*What is GDPR? Everything you need to know about the new general data protection regulations* by Danny Palmer clearly and thoroughly discusses the details of the European Union’s General Data Protection Regulation. The GDPR was put in place to give consumers as much control over their data in today’s society where their data is often stored by multiple companies. The regulation requires companies to be clear to users about how their data is being used by the company. The regulation also requires companies to notify people as soon as possible when their data is compromised to allow them to take the appropriate measures to deal with these issues. Companies that fail to meet the standards of the GDPR can face fines “ranging from 10 million euros to four per cent of the company's annual global turnover, which for some can mean billions.” (What is GDPR). In this case analysis, I will argue that utilitarianism shows us that the United States should follow Europe’s lead, because their policy is clearly superior and made to protect the consumer.

Michael Zimmer’s *But the data is already public: On the ethics of research in Facebook* further supports this claim. In the article Zimmer addresses how even only using information accessible on social media such as Facebook for research purposes is still unethical without the consent of those who one gathers information from. Zimmer pokes holes in the argument supporting using data that is already publicly available along with data that isn’t personally identifiable. In the article Zimmer first attacks the point that claims that it would be acceptable to gather personal information as long as it doesn’t identify the person, using a study taken from several Harvard students. Zimmer states that using data available in the study, such as each student’s major, ethnicity, and gender allowed outside sources to quickly narrow down where the school the study could have possibly taken place, pointing out that some of the majors included in the study were only available at Harvard University. The author states in the article that “While individual subjects were not identified in this process, the ease of identification of the source places their privacy in jeopardy.”. Zimmer’s point questions what is defined as “personally identifiable information”. The General Data Protection Regulation not only clearly defines personal data but also does so in extensive detail, including factors such as genetic data and IP addresses. This allows companies who store customer’s personal data to be held accountable when they put said data at risk. It also gives the companies a clear way of knowing what information they need to prioritize in keeping secure. Having a stable and precise regulation similar to the GDPR avoids confusion when it comes to responsibilities of handling personal data.

Zimmer further supports his idea by counteracting the claim that it is ethical to use data that is already available publicly on social media. Zimmer states in the article that the justification of using data that is publicly available on Facebook is only “true to a point”. During the study research assistants from Harvard were hired to search student Facebook profiles and saving their information. Although researchers confirmed that “Only those data that were accessible by default by each RA were collected, and no students were contacted for additional information.”, Zimmer adds the possibility that default access is based off of each individual’s privacy setting. Therefore, a user could potentially have their settings adjusted so that only those that are in a specific network (such as students at their school) can see their profile, however when this information is a part of the study it can possibly reach people that were never meant to see it. GDPR policies would forbid taking any of this information without the consent of the individuals, regardless of whether of it being public on social media. Zimmer concluded that “information should not be considered objectively ‘public’ or ‘private’ (or even ‘not on Facebook’) it should only be considered ‘public’ or ‘private’ from the perspective of the particular RA that downloaded the given student’s data.”. If a regulation similar to GDPR were adopted by the United States it could be developed to include Zimmer’s take, forcing people to take into account just how “public” and personal information they encounter is. With social media being the main way people share and acquire personal information, it is important that the United States works to regulate the way this information is spread and used. Users could be required to not share information with user’s who are not permitted. Although people may still decide to share personal information regardless of a rule change, it is still important that this policy is put into place to give those who have their information exposed a way of holding others accountable.

The principle of utilitarianism further supports the idea of adopting the GDPR policies. A utilitarian point of view supports belief that the decision that creates more happiness in the world than negativity. Most consumers care about their privacy, and adoption of GDPR policies would increase the protection of their privacy and ease the minds of consumers fearing of their privacy being violated. Giving users the option to hold those who spread their personal information without their permission would give users a more secure feeling when sharing anything about themselves on the internet. People find happiness in security, knowing that their right to privacy matters to their country will greatly increase morale overall. American citizen privacy is so important to them, it would almost be a disservice to not establish personal data regulations. Although it may be harder for some companies to obtain information on consumers, the policies would overall benefit the majority of people, making it the morally correct thing to do.

