

Case Analysis: User Data

In Danny Palmer's article, he talks about the General Data Protection Regulation (GDPR). Palmer expands on the GDPR and its purpose in the European Union (EU). The GDPR applies to any organization operating within the EU and any offering goods and services to customers or businesses in the EU. The significance behind the GDPR is that it ensures that personal data is gathered legally and under strict conditions but along with obtaining the information in a legal and ethical way, those who collect and manage the data are obliged to protect it from misuse and exploitation. Failure to comply with these terms will result in penalties such as a fine or imprisonment for up to six months. The GDPR expands on the idea of what is considered "personal data". Initially, names, addresses, and photos were considered personal data, but the GDPR includes IP addresses, genetic data, and any other data that could be processed to uniquely identify an individual like biometric data. In terms of consumers/citizens, GDPR is all about the people. The GDPR provides consumers with the right to know when their data has been hacked, easier access to their own data in relation to how it is processed, the right to opt out of their details being on mailing lists, and the right to have personal data deleted and forgotten if they wish. In this Case Analysis I will argue that the deontological tool shows us that the United States should follow Europe's lead because the EU is doing the right thing and being moral by having the GDPR in place.

In Zimmer's journal, he talks about the T3 project and the ethics of it all. Zimmer mentions that the project has many ethical flaws and privacy violations, such as the amount of personal information stored, improper access to personal information, unauthorized secondary use, and errors in personal information. In relation to Palmer's article, Palmer talks all about the GDPR and the ethical flaws of the T3 project mentioned by Zimmer would be in violation of the GDPR. The GDPR has rules in place to regulate how personal information or data is gathered while also not obtaining consent from the subjects. Additionally, the data collected by the T3 project researchers was being made available for download which may result in unauthorized secondary use. Subjects did not have a say in how their data was being used and I mention this because the GDPR ensures that consumers/customers are notified and aware of how their data is being used as well as having the right to not allow it or opt-out. The researchers would also store the subject's data for multiple years which also violates the GDPR. Finally, due to the subjects not being aware of their data being collected, they were not allowed to access/view the data to correct for errors or unwanted information.

The deontological tool backs up why I think the United States should adopt something like Europe's new Privacy Laws (GDPR). I say this because deontology is all about doing what is right. Immanuel Kant believes that doing the right thing simply means respecting others and not using them. Kant also feels that the duty to respect others is absolute, and it is never right

to fail to respect others for the greater good. In this case, respecting others is exactly what the GDPR is in place to do as it provides people with something that they are owed as a citizen and that is privacy, protection of data, and control of data. In the United States, we lack control of our personal data so once it's out there we have a say over how it is used, who has access, or how it is obtained. So, with the T3 research team should have avoided all these unethical practices and done so by simply getting consent from test subjects. Overall, Europe is doing what is right by having the GDPR in place because it is morally correct and ethical. There is no regard for the greater good as with deontology, the greater good shouldn't stop one from doing what is right no matter what the outcome is. The United States does have something like the GDPR, but it doesn't cover all types of data and the different laws only apply in certain states within the U.S. For example, HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA. In most states, companies can use, share, and sell any data that they collect without notifying the owners of the data. Furthermore, when companies sell data to third parties, those third parties can sell it without notifying you. The United States' way of handling user data is unethical and immoral, being the opposite of deontology and is like the ethics used by the research team for the T3 project.

In Buchanan's journal, she talks about how it is becoming more difficult to protect individuals' data and liberties with data becoming so readily available by the users themselves amongst other factors. The fight in the United States is primarily against large-scale data mining and analytics in the name of national intelligence and security. One of Buchanan's primary concepts is how big data mining is occurring and resulting in individuals losing privacy due to the results of big data research revealing much information about an individual and his/her networks of relations. This is backed by the fact that big data mining is often discriminate in being able to tell who is supportive of what as well as the interests that one may have. Buchanan explains that there is a process that can determine if someone is a supporter of ISIS/ISIL by obtaining their data and running tests. It is mentioned that the subjects have no control over whether their data is used in this test or not and there are clearly lots of ethical issues with this. It begins with users agreeing to their data being mined and used for marketing purposes but once their data is obtained, it can now be sold which is how it ends up being used in tests and experiments. Overall, this goes to show how users have no control over how their data is being used after it is out there.

The research ethics used in the project clearly have complications and these complications are addressed in the EU's GDPR. The act of data being mined and gathered for one thing but then being used for something completely different without one's consent or knowledge is immoral as it infringes upon one's privacy and would certainly violate the GDPR. This project is more than likely occurring in the United States due to the United States not having a countrywide law in place to protect all forms of user data from unethical practices like, in this instance, unauthorized use. The GDPR would first require companies to obtain the information lawfully and then after it has been acquired any usage would require consent from the owner. In contrast, the United States allows companies to acquire information and have free will with what they do with the information.

In relation to Buchanan's journal, with the use of the deontological tool, the team carrying out the project could avoid such unethical practices by obtaining consent from test subjects before distributing their data and using it for unauthorized purposes. The team is acting in a way that is opposite of what deontology is all about. Again, deontology is all about doing what is morally right no matter the consequences and/or outcome. However, I must include that the project was indeed for training and helping law enforcement officers better detect specific individuals and groups in large data sets. Even though this is the reasoning behind the action, it doesn't make it the right thing to do as it is still infringing upon the privacy of users and is immoral and unethical.

Overall, I firmly believe that the United States should adopt something like Europe's new Privacy Laws, also known as, the GDPR. The reasoning behind it is simply backed by the deontological tool. The deontological tool puts emphasis on doing what is right and doing it out of respect for others. I like to look at it as doing unto others as you would have them do unto you. The United States adopting such privacy laws would make sense as the United States after all as all human rights are of significance so what better place to start than the personal information of the people? In a deontological mindset, enforcing such laws would merely be giving citizens and consumers what is owed to them and that is the right to control their personal data. Adopting such laws would also come with consequences such as hurting smaller businesses that may not have many funds but after all, deontology is all about doing what is right with no regard for consequences.