Joseph DiGennaro

PHIL 355E

25 May 2023

2.4. Case Analysis on User Data

In the article by Palmer, it is explained that general data protection regulation, or GDPR, is essential to the EU's privacy infrastructure. It is a fairly new setup that allows for major changes in the way that data is handled and managed. GDPR also requires compliance with many various factors, and has very hefty fines for mishandled data breaches or non-compliance. The fines start at a minimum of 10 million Euros for falling out of compliance. Not to mention, if two percent of a company's annual revenue exceeds 10 million Euros, then the fine is a yearly reduction in revenue by that percentage. The fine is whatever is greater in monetary value. GDPR also gives consumers more monitoring over their data, and they can ask for their data to be deleted at their request, once it has been verified that there is no foul play involved. Businesses are required to document how they handle data, and keep consumers in the know. Palmer even explained how Tim Cook, an Apple tech giant, had called for "the US to introduce an equivalent to GDPR". In this Case Analysis I will argue that the deontological tool for moral reasoning shows us that the United States should not follow Europe's lead because it limits free will, and puts a heavy burden on those who must maintain compliance.

Zimmer makes many valid points throughout his paper, and presents two theories in particular that indicate a moral theory. These theories are a harm-based theory, which is more of a utilitarian theory, and a dignity-based theory of privacy protection, which is more towards a deontological view. Due to the deontological tool being used for this selection, this analysis will

focus more on the dignity-based theory that Zimmer mentions. A Dignity-based theory tends to keep morality into perspective. Zimmer states, “Ethical issues in human subjects research received considerable attention, culminating in the scrutiny of research projects". Also, Zimmer presents a unique question in privacy ethics in the way that the research data was gathered. Data gleaned from social media was analyzed over the course of years, and connections were able to be made. Though the researchers had made good-faith efforts to hide the student information and university information, the exposed data put the test group at risk.

When looking at the GDPR situation in the EU from a dignity-based perspective, the goals of the regulations seem to make life more safe and secure, but it comes at a cost. This theory based on dignity highly emphasizes the wellbeing of the community. Although the GDPR regulation appears to do that, it actually hinders wellbeing due to the highly complicated nature of the legalistic regulations. Not to mention, many false GDPR compliance emails were sent to customers during the time businesses were required to send consumers their GDPR data compliance information. These emails were actually phishing scams that stole user credentials, credit card information, email addresses, passwords, and the like. Hackers capitalized this time to take advantage of the situation. It is quite ironic that the exact thing GDPR set out to destroy, that is data and privacy breaches, is actually what allowed the nefarious attacks to occur. Zimmer’s research of good-faith also ties into GDPR in relation to how much is enough. In the 2008 research study, even though good-faith attempts were made the data still leaked out into the public. However, under GDPR, what will constitute good-faith measures? Failure to comply is a minimum of 10 million Euro fine, so how do people make sure that they are in compliance? This

poses a new challenge for businesses, as they could instantly go under if they make a wrong move, even if it had no malicious intent.

Kant explains how respect for others is highly important. People are supposed to be respected, and not used to achieve a means to an end. Zimmer covers the 2008 incident well, as he helps to bring into question the ethical side to research. Oftentimes, research tends to consist of the researcher(s), and the test subjects or target group. In this case, the results of the research actually put the data subjects in danger, which goes against Kant's duty to respect others. The data subjects were not given the proper respect when their highly sensitive information got leaked due to the research program. It seems as though the ends, or results of the 2008 research were prioritized over the safety and well being of the data subjects, which is never alright to do under Kant's principle of the absolute duty to respecting others. The unfair fines under GDPR issues will inhibit growth, and only ensure compliance out of fear, as Kant mentioned that one could do good things that were motivated by bad reasons. Instead, compliance should be about community building, that way it is done honestly and without bad motivational factors.

Moving onward, Buchanan's paper brings a very important factor to light. That central concept is data gathering, specifically, the methods in which it can be gathered. In today's day and age, data gathering is easier than ever! Buchanan mentions how Iterative Vertex Clustering and Classification (IVCC) can be used to filter through large data sets. Oftentimes, this can aid marketing professionals, and those who are trying to find a certain type of data subjects, like the FBI or law enforcement. Using IVCC, data sets can be thoroughly searched, and certain keywords within the search can result with precise matches. This concept is critical to understanding how research can take place today, and in the future. Many times, researchers are

using this data without informing the data set, as it is typically public information. Buchcanan explains how this data is becoming more and more valuable to the intelligence community. Another important fact to mention is the fine line between consent, and what is done with that data that the individual has consented for use. Buchanon mentions a great example by comparing marketing VS. intelligence purposes. For example, a user that agreed to a certain marketing campaign or purpose, has provided consent for that purpose. However, the user may not have consented for that data to be used in an intelligence campaign for demographic research. This fine line can cause problems that researchers need to be aware of.

When looking into GDPR, data gathering will most likely increase. Also, intelligence will likely increase due to elevated cyber threats. Not to mention, many service providers have had to stop catering to areas subject to GDPR due to fines. As mentioned previously, the minimum fiscal fine is 10 million Euros. So quite simply, service providers would rather stay away from EU users than risk a fine that could put them underwater. Data collection, specifically using IVCC methods, could cause big problems when used in the wrong way. Buchanan explained this in the marketing VS. intelligence example. What protections are in place to protect data that is supposed to be for one purpose from being used from another? GDPR requires many legalistic assessments and compliance data. This data will most likely be filtered through the GDPR system. Keeping in mind, this data is to be used by GDPR to show that the business in question is working properly. However, when this data is acquired, it could be used to target businesses with a low compliance score. For example, if GDPR wanted to send out fines, they could simply use IVCC data clustering methods and fine all businesses who had not shown proficiency by completing the latest compliance assessments.

The denological tool for moral reasoning can definitely be applied in this situation. Buchanan mentions that the IVCC methods can result in data grouping or clustering. Essentially, data can be grouped together and searched with ease. All that is needed are the search fields and/or keywords. Kant believes we have a moral duty to others. He explains that the right thing has to be done, even if that makes it a hard treacherous walk. It is no surprise that most will want the easy way, not the hard way, which can easily cause people to go astray from Kant's principle. Also, consent is essential in Kant's position. If people have not consented to something, and it is done to them anyway, then they have been violated. Being violated shows a lack of respect for the individual, which goes against Kant's principle. Not to mention, the fines that are laid upon people handling data are extremely deceitful, as they seem to take advantage for financial gain. A world where free will and consent are present can surely be a step in the right direction to solve this problem with GDPR.

In summary, there are many reasons why GDPR violates Kant's position, and the deontological tool for moral reasoning. Both Zimmer and Buchanan present interesting and valid points about research. Zimmer focuses more on a dignity-based theory where morals are more prevalent. He makes the connection between data, and the ethics behind how it is collected. Buchanan shows the same point, but from a different perspective. He explains how this data that was once collected for a specific purpose, can now be weaponized through IVCC methods. IVCC allows for searching of clustered data sets, often which are used for research/intelligence purposes. All of which can apply accurately to the GDPR situation in the EU. Some may argue that pushback on the GDPR program could inhibit cybersecurity and privacy, which may be partly true, until they are hit with a 10 million Euro fine for a simple mistake in handling data.

Works Cited

2.2.a Zimmer, M. (2010). “But the data is already public”: On the ethics of research in Facebook. Ethics and information technology, 12(4), 313-325.

2.3. Buchanan, E. (2017). Considering the ethics of big data research: A case of Twitter and ISIS/ISIL. PloS one, 12(12), e0187155.

https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/