 In *Considering the ethics of big data research: A case of Twitter and ISIS/ISIL* by Elizabeth Buchanan, Buchanan discusses the morality issues with big data collection and analytics. The author explains that “The Iterative Vertex Clustering and Classification (IVCC) model was proposed to identify ISIS/ISIL supporters among Twitter users.”. Once the model was proposed it raised various ethical questions on whether it was morally right to collect big data from Twitter users, noting that “data have become so readily available-provides by the. Users themselves”. If America were under the policy of the GDPR this practice would be strictly forbidden and punishable with fines without the researchers first getting consent from any who’s information was used in the study. Buchanan notes in the study however that “from a US-regulatory perspective, researchers would conclude that seeking informed consent from all 119,156 participants is ‘impractical’ and studies of this sort involve no more than minimal risk.”. Buchanan’s comment critiques the fact that American regulations rarely emphasize obtaining consent of all participants in a study, with most claiming that the collected data is ethical since it was obtained publicly through social media (although Zimmer already proved why this claim is partially invalid in the previous article.

Buchanan also mentions the GDPR in the article stating “As the EU General Data Protection Regulation goes into effect in 2018, researchers will be among those challenged by big data analyses and analytics and their uses in relation to individual and societal privacy.”. One can argue that it is supposed to be hard for researchers to conduct big data analytics, forcing researchers to gain consent from those they gain information from would also decrease the chance of researchers doing unethical or biased studies. The EU has challenged Big Data researchers to conduct their studies ethically, prioritizing its people’s privacy over large companies and their monetary gain. The author is also critical of social media sites failing to discourage the mining of this data, stating “With Twitter’s massive numbers of active users, combined with its openness for researchers to explore and exploit its data” makes it safe to assume that big data research will continue to grow. If America were under the same policy as the EU, the GDPR would hold the companies like Twitter accountable for protecting user data as well. Overall, it’s safe to assume that Buchanan’s article suggests support of the U.S. adopting the EU’s GDPR, as the EU has elected to prioritize protecting consumer privacy over the desires of the economically superior.

 Utilitarianism again can be used to justify Buchanan’s point. Once again prioritizing the needs of the many is most important. In Buchanan’s case identifying possible ISIS supporters could help the country politically, however it puts the privacy of the majority at risk, and without their knowledge. The question of who can edit said information also comes into play, leading opposers to wonder if these studies could lead to false classification of subjects without their knowledge. When applying utilitarian philosophy to this case, one can infer that the cost of invading innocent people’s privacy, which could also possibly diminish their trust in the government, isn’t worth the benefit of finding possible ISIS supporters, especially given the risk of this information being compromised or edited which could lead to false convictions of innocent people. This is a perfect example of the “good” from respecting people’s privacy far outweighs the “bad” of not being able to identify terrorist supporters. This concept of research could also be applied to other political subjects, such as individuals that supports causes such as Black Lives Matter, subjecting users to mistreatment for their views, and further reiterating the importance to choose the needs of the many over the few, as keeping people safe from discrimination based off their political beliefs is far more important than any type of research that doesn’t benefit the country as much as keeping its citizens feeling safe to express their beliefs. Adopting a regulation similar to the GDPR would give American citizens this freedom that they’re entitled to. This regulation could prevent companies from piling people’s beliefs into databases that could be used to discriminate against them, and allow those citizens to hold these corporations responsible when their information is collected without their knowledge.

Overall, the argument for the U.S. to adopt the GDPR stays consistent, both articles support the argument that removing “personal information” does not excuse extracting data from users without their knowledge or consent, something that GDPR strictly prohibits, regardless of where the information comes from. GDPR would also hold companies accountable for keeping the data of its’ consumers safe, which, had American regulations matched those in the EU, could have prevented American issues such as the Facebook controversy that led to many users discovering that their data was being sold without their knowledge or consent. Although adapting to the regulations of the GDPR would prove difficult for many large companies and would probably result in monetary losses for said companies, the overall result will lead to the policy benefitting more people than it causes trouble for and decreasing the overall amount of unethical activity in the country. The EU’s GDPR is overall far superior to America’s policies on privacy and adopting a similar policy would allow the country to prioritize its citizens right to privacy.

## 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

*What is GDPR? everything you need to know about the new General Data Protection Regulations*. ZDNET. (n.d.). Retrieved February 12, 2023, 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