Atticus Emilsson

PHIL 355E

Module 2

2.4 Case Analysis on User Data

In the article written and presented by Danny Palmer, titled *What is GDPR? Everything you need to know about the new general data protection regulations*, he lays out what the European legislation entails in an incredibly clear manner. The GDPR (General Data Protection Regulation) is the first, all-encompassing privacy legislation of its kind that exists to protect the data of the end-user. It has introduced a new lens for viewing user data and a framework for designing solutions and organizations in a way that considers protecting said data from its conception. There have been some attempts to replicate this on a state-by-state basis such as Silicon Valley's CCPA (California Consumer Privacy Act) and Virginia's VCDPA (Virginia Consumer Data Protection Act); however, these function on a state-by-state basis and are not quite as refined as the Europe's GDPR. In this Case Analysis I will argue that Contractarianism shows us that the United States should follow Europe's lead in developing data protection regulations because, under a veil of ignorance, any individual would prefer a society where their PII (personally identifiable information) is reasonably protected against overreaching organizations, governments, and advanced data processing technologies.

In the writings by Michael Zimmer titled *"But the data is already public:" on the ethics of research* in Facebook, he presents a research study performed that leveraged public

information available on Facebook; however, there was a critical misunderstanding of the privacy implications their study introduced. Zimmer presented various instances of the T3 researcher's failures to protect the private information of research "subjects." It is not always an easy feat to identify whether an entity's actions were indeed a breach of privacy, so Zimmer introduces a framework that was organized by Smith et al in a paper titled *Information privacy: measuring individual's concerns about organizational practices* (1996). This framework identifies four "salient dimensions of privacy violations" clearly and concisely that enable anyone to determine whether a privacy violation took place or not. These four dimensions are as follows: the amount of personal data collected, improper access to personal information, unauthorized secondary use, and errors in personal information. These dimensions also enable us to view privacy violations through a more objective lens, meaning we can argue for user data privacy and security more concretely through the implementation of new privacy legislation. We can leverage this framework that was designed by Smith et al and introduced by Zimmer to identify where the T3 researchers went wrong. The identification of failures to protect individual privacy and the lack of satisfactory effort to do so is essential in designing accurate definitions of what PII and other aspects of privacy consist of. The definition of PII varies greatly between different regulations, locales, and governing bodies. These discrepancies make it incredibly, but understandably difficult to design a consistent framework that protects such data. After all, how can you protect something that you simply cannot define? Zimmer also introduces two methods of viewing privacy and those are the harm-based and dignity-based theories. The harm-based theory revolves around the potential for a bad actor to leverage personally identifiable information with malicious intentions. These intentions include stalking (incl. cyber-stalking), unauthorized access to computer systems and/or networks (hacking), and assassinations. The

dignity-based theory states that one can exhibit concern for their privacy without there being a looming threat to their own safety and/or security. This is especially true if one considers a perspective where an individual's identity is comprised of their personal information/data where an attack on their information is an affront to their identity.

By using these theories and frameworks introduced by Zimmer, we can effectively identify where researchers fail to protect the privacy of the subjects and develop solutions that mitigate these privacy implications. If we leverage both a harm-based and dignity-based approach to identifying information that may pose threats to an individual's privacy, it becomes incredibly apparent that without any sort of formal data protection regulations, individual privacy is virtually non-existent. The T3 research team not only managed to extract information that could be perceived as harm-based such as home addresses and ethnicity, but also extracted information that is in obvious violation of a dignity-based approach to privacy. This includes information such as online activity, interpersonal relationships, and other personal interests. The actions performed by the T3 research team also clearly indicate a privacy violation according to the previously mentioned framework. They collected an absurd amount of personal information over the span of four years, leveraged research assistants who shared a network with the students which enabled them to collect information that was not necessarily public, gathered the information for secondary use in an unauthorized manner in the case of student emails, and did not provide a platform/method that enabled subjects to correct information that contained errors. These factors indicate a gross violation of the individual privacy of the students involved in the study.

