Khaliyd Fuller
Cybersecurity Ethics
Professor Montoya
Case Analysis on User Data
June 04, 2023

Having read through Danny Palmer's article regarding General Data Protection Regulation (GDPR) and its impact on individuals as well as businesses, I believe that the United States should adopt something like Europe's new privacy laws. As Palmer notes, the GDPR reforms are designed based on the digital age that we currently live in, in which data is fundamental to nearly every facet of our everyday lives. It is because data is so fundamental in this era that we must take issues such regarding data protection and privacy very seriously. We entrust a great deal of our personal information to businesses online, so it is important that this sensitive data remains protected and confidential. Having something like the GDPR in the United States would be a good step in the right direction towards holding organizations accountable for data breaches and ensuring that the handling of consumer data is consensual. In this case analysis, I will argue that utilitarianism shows us that the United States should follow Europe's lead because of the major importance of private user data in the digital age.

"But the data is already public," an article written by Michael Zimmer, details important concepts including the nature of consent and respecting expectations of privacy on social network sites. Zimmer challenges the nature of consent as the "Tastes, Ties, and Time" (T3) researchers likened the profiles of Facebook users to that of a "public square," suggesting that the researchers' justifications present a false comparison. Zimmer asserts that since researchers cannot simultaneously observe the randomly encountered people within a park, the data that is gathered is imprecise and limited. However, the T3 researchers employed a research assistant from within the network of users they were monitoring who was able to systematically access the profile data of the target students over the course of four consecutive years. Zimmer argues that the researchers failed to respect the expectations of privacy that are reasonably likely to be held by the subjects of the study regarding the relative accessibility and purpose of their Facebook profile information. From an ethics perspective, users should be able to maintain a reasonable expectation of privacy when utilizing social network sites, such that their information should not be harvested or published by third parties without their informed consent. It is reasonable to

assume that users of social network sites intend for the information published on those sites to be only accessible on that platform within a network of approved users.

Under the terms of GDPR, organizations are required to ensure that personal data is gathered legally within the bounds of strict conditions, protect the data from misuse, and respect the individual privacy of the users. GDPR defines personal data as information that could be processed to uniquely identify an individual, such as a name, address, photos, genetic and biometric data, as well as IP addresses. GDPR establishes one law across the continent of Europe and requires that international businesses based outside of Europe comply when conducting business on "European soil." This means that essentially every major business around the world will be required to comply with GDPR standards. Regulations such as GDPR encourage products and services to be developed with data protection and user consent in mind. Consumers who utilize online services will see great benefit from such regulatory practices, as businesses will be required to notify users as soon as possible if there has been a potential breach of their data. Consumers will also have easier access to their own personal data in terms of how it is processed, as organizations will be required to clearly detail how they collect and manage their data as well as provide an option for users to opt-out of non-essential data collection. GDPR also introduces a clarified "right to be forgotten" process, which grants individuals additional rights and freedoms to those who no longer want their personal data processed to have it deleted, provided the company has no legal grounds for retaining it. By ensuring that individuals are given the right to control their personal data that is processed by online services, businesses will be able to comply with GDPR standards and respect the privacy of their consumers.

"Considering the ethics of big data research," a formal commentary response written by Elizabeth Buchanan, reflects on the ethics of big data research and how it challenges the traditional principles of research ethics, especially with regard to the concept of the "data subject" as opposed to the treatment of a human subject. Buchanan suggests that big data research has changed the scale and nature of information collection and analysis across many disciplines, including social network analysis. However, big data research also poses ethical dilemmas with respect to aspects such as privacy, rights, and autonomy, as it can reveal a great deal of information about individuals and their networks without their consent or knowledge.

Buchanan considers big data research to be an "awkward" fit within western models of research ethics, as it does not comply with ethical research standards, which prioritize the individual and their well-being, and require informed consent and ethical treatment by researchers. Researchers have attempted to avoid this by creating a new category of "data subjects" who may not have the same rights and responsibilities as human subjects, but who may still be affected by "downstream harms" of data mining and analysis. Buchanan suggests that big data research requires further ethical consideration and policy debate, as it can be used for different purposes and contexts by various actors, such as researchers, law enforcement, intelligence agencies, or political dissidents.

If the United States were to adopt a similar regulatory stance regarding data protection to Europe's GDPR, then we would be more in line with the ethical standards of western research. Just as Buchanan had addressed the new category of "data subjects," the third chapter of the GDPR specifically addresses and outlines the fundamental rights that data subjects hold as individuals with regard to the processing of their personal data by organizations. The chapter explicitly outlines that data subjects have the right to information, the right to access, the right to rectification, the right to erasure (the aforementioned 'right to be forgotten'), the right to restriction of processing, the right to data portability, and the right to object. These rights ensure that data subjects and their information is being respected by organizations seeking to do business with Europe. Among the outlined rights, three are of particular interest:

1. **Right to information:** the data subjects' right to information regarding the processing of their information, the purpose of that processing, the categories of data being processed, and the recipients of the data (who has access).
2. **Right to erasure:** the right to erasure, or the right to be forgotten, grants individuals the right to request that organizations erase their personal data when there is no grounds for retaining it or the purpose for its collection have been otherwise fulfilled.
3. **Right to object:** the right to object grants data subjects the right to object to the processing of their personal data for non-essential purposes such as marketing.

The adoption of these rights would allow for American citizens to be more informed about the data protection statements they are agreeing to with respect to the processing of their personal data, the purpose of that processing, and who has accessed their data. These regulations allow for citizens to object to having their data processed for marketing purposes and empower them to request organizations erase their personal data when there is no grounds to retain it further.

According to the moral theory of utilitarianism, the United States should adopt a similar data protection regulation policy similar to Europe's GDPR in order to uphold the individual right to privacy and promote "the greatest good for the greatest number." GDPR serves to force businesses to develop their products and services with data protection in mind and seeks to ultimately protect the personal data of individual citizens from being accessed by unauthorized third parties without the informed consent of the data subjects. While it could be argued that the ability to perform big data analysis on a large number of data subjects throughout a number of years can provide a lot of utility from a research perspective, it is important to understand the ethical implications that can arise from mining the data of individuals without their informed consent and without taking the proper precautions in order to protect that data. In order to align with the ideals of utilitarianism, the United States should seek to establish clear regulations on data protection to all businesses that operate within the country to minimize the potential for harm from data breaches. Businesses that seek to adopt strong data protection policies in order to enhance individuals' privacy rights, improve data security, and build trust with their customers would contribute to the overall well-being of our society.