The United States should adopt a policy like Europe's new Privacy Laws so that we have more control on how our data is handled, to have the option to opt-in or opt-out of data usage and know when our information was involved in a data breach. In this Case Analysis I will argue that Deontological shows us that the United States should follow Europe's lead because it is very beneficial to the citizens and businesses by giving them power over their personal information and choices of what and where their information is involved in or not involved in regarding third parties. It also gives a broader definition of what our personal information is and how it is linked to us. It also makes organizations, and third parties think twice on how they are gathering users' data because of fines that are issued if proper handling is not taken into place. This makes organizations respect the rights of data owners.

In the Zimmer report the research that was taken place in 2008 over a 4-year span with about 1,700 college students at a US university was not organized correctly pertaining to the students' Facebook accounts. They had reported that these students' personal identifying information was encrypted and would be deleted after the research was over or when the "last wave of data is processed". From the very beginning, the college where the students were attending was founded from the majors, they interpreted it could only be either a few colleges and was later figured out that it was Harvard College. Data was extracted from Harvard including housing records and from Facebook without the students' knowledge or confirmation. This gave no opportunity to the students to either correct or approve the information that was collected.

If the US had a GDPR policy this kind of social experiment would not have happened. The students would have full control of their personally identifying information and most of them would have opted out of this because of the harmful impact that could be damaging to their families and their own reputation. The impact that could come from this includes their information getting lost or in the hands of someone not intended to see it. Under GDPR policy, the T3 research team would have been fined for exposing the students' PII. Such data acquired included the subjects' self-reported gender and ethnicity, their home state, nation of origin, political views, sexual interests, college major, relational data and cultural interests and students' housing information and personal email addresses were given to T3 research team from the college.

The main part of the ethical tool Deontological specifically the categorical imperative, is being moral all around, to respect not only yourself but everyone around you, the importance of free will and consent, and to always do the right thing even if it is harder. The right thing would have been to get proper authorization, asking the students for their consent before going to the college and onto their Facebook pages to collect information on them. Harvard college did not do the right thing giving T3 research team the permission to access the student's information, they did not consider them and should have gotten way more information on what the experiment entails thus resulting in the subject losing control over their data allowing others to be able to download the data released. Even though this would have been the harder thing to do because the T3 research team would assume most of the students would not consent to the experiment. The T3 research team did not consult with a privacy expert on this matter because in their excuse, the Facebook pages are already public so anyone could look at the students' pages if they wanted to. The students most likely did not know that their Facebook page was visible to the public and if they found out they would adjust that in their settings.

In Buchanan's reading, "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL", the Iterative Vertex Clustering and Classification model is used to identify terrorist supporters,

specifically ISIS on Twitter. For the safety of US citizens, protecting individuals here from terrorist organizations is law enforcements and military's top goals. To address this goal, they must put a name to the individuals and stop further communications so that the network does not expand. The big data research however does not ask for consent from Twitter users, but it is necessary to identify and study these groups in order to protect US citizens. Buchanan talks about reidentification techniques being used as risk and benefit factors in the current US Common Rule. If we had GDPR policy in the US, reidentification would not be an option because it would not be as easy to collect PII.

Buchanan states, "Individuals in research must be treated in an ethical manner by respecting their decisions and protecting them from harm, and ultimately, researchers are expected to secure and protect their participants' well-being." This statement is very ideal for deontological manner. By making sure that the individuals in this group are treated equally with respect even though they are in a terrorist support group is doing the right thing by treating them the same way you would treat anyone else. Like the "Tastes, Ties and Time" project, the data was publicly available on Twitter, so technically they do not have to ask for consent, but this is not moral. In order to be ethical, we must treat others how we would want to be treated. Even if our Facebook page is public it should stay on there, not be extracted out and be on display for more individuals to see. In a Deontological manner, doing the right thing means respecting others and, in this matter, respecting privacy on individual's social media pages not using their posts for experiments or for testing even if it is doing no harm, in fact it is worse that the individuals had no clue that their information was being used without consent. By failing to let the individuals have knowledge that their social media pages were being spied on for a span of 4 years is the same as lying to them. By doing these unethical procedures and wrongly justifying their actions is being unfair to others. Again, if you do not want to be spied on and have others collect information on you then do not do it to others, it does not make it better that the individuals had no clue that their information was being used as an experiment.

Cybersecurity and Privacy Law in a nutshell by Jay P. Kesan and Carol M. Hayes talks about a related case pertaining to the "Tastes, Ties and Time" project in an incident with Facebook on page 249, it states, "In the published article, the authors explicitly state that because Facebook conducted the study, the participants were already subject to Facebook's Data Use Policy, and because they had agreed to that policy, they provided informed consent. But according to archived websites, Facebook's data use policy did not say that Facebook could use your data for research until May 2012." This is a reason to always be aware of terms and conditions and to keep up with updated versions.

In conclusion, the United States should have general data protection regulation policies in place so that users do not have doubt or worry about if their PII is secure or not or in a study that they don't know about, instead users would be confident. If we had GDPR policies in place, our definition of personal data would be extended to pictures of ourselves, our IP address and sensitive personal data. We would be able to prevent our data being taken away or mishandled in case of a breach being notified in a timely manner. We would not have to go back and forth between companies to get off their mailing list or have our personal data deleted as well. Users will have trust and form a bond in organizations holding their data and securing it because they will have a better understanding of the policy and how to take appropriate measures in data protection since the fines of not holding up to the policy and complying with it are great.