Avanti N. Garcia

Professor Garnar

PHIL 355E

01/27/2023

**Case Analysis – User Data**

**Should the United States adopt something like Europe’s new Privacy Laws?**

The case analysis for User Data, with the subsequent reading material by Danny Palmer titled “What is GDPR (General Data Protection Regulation)? Everything you need to know about the new general data protection regulations” discusses and reviews the implications of data privacy laws that were implemented in the European Union to protect online users from companies and how those companies collect, analyze, utilize and store our personal digital data. The question posed for this module “Should the United States adopt something like Europe’s new Privacy Laws?” can be answered by first establishing the means or purpose of the law and what it seeks to establish. In this Case Analysis I will argue that Deontology/Kantianism shows us that the United States should follow Europe’s lead due to the nature of proposed equivalent of the GDPR, which is to implement a means for which a user’s privacy comes first to everything else.

The central concept established by Michael Zimmer in his 2010 paper titled “But the data is already public” is in his own words “articulates a set of ethical concerns that must be addressed before embarking on future research in social networking sites, including the nature of consent, properly identifying and respecting expectations of privacy on social network sites, strategies for data anonymization prior to public release, and the relative expertise of institutional review boards when confronted with research projects based on data” (Zimmer, M. 2010) or in other words, that through his own research he establishes that the T3 (Tastes, Ties, and Time) research team did what it thought best and did make “good faith” efforts to protect the hide the identity and privacy of the data subjects. However, what the T3 research team did not understand fully, is that PII (personal identifiable information) as they understood it, is not all inclusive to what can be used to identify an individual.

The T3 research team mission was to understand social media networking with regard to social spheres, in order to do so, the research assistants (RA) were tasked with collecting the Facebook information of data subjects at Harvard University over the course of 4 years. As part of the research was funded by the National Science Foundation it mandates a condition that certain levels of data is shared. All PII was removed from the data source to ensure that the data subjects’ privacy was maintained prior to the release of the conditional data material. What was included in the release was a comprehensive “codebook” which detailed descriptions and frequencies of the data elements to include gender, race, ethnicity, home state, political views and college majors (Zimmer, M. 2010). What the T3 research team did not understand, is that through that public information in the code book that established that this research was derived from a 2009 freshman class of 1640 students in the New England geographic region and further detailed information such as ethnicity, college major. Following backlash, T3 realized that individuals are still able to identify individuals through a process of elimination. Zimmer details these efforts in his paper, as some ethnicities were represented in a singular person.

Zimmer further discusses that the response by Jason Kaufman, the principle investigator of the T3 research project, was invalid. Kaufman defended his research team by stating that hackers or others may already have access to the data subject’s information as it was pulled from Facebook, and that information is otherwise already public, and that the research information was not private, since it was already public. What Kaufman failed to realize, is that the RA’s may have access to otherwise personal information based on the Facebook features and privacy settings of subjects. The research assistants were in a position others outside of Harvard may not have been in, thus allowing the RA to pull private data that would not have been otherwise viewable by those outside of Harvard University.

Zimmer’s paper establishes the need for a universal understanding of how companies, corporations, and research teams funded by organizations collect, analyze, utilize and store information on individuals. Had something similar to the GDPR been in place, the T3 research team would have been required to comply with all the necessary laws set forth by the GDPR prior to the release of information. Within Palmers article the GDPR defines who is regulated by the laws; controllers “person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data” while processors are “person, public authority, agency or other body which processes personal data on behalf of the controller”. Through this we can establish that the T3 research and the National Science Foundation both fall within these boundaries. Furthermore, the GDPR expands what is defined and covered as personal data.

From an ethical point of view, utilizing a Deontological view on what the T3 research team did nothing wrong. They sought to do something good (conduct research to further knowledge and understanding) and in doing so, did something “bad”. However, they did not consciously do so, the purpose of the research was good, they received permission from the university and students, the way in which they did it was deemed good, the bad or negative collateral was accumulated without prior understanding or cognizance. Once the T3 team was made aware of the failure in the research methodology the immediately restricted the data and began conducting revisions to remedy the wrong.

