Caleb Judy

Professor Nicol

9/29/23

Case Analysis on User Data

The article “What is GDPR? Everything you need to know about the new general data protection regulations”, written by Danny Palmer, showcases the European Union’s (EU) new data protection framework, known as the General Data Protection Regulation (GDPR). It is designed to give EU citizens more control over their personal data, which includes things such as their address, email addresses, credit card numbers, their social security number, among other things. Essentially, it emphasizes the importance of helping individuals who want to take control of their personal data. The GDPR is similar to the concept known as ethics of care (or care ethics). Ethics of care is distinct from traditional ethical theories, like utilitarianism, because it puts a strong emphasis on the principles such as interdependence and mutual flourishing. In this case analysis, I will argue that ethics of care shows us that the United States should follow Europe, and create a framework similar to the GDPR, because it will allow users to have more control over their personal data.

To start, I would like to explore an article written by Micheal Zimmer, “But the data is already public”. The article focuses on the ethical considerations involved in conducting research on Facebook and other social networks. Zimmer highlights the importance of obtaining informed consent from users whose data is being used for research purposes, as well as emphasizing the potential harm that social media research may cause, such as the exposure of one’s private information.

One of Zimmer’s main focal points is about the ethics of research in online social networks. The concept of the ethics of research in online social networks pertains to the moral considerations and principles that should guide academic research, as well as guide corporate research when conducting studies that use data from social networking platforms such as

Facebook. In this context, ethics includes a range of issues, such as user consent, privacy, transparency, and the potential for harm. It is crucial that researchers navigate these ethical challenges to ensure that their studies are conducted responsibly. One primary ethical issue is informed consent. Zimmer suggests that researchers must obtain clear consent and informed consent from individuals before they start using their data for research purposes. Zimmer's work emphasizes that relying on just a platform's terms of service, or assuming that data is public doesn't excuse researchers from this responsibility. Researchers must actively inform participants about the study's purpose, how the participants' data will be used, and inform the participants about any potential risks involved. He also discusses the potential to harm individual groups. Research that uses social media data can unintentionally expose sensitive information, impact privacy, or contribute to discrimination of an individual. Researchers need to proactively assess and mitigate these risks in order to protect the well-being of the users whose data they analyze.

Another concept Zimmer discusses is the public availability of data ("But the Data is Already Public"). This concept refers to the belief that data shared on social media platforms, such as Facebook, is already public and is therefore "fair game" for research, meaning that researchers don't need explicit consent to use said data. Zimmer argues against this, saying that public availability alone does not remove the need for ethical considerations and informed consent. Now while certain data on social media may be accessible to a wide audience, this doesn't imply that individuals have consented to its use in research. Data that is publicly available can still contain personal information, and its use in research can potentially have unintended consequences. Researchers need to recognize that even though some data is publicly accessible, ethical obligations can still persist. His work encourages a nuanced view of data availability, one that recognizes the importance of informed consent and ethical conduct in research, regardless of the perceived public nature of the data. This concept highlights the need

for researchers to be thoughtful, as well as being responsible for the data they collect and analyze, even when it appears to be in the public domain.

Ethics of care can support claims made by Zimmer, as well as support the United States adopting something similar to the GDPR. One of the main concepts of ethics of care is mutual flourishing. Mutual flourishing emphasizes the idea that individuals and communities should strive for the well-being and flourishing of others, and not just the well-being and flourishing of themselves. In this context, companies need to consider how mishandling data could affect the individuals they are collecting data from. The concept of mutual flourishing can be applied to transparency and accountability. Companies collecting data should be open about their data collection and use, and accountability mechanisms need to be instituted to hold companies responsible for any harm caused by data collecting activities. A system like the GDPR may not be able to directly hold companies accountable for mishandling data, but it could eliminate the problem altogether. A user would be able to have control over their data, so if a company wanted to gather information considered private to a user, the user would have the ability to not consent, thanks to a system like the GDPR. This process is much more transparent to a user, rather than a company just collecting the data without the data subjects' notice.

Another article I would like to explore was written by Elizebeth Buchanan, "Considering the Ethics of Big Data Research: A Case of Twitter and ISIS/ISIL". This article discusses the ethical considerations when conducting research with large datasets. The article specifically focuses on the analysis of Twitter data related to the extremist group/terrorist organization ISIS/ISIL, which was using Twitter to recruit people to the terrorist organization.

Elizabeth Buchanan discusses the concept of "Ethics of big data research", which refers to the moral and ethical considerations that researchers must consider when conducting research that involves large amounts of data, especially those collected from online platforms, such as social media. In the context of big data research, ethical concerns often revolve around issues such as privacy, informed consent, and the potential for harm. Researchers must

emphasize not violating the privacy rights of individuals when analyzing their data. Another big point of emphasis for researchers is informed consent. This means that individuals whose data is being used should be made aware of and also explicitly agree to how their data should be utilized. Additionally, researchers need to consider the potential consequences of their research, especially when their research includes the discussion of sensitive or controversial topics.

Buchanan discusses a case study that involves Twitter and ISIS/ISIL. In this specific case study, researchers collected and analyzed data from Twitter to study the online activities of the extremist group ISIS/ISIL. This case study raised several ethical dilemmas, discussed by Buchanan. First, there's the dilemma of whether using Twitter data in this manner infringes the privacy of users who could have unintentionally interacted with ISIS/ISIL related accounts. Second, there's a potential for harm, as sharing or publicizing such research could possibly contribute to the spread of extremist ideologies. It is crucial for researchers to weigh the benefits of their study, such as gaining insights into online extremism, against these potential harms.

Ethics of care can also help support the article written by Buchanan. Another one of the main concepts of ethics of care is interdependence. Ethics of care recognizes that individuals are inherently interconnected and interdependent with others. It emphasizes the importance of recognizing the relationships and responsibilities that arise from them. In the context of the ISIS/ISIL case study, researchers should have recognized the relationship between data subjects and data collectors. Data subjects rely on data collectors and organizations to handle their data carefully, responsibly, and ethically, while data collectors depend on the data subjects for the data that fuels their research. In this case, while data subjects gave data researchers their data, the data researchers were negligent with users' data, which raised several concerns, some of which being concerns over privacy, informed consent, and the potential for harm, as mentioned above. The United States should absolutely implement a system such as the GDPR because of cases such as this. A system such as the GDPR would allow users to control their data and protect their privacy, protect themselves from harm, and users wouldn't need to worry

about consenting, because the individual themselves would be able to control who is using their data, and what it's being used for.

The concept of “Ethics of Care”, as well as the two articles written by Micheal Zimmer and Elizabeth Buchanan, help support the idea of the United States implementing a data protection framework, similar to the GDPR. Zimmer’s segment of the public availability of data can be applied to mutual flourishing, specifically about how companies need to be more transparent with data subjects. Elizabeth Buchanan’s segment discussing the ISIS/ISIL case study can be applied to interdependence, as the people conducting the case study should have recognized the relationship between data subjects and researchers. While taking on such a project may be costly and difficult for the United States government to overcome, in a world where everyone’s information, including home addresses, bank account details, and other personal information, is all being stored online, it is vital that the United States creates a system similar to the GDPR. Not having a framework like the GDPR is an issue that isn’t talked about enough in this country, as not having something similar to the GDPR means people have less control over their personal data, which puts everyone’s personal data at risk, in my opinion.