

Brandon Pearson

Professor Andrew Garnar

PHIL 355E

12 February 2023

There have been major ethical dilemmas and debates revolving around the collection of user data by companies. The collection of data can be a complex topic when it comes to how the data is being stored and used. This has led to many issues when it comes to data privacy and protection over the years. Leading to Europe creating the General Data Protection Regulation or “GDPR” affectivity creating a widespread standard for how digital data should be collected and protected across Europe. The GDPR sets forth a standard that all organizations and companies must follow when it comes to data protection. Promoting a safer and easier-to-comprehend strategy for companies to implement. Due to the regulation, companies that do not follow the regulations will be subjected to large fines for neglect. This ensures that all companies that are collecting data are following the proper procedures. In this case analysis I will argue that deontology shows us that the United States should follow Europe’s lead in introducing General Data Protection Regulation. This will create a more ethical and easier-to-follow standard across organizations and companies. Ultimately, aiding in protecting users' privacy as well as promoting the user's ease of access in obtaining their data.

Michael Zimmer’s journal “*But the data is already public*”: on the ethics of research in Facebook introduces many interesting thoughts about ethics and the ethics

behind gathering data. His journal analyzes the ethical complexities of user data as well as highlights the issue when it comes to understanding what is considered private information or Personal Identifiable Information. Zimmer looks at a research study “Taste, Ties, and Time (T3)” and goes over the flaws that were present in how the study was conducted. One major point by Zimmer was the lack of an ethical understanding of data privacy regarding user data. This was seen in the study due to information being collected and presented about the people in the study still being able to be re-identified back to users. Zimmer makes multiple points conveying the importance of protecting user data. Another notable concept mentioned was, that if the U.S. had more clearly defined information on what is considered to be Personal Identifiable Information like the EU has, then the study would have potentially not had the same flaws it ended up having. Lastly, another important concept that is mentioned in the journal is the dignity-based theory of privacy. This theory comes from a deontological moral theory, which states that there are ways we can indirectly wrong people by undermining their dignity as people. Essentially it is wrong to breach someone's privacy even though no harm ends up coming of it because you are still undermining the person's dignity. Taking their ability to dictate where their information lies or persist.

When it comes to implementing a “GDPR” regulation in the United States it could bring about a lot of good. For instance, if the U.S. had such regulations in place, then the “Taste, Ties, and Time (T3)” study would have potentially not had as many flaws. Zimmer mentioned how the students conducting the study had a lack of understanding when it came to data collection and how to do so ethically. Having a GDPR-like regulation set in place would have made it easier for the students to educate

themselves on what data had to be removed to maintain the users' privacy. This also shows how not having a universal regulation for digital data privacy can lead to companies or organizations not protecting their users in the best way. Overall, having a regulation that is widespread and is the standard across a nation is easier to maintain and regulate than having to regulate each company differently.

Taking a deontology approach when reviewing this case, it is clear that the study could have benefited if the U.S. had a GDPR-like regulation. Zimmer brought forth the concept of the dignity-based theory of privacy. This theory represented a deontology moral perspective. It was clear that in the "Taste, Ties, and Time (T3)" study, the researchers neglected to account for the dignity and autonomy of the individuals. The researchers in their study neglected to gain proper consent from the individuals whom the data was from. Additionally, the researchers undermined the users' data and misappropriated the users' reasonable expectations of privacy. The right thing that could have been done in this study was for the researchers to have been better educated on data privacy. This could have potentially led to the researchers understanding the issues in the way they were conducting the study. This in turn could have prevented the researchers from taking away the users' autonomy as a person.

Elizabeth Buchanan brings forth points about the ethical complexities when it comes to big data research. Buchanan focuses on how traditional research methods may not be able to work when it comes to big data. When doing research involving big data it is hard to identify the subject. This leads to issues when it comes to identifying how to conduct the research. Traditionally participants know that their data is being used or viewed whereas in big data research can be done without the user knowing the

data is being used. With big data, research is done on large datasets, making the subject unclear. This brings forth the major concept of should data subjects have the right to consent to their data being used and how they would be able to. Another major concept mentioned is that the intent of analysis matters when it comes to research. When it comes to research there is a reasonable expectation of privacy as well as an expectation that the data collected is protected. The issue that persists is that big data research doesn't allow people to consent to their data being used. Overall, big data presents issues when it comes to research. Maintaining an ethical method for gathering data is complex due to the lack of consent in big data.

Incorporating a GDPR-like regulation in the U.S. could help make big data research more ethical. Implementing stronger regulations on data, in general, will ensure that big data only consists of things that are laid out in the GDPR. Promoting more security when it comes to data collection further protects the rights of the individual that data is being collected. This could potentially make big data research more ethical because the data that is a part of the "big data sets" would have to pass the GDPR framework. Ensuring that there isn't any information that could be re-identified to any one person. When it comes to research and traditional methods of gathering information, people are becoming collateral subjects to their data. There is no complete or perfect way to do big data research because it lacks the ability to accurately gain consent for the data at hand. Ultimately, the intent of the analysis is a major factor when it comes to big data.

Looking at this case from a deontology perspective highlights many issues with big data collection. Big data lacks the consent of the individual which in turn makes any

research done using big data unethical. Research using big data is violating the users' autonomy and dignity as a person. Ultimately using the person for their data rather than looking out for the person's best interest. Such as maintaining and protecting the individual's privacy. If there was a way to accurately get consent for the data, then the research would be ethical. This is why traditional research involving subjects or participants is ethical because each participant can clearly consent to be involved. Implementing a GDPR-like regulation could aid in giving the data subjects their privacy back. This results in subjects understanding how their data is being used and having a say in what their data is used for.

The United States should implement regulations like Europe's new Privacy Laws. While digital data privacy is a complex ethical topic. Creating stronger regulations around digital data privacy promotes a safer environment for consumers and product users. This allows users to have more control over their data and to be more informed on how their data is being used. Having a GDPR-like regulation in the United States would promote users' ability to give consent when it comes to data collection. This would be more in line with a deontology moral perspective. This results in people being treated with dignity and not just as data points or data subjects. Focusing on the humanity of the origin of the data rather than allowing companies to profit from users' data. Additionally, regulations promote a safer and easier-to-comprehend framework for companies to implement in order to maintain an environment that adheres to users' data privacy.