Through a contractarianism lens where we are completely unaware of what our societal position may be in the case of data collection and processing, coupled with the provided frameworks and theories that enable us to view privacy violations or potential implications objectively, the United States should implement a similar federal privacy framework like Europe's GDPR. Leveraging both a harm-based and dignity-based approach to privacy encompasses everybody included in this digital society. Under a veil of ignorance, one would indubitably decide to protect their privacy at the expense of enhanced advertising and marketing analytics.

The next referenced writing titled *Considering the ethics of big data research: A case of Twitter and ISIS/ISIL* is produced by Elizabeth Buchanan and featured in the PLOS (Public Library of Science) One journal. It considers the potential privacy implications of the Iterative Vertex Clustering and Classification (IVCC) model which was initially used to "identify ISIS/ISIL supporters among Twitter users." Buchanan introduces the possibility of this model being used for malicious purposes such as governments targeting political dissidents or party members targeting oppositional forces. The specific argument introduced by Buchanan was the possibility of using the same algorithm/model to target BLM (Black Lives Matter) supporters and activists. These possibilities are not far-fetched, as we already observe such malicious secondary uses of technology. One example of this is police officers and other variations of law enforcement officers leveraging their access to private information databases. These databases are only authorized to be used under specific terms; however, some individuals proceed to use this information to stalk ex-girlfriends or potential love interests.

Unlike the case presented by Zimmer relating to the T3 researchers and the information extracted from Facebook, where an individual uploaded the information (even though it may have been to a specific network or had other privacy restrictions), Buchanan's writings exhibit the IVCC model's ability to extract information regarding a person's interests and/or political affiliations without them explicitly stating them. This technology is incredibly dangerous if used by the wrong people and/or without proper and rigorous ethical review. These malicious use cases do not need to be political or governmental but can also be unethically leveraged by organizations. One of these potential use cases is identifying disgruntled employees. It can also be used during the employment and interviewing process to identify people who might partake in certain activities that are frowned upon by employers. This could be destructive to an individual's life, both figuratively and literally. Technology like this can completely bypass certain regulations imposed on employers and the employment/interviewing process.

Although this IVCC model is incredibly powerful and can prove to be beneficial in some cases, it introduces more capability to organizations and governing bodies to extend their reach of mass surveillance and data collection in an unprecedented manner. They might argue that they are only employing these technologies to identify potential terrorists or human traffickers; however, like many other technologies that inherently violate privacy, it will be used for other overreaching purposes such as identifying disgruntled employees and political dissidents. Any error in this model could also prove to be life-threatening. This technology would render the security and sanctity of those thoughts most private to us, nil. If this possibility were proposed to anyone under a veil of ignorance (per Contractarianism), especially considering the possibility of errors, they would not want this technology used. The privacy implications strongly outweigh the

potential benefits. This IVCC model makes it increasingly clear how little privacy we have. The only solution from a contractarianism perspective would be to implement stronger and clearer definitions of privacy and regulations on how people and organizations can interact with user data.

Zimmer and Buchanan both introduce profound cases that exhibit a clear lack of respect for the privacy of end-users or introduce technologies that may simply be too powerful. These cases make it increasingly clear how far these organizations are willing to go to obtain our private information, and how little they care about protecting it. Any safeguards implemented are the bare minimum and are not to protect users, but to protect their profits and reputation. Europe's implementation of the GDPR is a revolutionary implementation of privacy legislation that exists to protect individuals and hold organizations accountable for their ineptitude in respecting privacy. Of course, there are some cases where these technologies could be beneficial; however, the side effects could be disastrous. In the case of the IVCC model, the results are primarily predictive. Reliance on this for any form of accountability/prosecution would completely circumvent the "innocent until proven guilty" standpoint of the United States judiciary implementation and could be maliciously used in various other scenarios. Overall, it would be generally more invasive and imposing on the privacy of the individual in a way that nobody would appreciate if they were on the receiving end.