to give consent on accrued data?

Regarding the bigger scope of things, is this type of research moral? It seems nice in the way that it outs those who support radical groups such as ISIS and ISIL, but the same technology is used in our social medias to figure out our patterns in work and home routes, where we shop the most, and even what we like to eat. While we may think that we govern our daily activities and routes, we are still being observed through the data mining of our social medias, cellular devices, and other objects. In other words, no matter what, we are observed without our consent, not following the standards of deontology or plain ethical standards at all. If anything, this was a good project to accomplish their goal of finding those who support radicalized groups such as ISIS and ISIL, but morally, they are in the wrong. Using social media, there might not be a morally and/or ethically correct way to accomplish this task, but if they were to take the ethically correct road, here is what I would recommend. People would not be traceable due to privacy regulations, but what one could find is organizations. To keep the deontological view of keeping respect for the third party (in this case, the supporters on social media), I would recommend finding the organizations as there are places where they do organize and meet. Once found, they can perform a bust on their meeting, and find out possible activists and

supporters through the meetings. That would be the right thing to do overall in my opinion, but I understand that it would be next to impossible to find the actual supporters and activists of radicalized groups this way. There has been a shift in individual data subjects in that instead of using information to build networks, we now also use this information to get a closer look at one's lifestyle and choices. Everyone should be more than the sum of the information behind their social media accounts.

People should account for more than what their social media and sensitive data have to offer. Regardless of the content, the sensitive information should be given through consent when necessary for research purposes and other observational purposes. Concepts from both Zimmer and Buchanan were portrayed in how big data companies was unethically drawn for research. The point was to make sure that researchers gain a better understanding of the context behind privacy in these areas. It is not just enough to implement them after personally identifiable information has already been gathered. Another place to improve on is to make clearer what classifies as consent. The T3 case that Zimmer discussed proved that concerns about consent / privacy / anonymity do not disappear just because on is socially active online – in fact, it becomes even more important to protect them. Through the lens of deontology, I have argued that the United States should follow Europe's lead to widen the scope of user data safety through the delineation of case studies and examples.