CASE ANALYSIS ON USER DATA

In the article, "What is GDPR? Everything you need to know about the new general data protection regulations," Danny Palmer breaks down the who, what, where, why, when, and how of the European Union's slimmed down legislation of everything data protection related, catching it up with the technology of today. He also covers what data protection could look like in a post fully implemented GDPR world. The United States has similar policies and procedures in place with some in the U.S. calling for full implementation through federal legislation. In this Case Analysis I will argue that Contractarianism shows us that the United States should follow Europe's lead because, some of the groundwork is already done, the last few but hefty steps need to be taken, and it will significantly decrease what businesses and consumers need to know about the legislation and how it affects them.

First, in Michael Zimmer's, "But the data is already public," he raises serious concerns for the ethical use of data in social networking research. Despite researchers using a process to anonymize subject test group data and an institution of higher learning review board approving the proposed method. It was quickly shown to have severe lapse in not thoroughly, but merely adequately protecting the information collected. He highlights the improper understanding of social networking sites privacy features or the privacy concerns along with waiving the necessity of consent in using data belonging to the subject test group. This is a very valid concern as the outcome will depend on the individual or group conducting the research and the definition of what is private and what requires consent.

The GDPR may be a unified and well thought through piece of legislation enacted by a large body enabling some streamlining of operations for a significant portion of the world by businesses, but it is still up to interpretation. More than good-faith attempts are required to safeguard privacy and user data. Otherwise, it is more of the same protect user data, user data is breached, fine and other penalties are applied, user information is in the open space for repeated misuse. An ethical baseline, the same definition for privacy, what user data are, and other considerations are required to apply the legislation evenly. A step in the right direction is baselining the legislation as close as we can across the globe. The standardization of terms and legal practices will diminish the excuse of ignorance because the rules will be very similar no matter where you go, as will the substantial penalties, hopefully working better as a deterrent.

In the view of a Contractarian, everyone falls under the social contract, in this case, business and consumerism. The consumer gives the organization their patronage and the organization have a user agreement. The user agreement varies from organization to organization and is so wordy hardly anyone reads them. The European Union as a sizeable body had created a single piece of legislation encompassing not only its geographical borders but also its people, meeting the terms of a Contractarian, applying to everyone within that governed body. The GDPR gives more control of one's data to the individual thereby improving the quality of life for the individual. In the United States there exists a social contract for business and consumerism as well, though there is no GDPR equivalent. This leads to a person being worse off in the social contract because the same protections, rights, and notifications do not apply for this person as they do for a member of the EU under the GDPR. The U.S. is almost there, but some key pieces are lacking such as a single legislation instead of a patchwork of laws ranging between stringent and severely lacking. The nature of business and consumerism is that everyone is involved, and it is hard to opt out. The trade off in the U.S. is presently lop sided with more benefit going to the organization than to the consumer. The U.S. could raise

Commented [MDM1]: This is a bold step in the right direction in protecting user data and can be used as a starting point for other governments to follow suit.

Commented [MDM2]: The U.S. has a patchwork of laws that include state down to municipal laws across the 50 states. This can make it extremely difficult for businesses to operate nationally.

Commented [MDM3]: This is a moral theory that claims moral norms derive their normative force from the idea of contract or mutual agreement.

Commented [MDM4]: Includes overhauling and aligning various levels of government without overstepping constitutional powers.

Commented [MDM5]: Zimmer, M. "But the data is already public": on the ethics of research in Facebook. *Ethics Inf Technol* **12,** 313–325 (2010). https://doi.org/10.1007/s10676-010-9227-5

Commented [MDM6]: Designed to be open, therefore not hiding anything and the opposite of privacy.

Commented [MDM7]: This is accomplished by a business holding information on customers (aka the citizens of a country) which such legislation is enacted.

Commented [MDM8]: Once information is released, it can be sold to countless others seeking to use the data for nefarious purposes.

Commented [MDM9]: If a large majority can agree on terms an international law can be enacted to further strengthen user data privacy, perhaps even making them human rights.

Commented [MDM10]: The problem with current user agreements is that they are very long, and no one reads them, so the user enters a binding contract blindly. The format also varies greatly across the globe.

