Case Analysis 2 – User Data

Will Lawson

Within Danny Palmer’s, “What Is GDPR?” article, he discusses exactly what GDPR is and how it impacts individuals and businesses, along with ensuring compliance. GDPR, General Data Protection Regulation, is a regulation of the European Union that helps strengthen upon existing data protection frameworks. GDPR focuses on protecting user’s personal information by setting a command set of standards for organizations to follow regarding handling user data. In doing so, legal obligations are set for organizations to follow so that they take privacy issues more seriously. GDPR requires many important things such as notification to users of any breach, strict policies on handling user data, having the correct personnel, and so on. Any organization that fails to meet these requirements are subject to be punished with fines. Palmer stated, “In the year since GDPR was introduced, some of the world’s largest technology firms have attempted to re-position their products as privacy-focused- a strategy that has likely come about in some part due to increased awareness around privacy and consent.” Many countries such as the United States have questioned their own privacy laws due to the awareness raised by GDPR. In this Case Analysis I will argue that the deontological tool for moral reasoning shows us that the United States should follow Europe’s lead because of the stronger sense of privacy and security it provides users, thus guaranteeing a better chance at giving everyone the same kind of respect.

In Michael Zimmer’s article, “But the data is already public,” Zimmer discusses a case study involving a group of researchers, known as the T3 research team, who publicly released profile data associated with a group of Facebook accounts of college students. Within Zimmer’s article, he articulates a set of ethical concerns that must be considered before engaging in future research and shows how the T3 research team failed in maintaining the privacy of the Facebook users. The “Tastes, Ties, and Time” project was essentially a research project that took a group of college student’s Facebook profile information and attempted to remove the personally identifiable information away so that they could publish it. Zimmer focuses majority of his article on how easy it would be to figure out who these college students were, despite the T3 research team giving ‘good efforts’ to stop that from happening. In focusing on the insufficiency of privacy protection in the T3 project, Zimmer was able to show one key principle that the T3 research team failed to consider. Zimmer discusses two theories: “harm-based theory of privacy protection” and “dignity-based theory of privacy protection.” The “harm-based” theory focuses on the fact that if the data is protected against a hacker or someone that could potentially cause harm, the privacy is safe and maintained. The “dignity-based” theory focuses on the fact that one does not need to be a victim of a tangible harm for there to be concerns over the privacy of one’s personal information. Zimmer mentions in his article that one of the leaders mentioned hackers and other threats that alluded to an “harm-based” theory approach. Zimmer is proving that the T3 research team failed to consider a core principle of deontology. With the research team focusing only on the harm that could be produced as a means of privacy, they completely ignored the broader theory of “dignity-based.” The “dignity-based” theory recognizes that just something as simple as having “one’s personal information stripped from the intended sphere of the social networking profile” is enough to be a concern for privacy. Within Kant’s deontological moral theory, he states that there are ways that we can wrong others or do immoral, even if it doesn’t cause harm to them. By undermining one’s dignity, privacy is also lost. Specifically in this case, the group of researchers give a “good effort” to maintain privacy, but instead did the opposite while trying to do good. This is a perfect example of Kant’s deontology. Relating back to Palmer’s case study, it deontological ideals are spread throughout the structure of GDPR. GDPR is rooted in that privacy must be maintained amongst all users. In the case that someone’s data is breached, whoever is in control of that data needs to make the user aware of the breach quickly. This fits perfectly within deontology as people’s reasons should be based upon the best reasons and to treat others with the same respect. The United States should consider adopting similar regulations or standards that focus more on the privacy of the user and how data is handled. By using deontology as the moral reasoning behind the regulations, users would be closer to having protection due to everyone giving each other respect and by doing the right thing, even if it would be easier to do the other.

In Elizabeth Buchanan’s article, “Considering the ethics of big data research: A case of Twitter and ISIS/ISIL,” Buchanan reviews a related article to reflect on the ethics of big data research methodologies. Within her review she discusses how social media has allowed for the expansion of many different groups of people between law enforcement to terrorist groups. Large scale data mining and analytics are also introduced to show how the battle of protecting individual liberties has become more difficult. The discussion centered around ethics of big data brought up the point that finding different members of ISIS would be just as easy as identifying people who shop at Walmart. The methods that are used within data mining can transcend contexts which means that it can be used in any case. If it can be used in any case, areas that are less regulated could be at risk of being exploited. Data mining has brought more ethical reflection to the United States due to the potential impacts and consequences of it. With data mining readily available in every field, it becomes very difficult yet crucial to focus on regulating user’s privacy. This relates to the deontological tool for moral reasoning because people are realizing that they must focus on doing the right thing even if it is more difficult to do so. With this article and Palmer’s article mentioning the United States questioning their own privacy regulations, I believe it would be a good idea to follow in the footsteps of Europe. Buchanan mentions is this article that, “the last time the United States federal regulations around human research protections were revised was 1991.” This does not reflect the amount of technological change, therefore leading to concerns around privacy and security. Palmer also mentions that California is already following in the footsteps of GDPR by allowing individuals to have a stronger voice in how their persona data is handled. All these concepts and thoughts point to deontology. Deontology represents giving everyone the chance to choose for themselves and promoting respect towards others. Respect must be absolute and without respecting user’s information, issues arise. Both articles mention the concerns surrounding this and hint at the fact that the United States should follow this approach to give their users a better sense of privacy and security. Another point that Buchanan makes is that the intent of which the data mining and analysis matter. One user may be okay with allowing their data to be used for marketing purposes while that same user would not want their data used regarding intelligence gathering. However, the current structure of big data doesn’t allow the user the choice in a lot of scenarios. For the United States to give user’s a better voice, they must revise some of their regulations. Following an approach rooted in deontology, will assist in making sure that every user is afforded the same rights. Buchanan establishes many ethical dilemmas like those in Palmer’s case study. With many different organizations being involved in such a complex network, more regulations could only assist in making sure that individuals maintain their sense of privacy.

In this Case Analysis, I argued that the deontological tool for moral reasoning shows us that the United States should follow Europe’s lead because of the stronger sense of privacy and security it provides users, thus guaranteeing a better chance at giving everyone the same kind of respect. Looking at the issue of securing user data and privacy through a lens rooted in deontology shows that more regulations would assist in providing the same rights to everyone. It is our duty to respect others and to allow everyone to have the same voice. Within Zimmer’s article, it is shown that a lot of issues can arise when there is not enough prior thought into handling user data. What constitutes privacy should be thought of in a broader sense such as the “dignity-based” theory. Realizing that user data should be protected as if it were your own is crucial. Buchanan raises thought towards issues surrounding privacy and ethics of big data mining to essentially show revision is much needed. If the United States followed in Europe’s footsteps to implement better regulations for user data and privacy, I don’t see how it wouldn’t be somewhat successful.