A central concept presented by the second reading by Elizabeth Buchanan revolves around the ethics of utilizing online data mined from, in this example, Twitter to identify ISIS (Islamic State in Syria) / ISIL (Islamic State of Iraq and the Levant) members, supporters, and sympathizers for intelligence purposes. Buchanan’s paper “Considering the ethics of big data research: A case of Twitter and ISIS / ISIL” discusses the ethical implementation of using online social media platforms and other online venues to identify individuals through personal data. Buchanan establishes that in the twentieth century extremist groups such as ISIS utilize platforms such as Twitter to communicate, and through such, presents law enforcement agencies worldwide a new facet to which track and conduct intelligence operations on. But is it wrong to do so? Surely we can agree that using the personal data of a terrorist in the desert is not wrong, especially when that terrorist seeks to harm others and conduct operations that would cause fear and terror worldwide. But how far does the string go? When building a complex understanding of communication methods within an extremist group, how far is reasonable? If the terrorist sends an email to an individual in China, and that individual in China has a Facebook, and is in a group supporting ethical treatment of dachshund dogs, and someone stateside is in the same group, and they are part of a meme sharing group and a buy/sell page in Virginia, are law enforcement agencies allowed to follow the string from the desert to the home of a Virginia student because of overlapping spheres? Who determines what groups are observed? Buchanan also brings a valid point, that “big data” as she calls it, utilizes an algorithm to collect, store and categorize individuals. What do “big data” companies do with that information? If companies were to sell or share that information, it can just as easily be used to determine who loves dachshund dogs as it is to determine who sympathizes with extremist groups such as ISIS or ISIL. An additional concept brought forth by Buchanan deals with the implications of the theoretical handshake between agreeing to marketing and the agreeing to intelligence gathering. Individuals can agree to intelligence gathering for the purpose of ensuring a safer and more peaceful world, but not for the purpose that their information is sold to companies to increase profits for marketing purposes, and as commented by Dylan Whittkower “vice versa”. I may want companies to promote their consumer goods and services to me but not want to be surveilled by governments agencies.

The concept that government agencies and law enforcement can utilize companies stored data on consumers to categorically monitor them again enforces the need for legislature such as the GDPR. As mentioned by Buchanan, this paper was on the use of Twitter against supporters of ISIS/ISIL, however that data still remains for other groups such as the Black Lives Matter movement, Walmart Shoppers and possible political dissidents. Enforcing a GDPR like policy would ensure that companies cannot use mined personal data to identify the individual and furthermore do everything within their means to protect it. Having laws in place eliminate or at the very least reduce the capabilities for groups to use data to identify people based on digital fingerprints.

Deontological views would state that law enforcement should respect the privacy of individuals, and companies should refuse to share mined data with agencies and government structures on the basis that at any point, an individual can choose to do right. That by using personal data to categorize individuals on threat levels based on digital data compiled from the internet, would be already judging them, based purely on what they have done in the past. Deontology would dictate that building a profile of an individual would skew the perception of an individual, and that no matter what someone has done in the past, they are still owed respect as a person to their thoughts and privacy.

In conclusion, the United States should adopt or enforce legislature similar to Europe’s Privacy Law or GDPR (General Data Protection Regulation). Enforcement of such policy would ensure that when structuring online presence, any and all data collected is protected and is the foremost priority. Zimmer establishes that a policy such as the GDPR would ensure that all organizations, companies, and agencies utilize the same methodology to protect the same information that is defined as PII. Michael Zimmer’s “But the data is already public” established the need for a policy that establishes a universal definition of PII and how to protect it. Buchanan’s paper on big data and the relationship between personal data and how it is used by law enforcement agencies brings to light several questions regarding the extent at which LE (Law enforcement) are allowed to go in the name of national security. Buchanan’s concept of how personal data is used once collected again reiterates the need for similar legislature to the European Unions GDPR, to establish what can be collected, how it is to be stored, and how to ensure that PII is removed from that data. Furthermore, the GDPR establishes how individuals can manage their own data as well as holding companies responsible for the data they collect. Realizing that through this, we sacrifice “security” and safety for privacy, deontological view would first need to determine the purpose of the collection of data. Any answer would go against the privacy and respect owed to individuals. There should never be a need for a company to collect personally identifiable data and then store it for future use. This only sets up for failure to respect others on who they are now, but rather than who they were.