Janae Craig

Professor Montoya

PHIL 355E

13 December 2022

2.4 Case Analysis User Data

Internet users have been worried about their personal information being shared with other parties ever since the inception of the internet. The General Data Protection Regulation (GDPR) was recently enacted in Europe, making data privacy a subject of increased interest. The General Data Protection Regulation (GDPR) is a collection of rules for safeguarding personal information stored in digital form, and its implementation is mandatory across all EU member states. Users have the right to know what information is being gathered concerning them and the option to have it deleted. Businesses must get their permission before gathering, accessing, or disclosing user information, which indicates greater responsibility across firms, especially internet corporations, throughout the European Union. Despite the federal government regulating online space, there is no such collective body in the United States. The publications by Zimmer and Buchanan examined below highlight data privacy situations that can be avoided to improve the internet environment for people throughout the United States. In this case analysis, I will argue that consequentialism demonstrates that the United States should adopt the European data protection policy because it recognizes the value of personal privacy.

Zimmer's fundamental premise concerning privacy is that data shared or revealed by a person should be safeguarded and that preserving one's private data and privacy should be a priority. Zimmer brings up the issue of how organizations and scientists utilize public privacy

preferences to manage personal data while endangering people's privacy. According to Zimmer, moral considerations must be made while researching social networking sites like Facebook. Researchers should consider the possible damages their study may do to the participants on these sites since the data on them is public. The user should be given clear instructions and information. It is the obligation of the firm or social platforms he submits his information to ensure that it is kept secure and does not infringe on his rights. These Researchers also need to be looking at the potential consequences that they may encounter through their study and be able to think about if they are doing the right thing. With this new policy in Europe, users have the right to request the deletion of any personal data that has been collected about them. Before collecting, accessing, or revealing user information, businesses must obtain consent from users. Governments everywhere should act accordingly and pass legislation similar to those in Europe to ensure that everyone's privacy can be better protected and no one will be able to access anyone's personal information without their knowledge or permission. Through a robust policy such as the GDPR, the federal government can ensure that organizations address user privacy complaints and report breaches as they occur.

Another problem that Zimmer identifies in his writing concerning this ethical stance is deception. The European Union's policy on protecting user privacy emphasizes informing consumers about their options. It is crucial to emphasize transparency about privacy issues. The new European privacy regulation directly results from their efforts to safeguard their users' private data and keep their privacy intact. Consequentialism emphasizes the results of people's actions. A consequentialist believes that an act is ethical if its results are positive and immoral if they are negative. If one takes a consequentialist stance on the problem of data collection without permission and the protection of individuals' private lives, one would emphasize the potential

harms that result from violating people's right to anonymity. Violating someone's privacy, for instance, may cause financial consequences, physical and mental suffering, and future vulnerabilities. With that being said this proves why the United States should adopt this new European data protection policy because it's a way to collect data while also being transparent with the public and informing the public about their options. There may be fewer challenges and worries regarding data privacy because the public is more aware of the situation and it doesn't appear that the government is acting discreetly. As a result, people may feel more comfortable sharing more information with the government. According to a consequentialist perspective, this would benefit the greatest number of individuals. This new GDPR should be implemented by the government.

One concept presented by Buchanan in "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL" is the challenge of informed consent. She discusses how technology and social media developments have made it possible to identify Twitter users who support ISIS/ISIL via large-scale data mining and analytics. However, from her article, we see that due to the lack of regulations controlling the nuances of social media research, a "personal ethics" approach has emerged, in which individual researchers are responsible for determining what constitutes ethical conduct. The massive shifts in social media environments have given researchers easy access to petabytes of data; several high-profile research ethics controversies, including those involving OkCupid, Cambridge Analytica, and the Facebook Emotional Contagion study, enlighten us of the gravity of the ethical issues that have arisen. It is thus essential to determine whether or not the people whose data is being pulled from social media consented to have it made public before proceeding with any analysis. The terms and conditions

all social media network users must adhere to are a central point of contention. Thus, only user data that is publicly available should be gathered for analysis from social media platforms.

Another concept raised by Buchanan is the dire lack of anonymity in social media research. Buchanan does provide a substantial ethical conundrum since determining whether it is ethical to research internet platforms is difficult, especially when the goal is to uncover the activities of extremist groups. "Utilitarianism" is a popular form of consequentialism. According to a utilitarian, the proper course of action is the one that maximizes satisfaction and minimizes unhappiness. The results of an activity are considered good when they result in more good being done in the world. Therefore, to act morally, you must take action that will result in the greatest possible increase in good in the world. From a Utilitarian approach, the absence of anonymity might make possible dangers much more severe when processing social media data such as that about immigration. That entails dangers like profiling, data de-anonymization, data breach, and releasing a person's identity, geography, online community, and other private information like immigration status may lead to cyberbullying and hate crimes. Thus, decisions to preserve obtained data for no longer than is required should be taken, and appropriate anonymization or pseudonymization processes should be done as soon as possible to reduce the danger to people. That will shorten the period during which specific people may be identified. Any of these measures may be used instead of obtaining the account holders' informed agreement if it is necessary to reduce the potential dangers to their social media profiles. These initiatives can only be made possible if the United States adopts an adequate GDPR. The idea of the United States adopting this new GDPR is a great way to make American citizens feel comfortable about what's going on with their data behind the scenes. The united states would be taking a step in the consequential direction doing the most good for the most amount of people

There are various grounds against the United States adopting the GDPR. First, its implementation would be pricey. Second, it would be challenging to implement. Despite these considerations, the United States should adopt a system similar to the GDPR. The General Data Protection Regulation (GDPR) affects individuals and organizations because it gives them more authority over their private data. Data privacy is a fundamental human right, and the advantages of enhanced data privacy laws would surpass the implementation and enforcement costs. Concerning user data privacy, the case studies offered by Zimmer and Buchanan demonstrate that much work has to be done in the US internet business environment. Therefore, the United States should consider privacy breaches as a collection of consequences, necessitating the adoption of GDPR ideas into regulations that achieve beneficial results.

Works Cited

Buchanan, Elizabeth. "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL." PloS one 12.12 (2017): e0187155.

Zimmer, Michael. "But the data is already public": on the ethics of research in Facebook." The Ethics of Information Technologies. Routledge, 2020. 229-241.