In 2018 the European Union officially adopted the General Data Protection Regulation (GDPR) which was made with the intention to build upon the preexisting policies surrounding data collection and usage. This enacted regulation affords consumers more control over their own personal data that is being collected by various companies. It also requires companies to have more accountability for user data overall. Some of these requirements are data breach notifications, ensuring user data is collected under strict conditions, and then protecting that data from misuse or breaches. All of these changes and additions to the EU's exiting privacy policy were made with the intention of adapting it to better fit the modern age of technology, specifically by addressing data collection done by businesses via online spaces.

While the U.S. has multiple instances of privacy laws and policies, they are not as all-encompassing or clearly defined as the EU's GDPR. This raises the question as to whether the U.S. should take inspiration from the GDPR to develop and improve upon its own policies. In this Case Analysis I will argue that Consequentialism shows us that the United States should follow Europe's lead because the overall positive benefit to society as a whole outweighs the costs to businesses or data collectors.

In his paper "*But the data is already public": on the ethics of research in Facebook"*, Micheal Zimmer examines the "Tastes, Ties, and Time" (T3) research study, specifically identifying and discussing various shortcomings pertaining to the privacy of the collected data. The T3 study was created with the intention of evaluating the relationships concerning students and social networks, which was done by using the Facebook account data of a cohort of Harvard freshman for four consecutive years. The privacy concerns, however, stems from the release of the dataset collected by the study, which was done in order to meet the mandated condition needed to receive grants from the National Science Foundation. Since the project was partially funded by this foundation, that dataset was made publicly available in phases from 2008 until 2011 until all of the data was accessible to the public.

Zimmer first identifies attempts by the study to ensure the privacy of its participant's data and follows with how these steps fell short to truly prevent the release of identifying information about the students involved. All of the steps were taken in good faith in order to protect the identities of the students involved but introduced several ethical concerns, specifically re-identification of the individuals involved. Additionally, these proposed steps identified that the researchers did not fully understand the extent of privacy pertaining to online social networks.

One of these steps was used to defend the project's ethical privacy concerns in which the group behind the project stated that the project was to only use data that were accessible by default by each RA and were collected with no further information provided by the students. In other words, the claim was that the information released was already public, so no private data was compromised. Another key ethical concern was that no formal consent was obtained, and many were unaware that they were part of any research dataset. Regardless, Harvard's ethical board reviewed and approved the research project.

Zimmer himself references the EU's definition of personally identifiable information when discussing the project's decision to have a delay in the release of cultural taste data. This data protection step taken by the project was done with the intention of ensuring that participants stayed anonymous. He states that while the researchers recognized the unique, potentially identifiable, nature of the culture labels in the study, the delay they proposed as a mitigation was not a sufficient approach. This is especially true given the delay was only three years, making the time between when the students would have attended the school and the data being released relatively short, almost negating the delay's intended purpose. Would the study have considered the EU's broader definition of personally identifying information, as well as the GDPR's explicit requirement for informed consent, the privacy concerns and potential for harm could have been reduced.

In the case that Zimmer analyzes and discusses in his paper, it is clear that the decisions made in the T3 project were done with inadequate privacy protections that have every opportunity to lead to serious harm towards the group of students involved. Using a Consequentialist view of the project, the actions taken by the researchers resulted in a clearly negative consequence, all of which were permitted under current U.S. law. This shows the current privacy laws in the U.S. are not sufficient enough to properly protect data collection and usage in an ethical way.

Elizabeth Buchanan examines ethics behind large scale data collection in her paper *Considering the ethics of big data research: A case of Twitter and ISIS/ISIL*. In it, she discusses a paper that proposes an Iterative Vertex Clustering and Classification (IVCC) model that is meant to identify users on Twitter that are ISIS/ISIL supporters. This model allows for detection of specific individuals and smaller groups within a large data set and has the ability to create ties and relations using mentions, following, and hashtags. Due to this model's dependence on collecting and organizing data of various users online, Buchanan uses its example to examine the complexities that modern data collection and data mining poses, specifically in the research sector.

She states that the ethics and methods of a research project are interdependent, and that the rise of data mining across the Internet begins to raise certain ethical questions, such as to what ends the methodology will be used, who it will be used by, and who has the ability to manipulate it. Concerning big data research, Buchanan also notes that the intent of analyses matters, as the purpose that one user may implicitly agree to their data being used for doesn't mean that the same person would want their collected data used for another completely separate or unrelated purpose.

The GDPR requires that organizations be transparent and provide information to the consumer concerning details like the purpose of processing, who the data is being shared with, and the retention period for the data. Additionally, the GDPR also imposes purpose limitations on data collecting or data mining efforts. This means that any data that is collected is restricted from being used for a completely different purpose, addressing the concern that Buchanan notes in her paper. Alternatively, the U.S has no federal privacy law that enacts these same restrictions. Although there are some laws and policies enacted on a state level, like in California with the California Privacy Rights Act, general approaches to this specific privacy concern surrounding data collection and usage are not as comprehensive as the EU's GDPR counterpart.

Consequentialism focuses on creating positive outcomes and preventing negatives ones. Using this ethical philosophy, the U.S. having an absence of federal privacy law covering purpose limitations and having weaker, less comprehensive state privacy laws leave an opportunity for negative outcomes. When companies and organizations are not held to a strict set of rules concerning privacy, there is often an erosion of trust between these companies and the general public. Additionally, incidents such as large-scale data breaches and incidents of misuse of collected data are more likely to occur without strict standards.

The GDPR, when compared to the current U.S. privacy laws, provides more clear, stricter guidelines and regulations that also address the current gaps in U.S. privacy law as well. The GDPR appears to follow a more consequentialist view ethically as it works on a seemingly more cohesive level to prevent negative outcomes and promote positive ones, which exemplifies yet another benefit the U.S. would gain from creating policies similar to the GDPR.

The European Union's implementation of the General Data Protection Regulation (GDPR) in 2018 set a standard for privacy regulation surrounding the collection and use of user data. It also offered the question of if the U.S. should follow the EU's approach to data protection regulation. By following the ethical philosophy of Consequentialism, it is shown that the U.S. should in fact take inspiration from the GDPR put forward the EU. By adopting federal legislation that would place consumer data protection over the perceived inconveniences to companies that would come from having to put these policies in place, this Consequentialist outlook would ensure a higher standard of data protection for the U.S. as a whole. An argument could be made that the standards that would be put in place by GDPR inspired laws would interact with the current global trade and economic position that the U.S. currently has, since a main aspect of the GDPR is that any other country offering services to the EU must also be in compliance. However, I would have to make the rebuttal that adopting better privacy legislation not only improves the protection of the data of a country's citizens, but it encourages global trade with other countries that have similar high standards pertaining to user data protection. Overall, the U.S. would benefit from adapting current policies or creating new ones that draws its ideas from the GDPR.

References

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

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. https://doi.org/10.1007/s10676-010-9227-5