Commented [MDM11]: Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

the bar and achieve the full potential of both the GDPR and Contractarianism by choosing the legislation that provides the most benefit to all, equally, and enacting that as the overarching law of the land.

Second, in Elizabeth Buchanan's "Considering the ethics of big data research: A case of Twitter and ISIS/ISIL," she reflects on issues with developing uses of big data and the ethical concerns they raise. The more information people post on the internet for others to see, the more difficult it is to maintain a sense of privacy. She details how we should repel use cases where huge data sets are used to fish for information in the name of national security or intelligence gathering. It is a slippery slope because the evidence is not driving you to someone, instead you are searching for something. One can agree if you are searching for something, you tend to find something, even if there is really nothing there. This is of concern because it can discriminate people. It is tempting to use this data because it is available in large quantities thanks to users posting freely online in various ways and various forms of content. Law enforcement and other regulating authorities may feel driven to this means by the increase of criminal capability via the same social networks the data can be mined from.

To apply Buchanan's central concern to the GDPR and the U.S. getting onboard with an equal solution there are still some concerns. Mainly, how to account for data that is made publicly accessible from being used in mass quantities, for purposes other than it was intended. I believe the GDPR would cause an undue burden on the processors and controllers as defined by the GDPR. I think the use would be based on an honor system, with law enforcement being more honest and being bound as a public authority from skimming the information without consent. Any other organization that chose to do so could potentially skim the information from social sites and unlikely to be pursued, a high gain low risk situation. Still the organization hosting the site would be responsible under the GDPR for the misuse of the information, though the penalty could be the minimum if they have taken every other precaution to avoid the misuse. It could not constitute a breach because it is posted publicly and starts to pose a grave concern when it is aggregated and queried against.

To apply Contractarian view to the case of the U.S. implementing a GDPR type of legislation, while addressing the concerns of Buchanan, would make individuals worse off in specific situations. Those situations mostly being the aggregation and query of data leading to discrimination towards people based on their social habits. While this would be prohibited by public officials under the GDPR, it does not mean it will not happen by public officials or any other non-regulated body. That discrimination could apply to any query run against the aggregate sum of data, not just terrorism related searches. The second is that it may cause some to be worse off because of the threat GDPR would bring for a situation they could not completely mitigate, like the skimming of publicly available data in huge swaths and its misuse.

In conclusion, the lag between the advancement of technology, uses of the internet and the ability of the legislature to keep up creates a gap where one is more mature than the other. The less mature law still stumbles and does not fully understand how to address the other with the necessary concerns in mind. The U.S. implementing a similar GDPR legislation will increase the commitments of a social contract that exists between everyone primarily through business and consumerism. Because the law is still a novice in a technologically advanced world there are some inequalities, but the U.S. is almost at GDPR equivalence, baselining legislation

Commented [MDM12]: Buchanan E (2017) Considering the ethics of big data research: A case of Twitter and ISIS/ISIL. PLoS ONE 12(12): e0187155. https://doi.org/10.1371/journal.pone.0187155

Commented [MDM13]: Data collected in large swaths across a large population can render tremendous power in manipulating people when applied to a plethora of metrics.

Commented [MDM14]: An example of potential misuse, instead of seeing what is there, a temptation to search for a result in the data and can be materialized.

Commented [MDM15]: This is something people do, not data.

Commented [MDM16]: A result of people not reading the user agreement and signing their rights away.

Commented [MDM17]: This is a huge undertaking; it is best to control the data has yet to be released. Everything that is already out there is in damage control mode.

Commented [MDM18]: Recent highlights in media show this varies from municipality to municipality.

Commented [MDM19]: Using tools to gather publicly facing information from social media sights in large quantities.

Commented [MDM20]: Use in any other situation other than what it was originally released for.

Commented [MDM21]: The resulting pool of individuals that return from a query of the data identify commonalities and potentially target.

Commented [MDM22]: A common known fact is typically every 18 months or so, computer processing speed doubles.

Commented [MDM23]: An implicit agreement among the members of a society to cooperate for social benefits.

throughout the U.S. will catch them up, and makes it easier for individuals to understand their rights and protections afforded by it.