Reed Wilhelm

PHIL 355E

2/8/24

Case Analysis 2.4

Data protection and online privacy laws have always been important since the beginning of the digital age, and as more things move online, securing personal data has never been a more difficult and important task. Additionally, there are more dangerous threats online now, and whether they're hackers or simply scammers, personal data is something that's incredibly valuable to these online threats. In early 2012 the European Union (EU) realized how potentially dangerous these online threats are and started work on creating the General Data Protection Regulation (GDPR), which was put into effect may of 2018, with the goal of protecting personal data and holding companies and organizations accountable for any breaches. The article, "What is GDPR? Everything you need to know about the new general data protection regulations," by Danny Palmer, outlines the general purpose of the GDPR and how it enforces its rules. One of the first thing that palmer points out is what the GDPR considers to be personal data, which includes things from IP addresses to genetic and bio metric data, along with anything that could be used to uniquely identify an individual. on top of that, Palmer also notes the strict fines and penalties for companies that have a security breach as a result of failing to complies with GDPR rules, the maximum fine is 20 million euros or 4% of the companies worldwide turnover, and a fine that amount would result from an infringement on the rights of the data subjects, whether that be something like unauthorized transfer of data or failure to put adequate protective measures in place. Smaller fines from the GDPR are in the range of 10 million euros to 2% of the

company's turnover, and this type of fine would be for something like mishandling data, failing to meet regulations, or not informing relevant parties of a data breach. Overall, in think that the GDPR is a good way of helping hold companies accountable for their user's personal data, and using Contractarianism, I'll explain why something like the GDPR should also be implemented in the United States.

As I mentioned before, online privacy has always been an issue, however it's even more relevant when looking at social media. Since they first launched social media sites have always been the subject of much criticism when regarding their online privacy measure, however no platform has received more scrutiny that Facebook. A good example of this is the "Tastes, Ties and Time" project (T3), which privacy and data ethics scholar Michael Zimmer wrote about in an article titled "But the data is already public," where he discusses the T3 project and the ethical concerns around its use of data pulled from Facebook accounts. For a brief overview of the T3 project, Tastes, Ties, and Time was a study done by a group of researchers, where they collected and analyzed data from a class of college students over the course of their four years in school at an unnamed northeastern university. All the data in T3 was collected using Facebook and done without the knowledge or consent of the students. The university as well as Facebook approved the project and allowed the T3 group to access the publicly available Facebook profiles of the students, T3 also managed to get information on profiles that were set to private by using research assistants at the university who were within the private profiles network. In an effort to try and keep the students anonymous, T3 deleted what they considered to be identifiable information, part of this was replacing the names of students with numbers,

however beyond that much information was viewable when T3 started to publish. Among the information that was released was the students major, residence, race, gender, political views, and home state, city or country. All this information combined resulted in the college being identified as Harvard University, and the ability to identify almost every student in the entire class of freshmen with relative ease. The issue was that, while the information may be innocent on its own, once an identification number is added and all the information is combined it's easy to re-identify the subjects of the study. So how would something like the GDPR along with a contractarian view of ethics help to prevent something like this in the future?

Contractarian morality is based off the unspoken social contract between members of society. And contractarianism argues that actions themselves aren't inherently right or wrong, but we decide what is acceptable through the basic set of ground rules that is the unspoken social contract. A couple examples of something that might be considered a breach of this social contract would keeping tabs on people without them knowing, or maybe looking through windows into someone's house. If a person got caught doing either of those it would be considered very odd behavior and an invasion of privacy. In the case of T3, keeping tabs on people without them knowing is exactly what they were doing, except they did it to an extreme that could be considered stalking, and they achieved all of it using Facebook profiles.

The reason that I believe a contractarian view would support the idea of the GDPR is that while T3 might be considered unethical, there was no true repercussions for either the T3 research group or Facebook aside from bad press. But if there were the General Data Protection Regulations in place, Facebook would've at least been held accountable for mishandling user data by letting T3 gather and study it, which would result in a fine. It's also important to note

that T3s main defense for publishing their findings which allowed students to be identified is that the data was already on Facebook and therefor viewable by the public. However, a contractarian view would once again disagree with this, as while the information was posted on Facebook, “it does not mean it’s fair game to capture and release to all” (Zimmer). Its also worth pointing out that, like Zimmer says, privacy on social media is something that’s still very poorly defined. We agree to the terms and conditions when first joining a platform, but most people don’t really read them or understand what the terms and conditions actually are. And finally, most social media platforms already are GDPR compliant for their users in the Europe, meaning it wouldn’t cause too many issues for them if the GDPR came to America. Satisfying parts of the unspoken social contract by an increase in privacy along with adding repercussions for companies that mishandle user data like how Facebook did with T3.

