Ava Baratz

CYSE 355E

Professor Montoya

September 22, 2022

Case Analysis On User Data

General Data Protection Regulation, or GDPR, implemented in 2018 by the European Union, is a list of guidelines organizations adhere to to ensure the protection of their users' data. The GDPR framework establishes necessary transparency between organizations and consumers as data is accurately logged and properly protected. GDPR allows citizens to become knowledgeable on how their data is being used and collected ethically. With GDPR, navigating user data is more easily accessible. This encourages consumers to place more faith in organizations to be forthcoming on actual reports of user data. In this framework, companies are required to directly report breaches to the consumer within 72 hours of the incident. If companies do not comply with breach incident notifications, they can face penalties, including extensive fines of 10 million GDP, (Palmer, 3). Additionally, breach notifications are required to include details of the breach that are helpful to consumers, including types of personal information that were leaked, how many parties were involved, and the consequences resulting from the breach. This framework promotes accountability within organizations and promotes the privacy of the consumer at the forefront of product and service design within all organizations. In this Case Analysis, I will argue that utilitarianism shows us that the United States should follow Europe's lead because user privacy will become a priority, companies will

rightfully be held accountable due to framework disobedience, and public trust in companies will drastically increase.

Professor, Micheal Zimmer, in his published work, *But The Data Is Already Public,* illustrates the fallacies in the lack of ethics Facebook displayed in a college research study in 2008. The social media giant, Facebook, executed a research program that aimed to gather extensive information on a freshman class that would help understand user data and algorithms on the platform. After four years of collecting data, Facebook released the data publicly and the subjects that were researchers were easily identifiable, ultimately compromising their safety. Although Facebook attempted efforts in hiding identifiable information, such as names and student identification numbers, Facebook included invasive data, such as ethnicities, political views, and financial status that were used to identify individuals utilized in the study.

This research raises concerns to an array of ethical concerns in gathering and collecting user data. One of the most noticeable concerns is improper access to data. Facebook failed in gaining explicit consent from participants in the research. The students that were a part of this research were not aware of the types of data that were being collected, the way their data was stored, and how their data was ultimately going to be used. Additionally, these participants were not granted access to the data, (Zimmer, 2). This creates difficulty in verifying the information that was collected. Because of this, the data that was published has a high potential for being inaccurate. Facebook claimed this study was intended to be used to identify data and patterns among college users present on their platform. However, this can become difficult to understand as Facebook continued to intrude on the college student's privacy as they continued to gather invasive

information for years that was not intended to become public knowledge. Facebook failed to consider the privacy of the students by disregarding the fact that many accounts have their profiles private to the general public. Some profiles only want to share information with the networks they belong to with people they know. By having a private profile, a user feels protected as their information is safeguarded from the dangers present in the digital world. Facebook disregards this matter by continuing to collect data and publicly posting it without fully removing identifiable information of the subjects that were involved. Ultimately the researchers disregarded the need to be transparent in the intentions of the data that was collected and failed to acknowledge the unethical practices Facebook used to collect data. To prevent these ethical concerns from arising, Zimmer suggests implementing access controls and consent in collecting, viewing, and storing user data. He argues that articulating an acceptable use of data to consumers will allow for clear knowledge of how an organization plans to utilize user data.

Zimmer's suggestions on increasing privacy protection closely align with the European Union's GDPR. In the framework, one of the main concerns is to ensure that user data is completely protected. In the GDPR, access to user data is extremely limited, and safeguarding that information is established as a serious matter, as the Union threatens fines for the liable party that causes harm to any data. The GDPR places emphasis on a company asking for consent before collecting any data from its users. This framework ensures honest and reliable communication from companies to their users. Facebook's efforts in this research do not align with GDPR standards because they did not ask for consent when gathering information on the subjects involved in the research study. Facebook displayed a lack of ethical concerns when conducting the research that

resulted in the subject's identities being compromised for second parties to use to their advantage.

