Jonathon Clark

Professor Nicol

PHIL 355E

2/12/2023

**Case Analysis on User Data**

In recent years, through the European Union, governments in Europe have taken a more active role in data privacy. The General Data Protection Regulation (GDPR), created in 2018, was the response to these data privacy concerns (Palmer, 2019). The GDPR is a list, comprised of various rules and policies, that attempts to create more control over how users’ data is collected, stored, and used throughout Europe. After passing the General Data Protection Regulation in Europe, many have called on the United States of America to adopt similar legislature and policy. There have been many arguments presented both in favor and against the United States adopting similar guidelines. I believe, while there are certainly lessons to be learned from Europe’s General Data Protection Regulation, that the United States should not adopt a “carbon copy” list of rules. In this case analysis, I will argue that Confucianism shows us that the United States of America should not follow Europe’s lead because not everyone’s “correct path” is the same.

First, I will use concepts from Michael Zimmer’s written work, ”’but the data is already public’: On the Ethics of Research in Facebook” to support my argument. One of the main concepts from this reading concerns the T3 project. T3 stands for “Taste, Ties, and Time.” This project involved researchers from the Berkman Center for Intern and Society and college students (Zimmer, 2020). These researchers collected and examined data from the Facebook profiles of these college students. This was publicly available information and the researchers intended to keep this data as anonymous as possible. However, just by looking at the data itself, it was easy to see that these students were all from Harvard College. Once the students found out just how identifiable the information that had been collected was, they became concerned that they might fall victim to targeted scams or potentially worse situations. This forced the researchers to abandon the project and the study ended in failure. It did, however, raise other important questions about how this “publicly available” information could potentially be used to identify people. The concerns that were raised surrounding this study have a direct relationship to the idea of the United States adopting a General Data Protection Regulation stance on user data protection. At first glance, a GDPR-like policy change in the United States could prevent data like this from being collected and used. However, it is important to note that GDPR policies only apply to the way data is collected, stored, and the way it is used. All the information gathered from Facebook in this study is information that was posted publicly, by the students. A GDPR-like policy created by the United States would not have much effect since this data was willingly given by the students. A better way to approach this problem would be through using the Confucian ethical tool. Confucianism is all about following the “right path” and specifies that the “right path” isn’t the same for everyone. Every person has unique situations in their lives that cannot be addressed by simply creating broad policies like in the case of the GDPR. Instead, through Confucianism, users should be given more choice in the way that their information is displayed and how visible to the outside world it is. Users must be allowed to walk their own path in regard to sharing their data. Some users may not care about all the things that they post to Facebook and have little hesitation to put sensitive information out there. Other users may not even want people to see what university they attend, for example. If the United States adopted a more Confucian-like set of rules and policies, users would have more flexibility in choosing the way their data is used. With a GDPR-like set of policies and regulations, everything appears to be clear cut and straightforward. However, these all-encompassing policies will have grey areas and loopholes by which user data collection could be exploited. This also relates to Confucianism when considering the roles of the individuals involved. Should the government be the ones who decide what information is too sensitive to be shared? Or should the owners of the data themselves be the ones to decide? Confucianism dictates that individuals must stick to their roles to follow their own respective paths.

The second article that supports my argument comes from Elizabeth Buchanan’s written work “Considering the ethics of big data research: A case of Twitter and ISIS/ISIL.” This article focuses on data collection methods that are utilized by Facebook and Twitter. These platforms use what is known as the Iterative Vertex Clustering and Classification (IVCC) model (Buchanan, 2017). Using this model, platforms are able to identify members of groups like the Islamic State of Iraq and Syria (ISIS) and Islamic State of Iraq and the Levant (ISIL) simply by searching. Using this method, individuals can be singled out by looking for identifiable characteristics like location, age, and even names that belong to certain cultural groups (e.g. Muhammad, etc.). Governmental and law enforcement entities are able to monitor such individuals with the help of Twitter, Facebook, and other social media platforms. While this may seem to be a great idea that will help keep our national security posture strong, it can also lead to innocent individuals being targeted. There is a big difference between radical extremists and those who follow a specific belief system. Using this type of model, there is no real way to differentiate between the two. This directly relates to the topic of the United States adopting a GDPR-like set of policies and rules. It is no secret that the United States government has had a questionable history in regard to American citizen data. The information leaked by Edward Snowden concerning the NSA and Homeland Security spying on its own citizens raises a lot of questions about how a GDPR-like set of rules would apply to the United States government (Reed, 2013). More specifically, would the United States government also be bound by a GDPR-like set of regulations? Or would there be exemptions for governmental agencies and law enforcement? The IVCC model that is currently in place would be problematic to the United States adopting policies similar to the Europeans. The answers to these questions, and more, become more obvious when they are approached through the eyes of Confucianism. Confucianism emphasizes the importance of people and organizations playing their roles properly. Confucianism also specifies that fulfilling our roles will help in other areas of life. This is beneficial because we play different roles every day. However, one role does not supersede the other. The United States government plays the role of governing and protecting its citizens. The United States government has been proven to overstep these boundaries like in the case of Edward Snowden and in the case of Twitter and ISIS/ISIL. United States citizens play their role by obeying laws and contributing to society. If the United States government oversteps their boundaries and does not fulfill its role, it makes it much harder for United States citizens to fulfill their role. For these reasons, the United States should not adopt a GDPR-like set of policies and regulations. With the United States government’s track record, such policies and regulations could potentially make it harder for everyone to walk their “own path.” The United States government absolutely needs to play their role in protecting citizens data, but in the right way.

After analyzing the question of whether or not the United States should adopt a list of regulations and policies similar to the General Data Protection Regulation established in the European Union, the answer is made clearer. Through the articles written by Elizabeth Buchanan and by Michael Zimmer, parallels have been drawn. Finally, through the use of the Confucian ethical tool, the only logical answer is that the United States should not adapt the General Data Protection Regulation directly. That being said, the United States should play more of a role than what they currently are. But, as seen through the Confucian tool, what is right for the European Union might not be what is right for the United States. Everyone must play their roles to protect user data. It starts with individuals and ends with the government. The United States must enable individuals to “walk their own path” in regard to protecting their own data. Instead of all-encompassing rules and regulations, issues should be handled on a case-by-case basis.

Reference

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. (2020). “but the data is already public”: On the Ethics of Research in facebook. The Ethics of Information Technologies, 229–241. <https://doi.org/10.4324/9781003075011-17>

Buchanan, E. (2017). Considering the ethics of Big Data Research: A case of twitter and Isis/ISIL. PLOS ONE, 12(12). <https://doi.org/10.1371/journal.pone.0187155>

Reed, B. (2013, June 11). Edward Snowden: The whistleblower behind the NSA surveillance revelations. The Guardian. <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>