Ethen Brandenburg

Professor Montoya

PHIL 355E

20 July 2023

Case Analysis: User Data

User data is a very important piece of the way the online world works along with data protection. EU or European Union, they have constructed a regulation called, The General Data Protection Regulation (GDPR) which is governed by the EU or European Union. This regulation was created to ensure that user data is protected and if it is not then the parties involved with the data leak would be held accountable. This regulation, which is still in use today, has many good "regulations" or rules that are needed to be followed in order to be compliant. Most of them are proper ways to store and use user data along with reporting attacks or leaks to the EU and the user, depending on the use case of the data.

The EU presented this regulation in April of 2016 but it was not put into effect until May of 2018. The businesses affected by the GDPR included retail, e-commerce, or basically any other business that would handle user data. User data is names, passwords, emails, addresses, etc. Most of that data is PII (personally Idenfinable information) and information that should not really be on the open internet. In order to be compliant with the GDPR companies are required to store and use data in specific ways along with reporting any "outbreaks" or leaks that occur on their platforms. Even in certain situations, they are required to let the user know of the leak

unless the GDPR states not to, but those are very limited circumstances. In this Case Analysis I will argue that Consequentialism shows us that the United States should follow Europe's lead because having a power that regulates and enforces data protection is what we need in the United States.

In the United States, we have laws regarding data and how we should store that data. But we do not have a centralized regulatory committee like the EU has with the GDPR. With GDPR they are required to report that data leak and the company is held accountable, financially and with their reputation. In the United States, we do not have a regulatory committee for user data, which means we do not officially hold companies accountable for data breaches as we should.

Now looking at this from a consequentialism point of view we can state that companies in the EU or European Union, we can say that companies might be acting out of consequence. For instance, a company strives to protect user data just due to the fact that if they do not they will be fined. This is not necessarily a good idea because as a result, we would be making the "wrong" choice ethically because we do not do this without looking at the consequences. But in reality, we all work off of consequentialism because we all know if we do something because we know if we do not then the consequences would be bad or vice versa. I believe that most of the companies in the EU work out of consequentialism due to the fact that if they mess up they can be fined or destroyed by their reputation. In the United States, we need this committee to instill "fear" or consequences in companies that do not practice the same or close to the same standards as the EU does with the GDPR.

Michael Zimmer argues a few great points in his article "*But the data is already public": On the ethics of research in Facebook. Ethics and information technology,"*. The article give the kind of a brief overview of how Facebook obtains data and "sells" it to researchers. This data included PII (Personally Identifiable Information), profiles, posts, and people's interests are. Now data collection is not anything new and really is what is the backbone of how the internet works. You enter what you want and it queries databases that find related information. A use case for the data collection would be to "pre-query" the databases for recently searched topics in order to have the information pop up faster than waiting for it to load. This not only makes the user happy but also takes the strain off of the database but it comes with a risk as well.

The risk is that the protection of the data is somewhat compromised when it's being sold and collected by other companies. Not only is the transmission risky but also the storing of that data and use of that data that was not explained in the original company's terms of service. In the GDPR, companies are required to explain how data is stored and it has to be approved before that service hits the market. This is not the case in the United States and Zimmer brings this up with his views on the way data is stored and used by those third-party companies. This one is a major security risk but it could be stopped or even slowed down in being a risk if the United States had a regulatory committee like the EU's GDPR. Even if we took this view and partnered it up with the consequentialism point of view then we could even say that we would do it out of the fear of bad consequences. This in itself would be a "bad" action because it's not genuine but it is a good reason to move to a GDRP-like system.

Another author, Buchanan, brought up a good argument when he said that there needs to be a fine line drawn between gathering information for marketing and gathering information for intelligence purposes. The GDPR has strong regulations when it comes to using information for marketing purposes but it also has strong rules regarding how the data can be used. The United States really does not have anything governing the difference between the two. Sure there are some regulations with storing PII but not strong regulations on how and why you are using the PII. With consequentialism, we could say that if there was a line drawn between gathering information for marketing and for intelligence purposes, you'd see people comparing and contrasting the two "worlds". Obviously, this would cause people to lean towards gathering information for the less invasive approach, marketing, instead of intelligence information. Only because people would be afraid of the bad consequences that can occur if they do not do the right thing. Either have your personally identifiable information thrown around or be afraid of that happening and you choose the "right" thing or less bad thing. This obviously is not the way to think and live your life but many people do this to this day and Buchanan was very smart when I stated that there needs to be a clear line between the two. Without the line there would be no morals and without morals there would be no structure.

Data is a precious resource when it comes to the internet and all the web applications that you can possibly think of, but it comes with undeniable risks. The EU developed a simple but effective way of controlling and minimizing data leaks called GDPR (The General Data Protection Regulation). This regulation is a very important structure in the EU when it comes to data protection and uses. It lays out how and when to report certain events and also who and why certain pieces of data are being stored and accessed. With these regulations in effect the EU has

cut back on the data leaks and the United States should consider adopting this system. Now the EU has made the GDPR relatively strict but it is also very straightforward and has repercussions if it's not followed. If the United States carried out a similar approach to the GDPR I believe that we would have fewer data leaks/breaches and fewer cyberattacks trying to steal or manipulate data.