Although GDPR may limit access to specific websites, such as international journalism sites, the implementation of this framework in the United States would ensure that users' privacy is the priority. We can view the GDPR through a utilitarian lens that allows us to see the benefit for the entire world rather than the individual. This type of data collection would benefit a select amount of people greatly, such as the researchers that rely on this type of extensive data. However, because of the immense harm and ethical concerns carelessly storing and using user data, there must be an approach implemented that values the overall protection of user data. If the United States implemented a framework, such as the GDPR, it would provide greater benefit for the general public, knowing our data is protected and completely transparent. This framework can be viewed through a lens that limits minimal harm to users and provides extensive benefits in return. Specifically when discussing this Facebook study, if GDPR was implemented, many ethical concerns would have been limited. For example, participants would be asked for consent before Facebook would have collected any data. Additionally, they would know where their data was going and how it would be used. As a result, privacy would become the main asset to protect in the study, increasing overall trust with the social media giant.

Similar to the ethical concerns Zimmer highlights with Facebook, Elizabeth Buchanan discusses the ethical issues that arise with a group of researchers that identified users on Twitter to seek out ISIS terrorists and supporters. Although the researchers had decent intentions, the way they identified users raised concerns about user privacy and

promoted discrimination against individuals on the platform. Buchanan argues that we have become solely data subjects to these researches and that the fight for privacy becomes imperative as we increasingly rely on technology. She argues that companies need to include “reasonable expectations of privacy”, (Buchanan, 3). This states that companies need to clearly articulate their uses of data and how it affects user privacy. She argues that often individuals will agree to have their data used for a specific purpose, but companies tend to find another use for it without transparently disclosing it to the consumer.

If the GDPR was implemented in the United States, issues concerning privacy and discrimination would not arise as often. In this case, researchers would ethically gather and collect data that eliminates the opportunity for discrimination to occur for the users that are studied. If companies and researchers are expected to follow this privacy framework, the inclusion of privacy would ultimately be at the forefront of the product’s design. The use of accountability can be used to deter deviance when companies handle matters concerning data. Implementing fines that result from the misuse of data would discourage individuals from unsafe data practices that compromise user safety. Instead of waiting till damage occurs and being responsible for paying fines, companies would be more inclined to include privacy in their companies' design to evade paying fines. The use of fines as a deterrent is effective in ensuring companies consider privacy as the main right to protect their users. The use of this framework will eliminate companies from viewing individuals as “data subjects” as Buchanan suggests, but rather as human subjects that deserve honesty and protection when it concerns their data. This framework ensures that individuals are considered a priority over company benefit.

Through utilitarianism, it can be seen that a framework, such as the GDPR, implemented in the United States would be beneficial to individuals across society where safety and privacy are highly valued. This framework would alleviate most of the suffering of society by eliminating dishonest and unethical practices regarding how companies handle user data. This results in companies ensuring practices to protect user privacy as it becomes the main priority over company benefit. Users would be able to recognize how companies use and store their data. Companies would consider protecting user data more seriously as they will be held accountable by law. The implementation of fines leads to organizations preventing unethical practices before they occur. This additionally promotes the importance of having a reliable reputation as a company because of public awareness of breaches and fines that occur. Lastly, the overall trust between consumers and organizations would increase as consumers can rely on a company to accurately report any breaches of data regarding their personal information. The need to have trust in companies becomes increasingly important as more of our data is collected each day.

Through the lens of utilitarianism, it is evident that the United States can greatly benefit from implementing a privacy framework, such as the GDPR for the overall utility of society by placing importance on user privacy, ensuring proper accountability for companies not complying with the framework guidelines, and overall developing trustworthiness between consumers and organizations through transparency and honest communications. Although implementing a privacy framework of this sort may limit certain freedoms, such as accessing international journalism sites, its benefits would greatly contribute to the societal alleviation of concerns caused by improper data usage.

Knowing this, databases will only continue to grow as we technologically advance. Companies will increasingly rely on data as we adapt to more of a digital world in everyday life. Having a strong foundation between the growing companies and everyday users that this privacy framework allows for will provide users with comfort and ensure safety knowing that their information is fully protected from online threats.

Works Cited

Buchanan, Elizabeth. “Considering the Ethics of Big Data Research: A Case of Twitter and Isis/ISIL.” *PLOS ONE*, vol. 12, no. 12, 2017, https://doi.org/10.1371/journal.pone.0187155.

“What Is GDPR? Everything You Need to Know about the New General Data Protection Regulations.” *ZDNET*, https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.

Zimmer, Michael. “‘But the Data Is Already Public’: On the Ethics of Research in Facebook.” *The Ethics of Information Technologies*, 2020, pp. 229–241., https://doi.org/10.4324/9781003075011-17.