# Case Analysis on User Data

Wesley Faxlanger

Dept of Philosophy & Religious Studies, Old Dominion University

PHIL 355E: Cybersecurity Ethics

Professor, Nathaniel Nicol

11 February 2024

**Case Analysis on User Data**

Since the beginning of the digital age, governments and organizations alike have yet to create a policy that perfectly encompasses the complexity of IoT and the nuances of online privacy in a meaningful way. However, the General Data Protection Regulation (GDPR) put in place in Europe comes close to addressing the many issues related to online data collection with the added benefit that the policy favors the interests of citizens rather than the organizations collecting the data. The United States, on the other hand, has many policies regarding data collection; however, there are few consequences for organizations that do not strictly adhere to these policies. Due to this unfortunate fact, cyberattacks against tech giants or even smaller companies can cause catastrophic damage to individuals trusting organizations to protect their sensitive information. Failure to protect this information can result in things such as identity theft or the compromising of individuals' privacy. From a Deontological point of view, The United States should undoubtedly rework how Data collection is regulated, as many organizations act solely for self-interest and knowingly put their users at risk.

In the article *"But the data was already public"* by Micheal Zimmer, an accidental data breach is discussed as researchers accidentally released large quantities of personally identifiable data. This is troubling because the researchers were obligated to use the data responsibly and provide anonymity for the individuals whose data was used throughout the study. However, in practice, the anonymity of the data was nonexistent as individuals could easily trace the data back to its source, ultimately exposing almost two thousand Facebook users. The anonymity of the study was inherently flawed as, according to the article, "some nationalities are only represented by one person" Zimmer, (2010). This is problematic because while a name might not be directly linked to the individual in the study, with minimal effort, that student could be

identified and paired with the sensitive information stated in the article. Even the method by which the researchers collected the data is somewhat controversial. They used a process called “scraping,” in which they searched the student's names and collected any relevant data. While a third-party service is usually used, or the students would have been asked to opt into the study, these methods were deemed ineffective and prompted the researchers to result in “Scraping.” While this data was already accessible on Facebook before the research was published, removing informational friction is one of the major problems resulting from the publication of this research. Not only were the involved students harmed in the study, but the university itself was identified because of individuals linking the data to students.

Despite the harm caused by the study, the researchers were not acting maliciously but rather had good intentions, seeking to carry out what should have been an ordinary study that could have benefited humanity. For this reason, the researchers had done nothing wrong from a Deontological point of view. While the researchers may have had good intentions, their actions still had negative implications that could have been avoided with a proper framework to guide them. Looking at the GDPR in Europe is an excellent example of how this incident could have been avoided, as clearly defined policies and practices would have been made readily available to the researchers. Under GPDR, the researchers would have been required to properly inform the students of their data use and obtain their consent after ensuring the participants understood their consent. If the researchers had been more responsible with the collection and realized the data used in their study, violating the student's privacy could have been entirely avoided. This is why it is imperative to rework data collection policies in the United States to protect citizens from malicious actions and accidental breaches caused by negligence. The Deontological perspective would likely not consider the study's outcome as a factor in the morality of the

researchers but rather their intentions or reason for surveying the first place. That being said, collecting the students' data via scraping and failing to protect the data would be immoral if the researchers were capable and chose to be careless.

Ethics, as it relates to data collection, becomes significantly more complicated when factors such as terrorist organizations are introduced. As stated in the article *Considering the ethics of big data research: A case of Twitter and ISIS/ISIL,* by Elisabeth Buchanan, social media has been used to spread terrorist propaganda across the world, ultimately posing a significant issue for law enforcement and world governments alike. While it is widely accepted that monitoring software is used to track online terrorist activity and stop the spread of propaganda, there is a significant moral issue that arises when this technology is misused. The article discusses the idea of consent not always being possible while maintaining the same results, as stated in the quote, “From a US-regulatory perspective, researchers would conclude that seeking informed consent from all 119,156 participants is impracticable” (Buchanan, 2019). The use of technology to identify online terrorist groups is justifiable; however, from a deontological perspective, using this technology for purposes such as advertising is inherently wrong. Even monitoring private citizens without probable cause could be considered amoral under this definition, as government agencies would be stripping private citizens of their privacy without any solid proof that they might be related to terrorism. While this technology is not unique in the way of being a slippery slope, there are still many ethical considerations regarding its use. The article mentions Edward Snowden, who exposed mass government spying on private citizens in the name of national security. While one could argue that protecting citizens from terrorism via mass spying is justifiable due to the protection it provided, it was ultimately a violation of trust as well as the rights afforded to citizens of the United States.

A significant issue with the United States federal policy regarding data collection is that it favors giving discretion to the government rather than protecting the rights of citizens. The data found on social media platforms such as Facebook and Twitter are considered in most cases to be public unless otherwise defined, such as in GPDR. The idea that national security is a justification for infringing the rights of private citizens is concerning. The lack of clearly defined guidelines for these practices leaves massive room for interpretation, which can have dire consequences when paired with a general lack of proper oversight. This is where policies such as GPDR are needed in the United States to regulate private organizations and the government. As left unchecked, it is clear that the needs and rights of private citizens will be overlooked in favor of benefiting the government or other organizations. Even something as simple as requiring a warrant to collect data on individuals' public social media profiles would significantly reduce the unnecessary government surveillance experienced by private citizens. Apart from the deontological perspective, there is undoubtedly a benefit from the government monitoring social media traffic so long as civil liberties are not violated. Ideally, government agencies should be held accountable, and the data should be used responsibly to benefit society without compromising social media users' rights.

In conclusion, user data, particularly sensitive information that is personally identifiable, needs to be handled with the utmost discretion and care to ensure that users are protected. The GPDR, as it exists in Europe, is a great example, although it is far from perfect. While ensuring the protection of citizens is essential, it is no less important to ensure their civil liberties are upheld. Citizens must also be protected from private organizations attempting to misuse user data, mainly when the goal is monetary gain through selling information to advertisers. Even allowing users to access the information that is being collected would ultimately improve the

situation rather than essentially taking advantage of the general population's ignorance. From the deontology perspective, ensuring social media users' protection and informed consent is imperative before data collection, as choosing to take advantage of these users is inherently immoral. While informed consent is not always easy to obtain, it is nonetheless necessary to ethically obtain data.

Works Cited

Buchanan, E. (2017). Considering the ethics of big data research: A case of Twitter and ISIS/ISIL. PloS one, 12(12), e0187155.

Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of "personally identifiable information." *Communications of the ACM*, *53*(6), 24–26. https://doi.org/10.1145/1743546.1743558

Palmer, D. (2019, May 17). *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, M. (2010). "But the data is already public": On the ethics of research in Facebook. Ethics and information technology, 12(4), 313-325.