Another article that can be used to show why a contractarian view would promote the idea of the GDPR in the U.S. is “Considering the ethics of big data research: A case of Twitter and ISIS/ISIL,” by Elizabeth Buchanan. Like the title implies the article deals with the ethics of collecting and analyzing data from twitter to identify and restrict accounts associated with ISIS/ISIL. From the start Buchanan points out, the current context of the Twitter data being gathered and Analyzed for the purpose of identifying accounts associated with ISIS doesn’t seem bothering at all, it makes sense and doesn’t seem like a cause for ethical concern. However, ethical questions are raised if the context is changed, Buchanan use the example of changing the goal of the research from identifying ISIS sympathizers to people who support the Black Lives Matter movement. And goes on to state that “Big data methodologies are not

discriminate," and that the algorithms used to identify ISIS/ISIL supporters can just as easily be applied to finding people with different political views or someone who shops at Walmart over Target.

By changing the context and goal of big data research projects the ethics of the situation change drastically, I think that most people wouldn't have a problem with big data research being used to identify ISIS supporters, but like Buchanan notes, once the context is changed people will probably feel different about it. This is where applying contractarianism helps to gain a clearer picture. A contractarian might argue that gathering and analyzing data with the purpose of identifying a group online is immoral due to it being a breach in expected privacy. Similar to what I said regarding the T3 project, looking through the windows of a house to try and find out more about a person's life, while not illegal, would be considered a breach of the unspoken social contract. in the case of using Twitter for big data research, a Twitter profile can be an open window, but that doesn't mean its socially acceptable to stare through that window and use what can be seen as data for identifying what group someone may belong to. and just because the information is public doesn't mean people would be okay with it to be analyzed by companies or governments. The reason I think that a contractarian would agree with implementing the GDPR in the U.S. because, while it might not restrict big data research, it would limit the ability for third parties to get their hands on information that wasn't intended for them. All while penalizing platforms like Twitter if they were considered to be mishandling private user data by the General Data Protection Regulations.

Another key point that Buchanan touches on is how agreeing to the terms and conditions of platforms like Twitter is somewhat of a "all or nothing" situation. Users can agree

to the terms, allowing them to use the platform and allowing for their data to potentially be used in both marketing and intelligence gathering big data research projects, or users disagree with the terms and conditions and are subsequently unable to use the platform. Buchanan goes on to note that while most people might be okay with their data being used for marketing purposes, intelligence gathering is much more invasive and the data being used would violate what many people consider to be their reasonable expectations of online privacy. This is another area that a contractarian might promote the idea of the GDPR in America. Placing limitations on what can be part of a platforms terms and conditions would help to maintain a basic level of privacy that we associate with the unspoken social contract.

One final point Buchanan briefly mentions that really stuck with me and that I think a contractarian might find interesting, is that in big data research using social media, the concept of a "data subject" is essentially a replacement of a "human subject." The sheer scale of big data research makes us lose sight of the human aspect of its subjects. For example, collecting and analyzing data from 100,000 Twitter profiles feels like looking at a bunch of data points and trying to find relationships between them. But if that number is scaled down to 100 Twitter profiles, analyzing that data now feels unethical, almost like stalking 100 different people and keeping tabs on them to try and draw conclusions about who they are. Once again, this falls under the idea of violating what might be considered a reasonable expectation to privacy, and once again something like the GDPR would be able prevent big data research projects in America from going beyond what would be considered ethical from a contractarian view.

In conclusion, the protection of personal data has, and will always be an issue all over the world. The goal the EU had in mind when creating the GDPR is to protect private user data as best they can while holding companies and organizations accountable when they fail to do so. I think that contractarianism would agree with the GDPR, or a similar set of regulations being implemented in the United States, as much of what the GDPR aims to protect falls under what many might view as part of the unspoken social contract that contractarianism revolves around. Having the GDPR in the U.S. would also help to prevent situations like the T3 project, and as a result over 1500 Harvard students wouldn't have had their personal information published without their consent. Along with that, having the GDPR would mean that people wouldn't have to worry as much about their Twitter history being analyzed with the goal of finding out who or what they support. I understand why some people might be opposed to the GDPR, with the main reason that I can think of being national security. Being unable to collect information as easily through platforms like Twitter and Facebook would mean it would be harder to identify and stop are those who are trying to spread harmful information. But that's another place where a creating a version of the GDPR with a contractarian view could help and basing it off what's a reasonable expectation to privacy would allow for exceptions in certain cases.

Works Cited:

Buchanan, Elizabeth. “Considering the ethics of big data research: A case of Twitter and ISIS/ISIL” *Plos One*. Dec 17, 2017. https://odu.voicethread.com/lti-student/3968938/?tok=63242861065c3fcafef54a1.55511815

Palmer, Danny. “What is GDPR? Everything you need to know about the new general data protection plan.” *ZD Net*. May 17, 2019. https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Zimmer, Michael. “But the data is already public” *Ethic and Information Technology*. (12), 313-325. 2010. https://odu.voicethread.com/lti-student/3969437/?tok=138229776765c50ca5301de3.77139209