Case Analysis on User Data Using Contractarian Moral Reasoning

Rebecca Hight

Old Dominion University

PHIL 355E

June 30, 2024

Introduction

Fears of data privacy and protection have emerged due to the advancement of technology in the digital age. The General Data Protection Regulation (GDPR) implemented in the European Union (EU) in May 2018 can be seen as a major change in data protection that has been developed to provide EU citizens with more options regarding their personal data. This regulation has caused discussions on the need for other countries to adopt the same law, such as the United States. This case analysis focuses on the moral issue of user data privacy and whether the United States should adopt GDPR-like privacy laws. According to contractarianism, a theory that deals with social contracts, moral norms are legitimate simply because people in society agree to them (Butler, 1991). In this case analysis, I will argue that, based on contractarianism ethical principles, the United States should embrace EU's GDPR because it will promote the fair and just use of individual data.

Zimmer Analysis

Central Concepts from Zimmer

Michael Zimmer focuses on the ethical implications of using publicly available social media data. The concerns raised by Zimmer include lack of consent, insufficient data privacy measures, and data re-identification concerns. In Zimmer's opinion, the lack of clear prior consent from users and inadequate data anonymization are the two crucial ethical issues that researchers face. Zimmer's argument is based on the fact that privacy is a right, and public data collection and use infringes on this right. His work raises awareness of users' expectations of privacy and the ethical obligations of researchers in handling data (Zimmer, 2010). Through the "Tastes, Ties, and Time" (T3) project, Zimmer exposed how easily distinguishable data can be abused. This raises concerns about such forms of research and their ethicality.

Application to the Case

Applying Zimmer's ideas to the GDPR case, it is reasonable to conclude that GDPR's high standards for consent and further anonymization address the ethical issues described by Zimmer. To achieve this, GDPR requires organizations that want to collect and process users' data to obtain their consent, which gives users adequate information on how their data will be used. Furthermore, GDPR requires an organization to give sufficient anonymization to reduce the likelihood of identifying the individuals. They ensure data subjects have control over personal information and that their privacy is respected (Palmer, 2019). GDPR aligns with the ethical principles pointed out by Zimmer and promotes higher levels of transparency and responsibility concerning the data management process. These regulatory measures also protect individuals' privacy and instill confidence in organizational institutions (Zimmer, 2010). Thus, other countries should replicate such measures.

Ethical Assessment

From the contractarian point of view, GDPR complies with the principles of fairness and recognition of the privacy of an individual. Overall, this makes GDPR fair and equal in its approach towards protecting users and their data from potential risks. On the other hand, there are no similar laws in the United States, and people's data can be used in a way they did not agree to, raising privacy issues and ethical questions. The contractarian approach to the justification of moral norms relies on the consent of the individuals concerned, and GDPR reflects this idea by entrusting individuals with the regulation of their data. Therefore, implementing GDPR-like regulations in the United States would not only enhance data protection but also be ethical within the spirit of contractarianism, promote fairness, consent, and respect for data subject rights (Palmer, 2019).

Buchanan Analysis

Central Concepts from Buchanan

The areas highlighted by Buchanan for big data research ethics primarily relate to privacy and security. Buchanan also identifies the continuous policy discourse as necessary in addressing the issues of ethicality in data mining. According to Buchanan, big data is beneficial when it comes to generating insight, but it is equally problematic when it comes to privacy and freedom. For instance, Buchanan (2017) called for ethical scrutiny arguing that researchers need to think through the overall impact of their work. Buchanan raises the topic of “data subject” and how the shift from “human subject” poses challenges to conventional research ethics (Buchanan, 2017). She also emphasizes the need for policies and regulations on how big data research is done without infringing on the rights and freedom of people in the process of gaining knowledge from data analysis.

Application to the Case

Buchanan argues that sound legislation like the GDPR plays a key role in handling the ethical issues of big data. Compared to Buchanan’s argument, it is reasonable to state that GDPR has directly responded to the challenges of data minimization, purpose limitation, and accountability. GDPR mitigates the risks of big data research by requiring organizations to collect data relevant only to the objectives of the research and also inform about the further use of the data collected. These provisions ensure that data is not collected and processed in large quantities or outside the consented scope, protecting the rights of the users to privacy and self-governance (Palmer, 2019). In this case, no matter what regulations are put in place there is always an ethical and proper way of handling data. Not only does this regulation protect people, but it also helps in the use of proper research methods, promoting the responsible use of data.

Ethical Assessment

Buchanan's ethical framework allows us to conclude that GDPR truly balances threats of big data and big data abuses. GDPR ensures the protection of individuals' rights and their ability to control the data being processed. Adoption of the above measures in the United States would help unleash the opportunity of big data, besides addressing the ethical issues surrounding the field and making the use of technology fair to all. Buchanan also outlines the ethical principles that should be applied to practices regarding data and justifies the notion of learning from data without violating the rights of any person. This approach is just, reasonable, and in line with the rationale of contractarian theory that seeks to preserve the contract consensus. Implementing laws similar to GDPR in the United States would enhance the proper usage of data, safeguard the rights of individuals, and foster innovation responsibly.

Comparative Analysis

Zimmer and Buchanan's arguments share a common point that ethical concerns require individuals' data privacy protection. For Zimmer, it is crucial to highlight the aspects of consent and anonymization, and for Buchanan, it is essential to mention the policy and ethical levels. Both approaches provide the rationale for regulations similar to GDPR for the ethical handling of data. The emphasis that Zimmer placed on prior express consent and the proper techniques of anonymization correspond to GDPR fundamental principles, which expects that people should control their data and should know and approve how the data will be utilized. By emphasizing the need for ethical supervision and responsibility, Buchanan offers a useful way to enlarge Zimmer's argument and consider the overall regulatory system that is required to oversee large-scale data analysis. The United States must also follow GDPR-like regulations to help it address the ethical issues that both Zimmer and Buchanan have identified to improve the overall fairness and responsibility of a digital setting. This comparative analysis highlights the parallels between the two frameworks to show how an integrated approach provides ethical protections for data subjects and actions that are accountable to the members of society.

Conclusion

Passing GDPR-like privacy laws in the United States would go a long way in addressing ethical problems. Zimmer's and Buchanan's research stress the principles of consent, privacy, and ethical regulation in the digital era. The GDPR empowers people to own their data and shields them from risks that could be detrimental to their well-being, thereby promoting fairness in cyberspace. Implementing the same regulations in the United States would also provide a contracts-based solution to the alleged ethical dilemmas of big data and rebalance in favor of free enterprise and innovation while respecting citizens' rights. Despite the potential counterarguments regarding its disadvantages in terms of its influence on business and innovation, it is crucial to highlight that the ethical advantages of guarding people's personal data outweigh these arguments, making the necessity of adopting GDPR-like regulations in the United States undeniable. Adopting these regulations would provide fair, reasonable, and compliant data practices while protecting individual rights and allowing for continued innovation in a sustainable manner in the digital age.

References

Buchanan, E. (2017). Considering the ethics of big data research: A case of Twitter and ISIS/ISIL. *PLOS ONE, 12*(8), e0181803. https://doi.org/10.1371/journal.pone.0187155

Palmer, D. (2019, May 17). What is GDPR? Everything you need to know about the new general data protection regulations. *ZDNet*. Retrieved from https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Zimmer, M. (2010). "But the data is already public": On the ethics of research in Facebook. *Ethics and Information Technology, 12*(4), 313-325. https://doi.org/10.1007/s10676-010-9227-5

Butler, O. E. (1991). *Bloodchild and Other Stories*. Thorndike, USA: G.K. Hall & Co.