Europe's new privacy law, GDPR, or General Data Protection Regulation, is an essential step toward user data protection. This act of legislation by the European Commission ensures that all residents in Europe have the right to know when their data is stolen. This move is crucial and should set a standard for other nations. The United States, a considerable portion of online users worldwide, could greatly benefit from a law similar to Europe's. The amount of data stolen from U.S. citizens without their knowledge is embarrassing, and something needs to be done about it. Companies like Facebook continue to get away with unrevealed data breaches with no consequences. A huge fine will be a great incentive to push companies to better communicate with their users' about their stolen data. In this Case Analysis, I will argue that consequentialism shows us that the United States should follow Europe's lead because the sacrifice that many companies will need to make will benefit all of the United States.

Although data breaches are preventable, sometimes mistakes are made, and one occurs. While data breaches can be forgivable, the main reason the occurrence is an issue for most companies is that they fail to respond and communicate the loss of data to their users or clients. Additionally, some companies do not even have the required protection needed, like Cybersecurity professionals, to prevent a breach from happening in the first place. This lack of security and communication leads to frustration and loss of trust for users. Cybersecurity should be a requirement for all companies that deal with vast amounts of data, especially personal data.

Companies and websites are not the only ones that can fail to protect their user's data. Even researchers can reveal too much information on their test subjects, extinguishing the anonymity of their experiment. For example, in Michael Zimmer's article ""But the data is already public": on the ethics of research in Facebook," he discusses a Facebook experiment that went wrong. The trial involved collecting data from the Facebook profiles of students from an

unnamed university; however, the university's identity was soon discovered, compromising the identities of the college students involved in the study. The data leak was not pleasant, and the researchers learned a valuable lesson. Despite their mistake, they did not face harsh consequences; instead, they set an example of the dangers of using social media to research. With no set punishments, what is to say that this event will not happen again?

The importance of privacy is crucial. Nobody deserves to have their personal information revealed to the world. With a law similar to Europe's new privacy law, the United States could benefit greatly, adding a set standard for companies and researchers to follow and set punishments for broken rules. With the idea of consequentialism in mind, some companies may have difficulties with stricter laws on privacy. However, Consumers, a more significant majority, will benefit and sleep easier knowing that they will be notified when their data is stolen so that they can take the appropriate measures to deal with the issue. Consequentialists believe that any decision is moral as long as the greater good is benefited. So, if the extra steps that companies will have to take will help a vast majority in the long-run, then the change is worth it.

With the above idea in mind, I believe the right thing to have done when the test subjects' identities were exposed would have been to punish the research team with a fine or something equal to that. Additionally, the students who were exposed should have been compensated financially or something of fair value to the loss. No matter how the issue is resolved, the students at Harvard University will not be able to take back the information that was shared about them through the experiment online. Hopefully, if any tests like this one are performed in the future, the researchers will do a better job of keeping the identities of the subjects anonymous. Furthermore, I hope that the United States will take matters of privacy invasion more seriously.

Facebook is not the only social media platform that privacy is essential. Platforms like Twitter, Snapchat, and Instagram are examples of social media that allow people to share their lives and thoughts with others. With options to keep their account private, people are given the ability only to enable people that they accept to view their posts. However, some people use these platforms for the wrong reason. For example, in Elizabeth Buchanan's article "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL," she discusses the ethics of big data research, specifically, the appearance of ISIS supporters on social media. Everyone has the right to their own beliefs; however, to many nations, ISIS is a terrorist group with the intent to harm, so their right to free speech on the internet is questionable. With ISIS' involvement in this case aside, Buchanan starts the article with the ethical use of big data research, claiming that "Ethicists and privacy advocates" have "pushed back against large-scale data mining and analytics," but "data have become so readily available," being that it is provided by the users, "the battle to protect individual liberties seems increasingly more challenging." A stricter privacy law similar to Europe's in the United States could put a more stringent hold and specify the ethical and unethical uses of public accounts in research. This law could set a standard for what researchers are allowed to do and the methods that they would face the consequences of using.

Since many people use social media and privacy being an option, many people open up their personal lives to the public, allowing anyone and everyone to see it. While this is rare in most cases, unless they're a celebrity or public influencer, the question in the air is, "Is using public accounts in research without the user's permission ethical?" The answer to that question, in my opinion, is yes. Setting their accounts to public opens them up to everyone with internet access, so I see no harm in their account being used in research as long as their identity is not

revealed. Even though their accounts are open does not mean that the researchers would need to mention the names of their profiles, revealing their existence to more people.

From a consequentialist's point of view, the use of public social media accounts in research would be seen as harmless. It does not have a significant impact on anyone, aside from the knowledge that can be learned. While a consequentialist may not focus on it, they would not see it as having a significant impact on the greater good, making it acceptable to them.

In the case of the ethical use of big data research, I believe it is harmless to use public accounts without the user's permission in research as long as the users' identity is not revealed. With a consequentialist's ideals and the privacy options given to social media users in mind, the use of public accounts in research is harmless to the individuals. As long as the topic is not too narrow, I do not see a way of someone finding out the subjects' identities through experiments.

In conclusion, with the two articles mentioned and the theory of consequentialism, I believe that the United States needs to adopt a new privacy policy similar to Europe's to prioritize the importance of privacy. In the example of the experiment in Buchanan's article, no law was set to punish the research team for allowing the identity of the university used to be exposed. Furthermore, nothing was done to make up for the damage that was done to the students involved in the experiment. The students had private information revealed about them that was entrusted to the research team. Additionally, consequentialism shows that new privacy laws in the U.S., similar to Europe's, would help the greater good, allowing everyone to feel safer about the data they have entrusted with companies. With no set laws, companies can get away with data breaches, leaving people with nobody to trust. If there was a consequence for companies to face for not communicating with their users about losing their data, they would

strive to do a better job at protecting their users' data and communicating with them when it is stolen.