Data Ownership

The rise of the internet has made it easy for massive amounts of data to be transferred and stored. While access to extensive data on various topics can be incredibly beneficial for advancing society by enabling thorough research, it also raises many ethical concerns. Perhaps most notable is the ability to gather and use personal information for secondary purposes not authorized by the data's owner. The question of the ethics of collection and secondary use of information without its owner's consent has been accelerated in the United States (US) due to the European Union (EU) enacting the General Data Protection Regulation (GDPR) in 2018. The GDPR contains many privacy protections the US currently lacks. For instance, the GDPR reinforces the right of individuals to own their data through stipulations such as requiring consent from the data owner before using it for secondary purposes (Palmer, 2019). Furthermore, the GDPR forces those collecting personal data to be more responsible by hiring data protection experts to oversee such operations. This analysis will explore how the US can use virtue in adopting regulations similar to the EU's GDPR because it will give individuals greater personal freedom and empower them to take control of their data.

Virtue ethics involves thorough consideration when decision-making, with the ultimate goal of making the best and most moral decisions for a given situation. Virtuous people are concerned with how their actions affect everyone around them, not just themselves. Learning to act virtuously involves embodying many attributes that do not necessarily come naturally, such as generosity, temperance, commitment, courage, and wisdom. As a result, a person must practice exemplifying these attributes if they wish to make the right decisions in a given situation. Virtue and its associated characteristics can be used by the US in creating legislation

similar to the GDPR, which would have produced better outcomes in the cases outlined by Michael Zimmer and Elizabeth Buchanan.

In his article “But the data is already public,” Zimmer (2010) discusses how the amount of information gathered on one entity can impact whether it can be used to identify individual subjects. The amalgamation of all a person’s characteristics and interests can be seen as a unique identifier because it is improbable that any two individuals have identical attributes. As a result, an observer is more likely to discover to whom the information in a study belongs if a large amount of data is collected, even if it has been anonymized by removing traditional personally identifiable information (PII).

Based on Danny Palmer’s (2019) description of the EU’s GDPR, the college social network study subjects could have been better protected if the US had implemented similar regulations. For instance, the researchers conducting the study received consent from everyone involved except for the students whose data they collected and released to the public in a compiled format (Zimmer, 2010). The GDPR empowers individuals and strengthens the idea that a person owns their information and should have control over it (Palmer, 2019). If the US had similar protections, the students would have needed to consent to their data being used, and the school would not have been able to hand over additional student information for secondary uses. Furthermore, the researchers could have been more virtuous by being more committed and gracious to the subject’s desires. While the study would have been less organic, the researchers obtaining consent from everyone except the student subject is disrespectful. In this way, the researchers seemed to lack compassion for the subjects and disregarded traditional research ethics. By being more gracious and committed to their subjects, the researchers could have likely gathered valuable information without betraying the subjects and risking their privacy. Actions

such as these would have demonstrated that the researchers weighed the risks and benefits to make the best decision for both students and researchers.

Legislation similar to the GDPR could have further protected the students' data because it requires that companies that collect user data have oversight from a data specialist (Palmer, 2019). Employing someone in the study who is familiar with data protection would have likely prevented the mistake of hiring research assistants who attended the studied school to collect data. This would have protected the information students were sharing only with other students and helped the research team achieve their goal of only using what was already available to anyone with an internet connection. While the researchers may have been well-intentioned, evidenced by their consideration of the subjects' privacy, they lacked wisdom by not realizing their shortcomings in data science expertise and having an external source more familiar with the matter as part of their research team. If they did so, the researchers may have been able to filter and release the data in a way that would put the subjects at much less risk of adverse outcomes while still reaping the benefits of the research. The researchers' excitement about the potential of advancing sociological understanding brought by this first-of-its-kind study may have made them hasty and proceed with releasing the results without sufficient care. If the researchers had greater temperance, they could have contained their enthusiasm and waited to release the data until the risks posed by the timeliness of the data were lessened. The data would probably have been just as valuable if released later to respect the subjects' privacy.

One of the central concepts that Buchanan (2017) discusses in "Considering the Ethics of Big Data Research: A Case of Twitter and ISIS/ISIL" is how the vast amount of data accessible on the internet has potentially changed how researchers should think about the ethics of research subjects. Researchers must obtain informed consent from all individuals involved in more

traditional studies, which is relatively straightforward because of their smaller size. However, the immense number of individuals studied in big data research makes it difficult to gain consent from all involved, and some researchers believe doing so is too impractical. Some argue that there should be a new classification of subjects known as data subjects, which are used to study groups rather than individuals. As a result, the information gathered should have little risk of hurting any one subject in the group. Because of this distinction, some say consent from all subjects is unnecessary because no single person is being scrutinized specifically.

However, these distinctions are insufficient to justify the collection of internet users' data without consent. First, the difficulty of obtaining consent is a poor excuse for violating others' privacy and using their data for unauthorized secondary purposes. Both the researchers and US lawmakers could use a more virtuous mindset to counteract such a notion. For example, the researchers in this study could have been more committed and gracious to their subjects by attempting to inform them about the potential risks and only studying those willing to take the risk, even if doing so requires considerable effort.

Additionally, collecting massive amounts of group data in a central location can be used to extrapolate detailed information about individuals within the group (Buchanan, 2017). Consequently, individuals might endure significant indirect harm from group data collection. This provides another reason why the US should adopt laws similar to the GDPR and allows US lawmakers to use virtuosity in helping solve these issues. As previously mentioned, the GDPR places great importance on individuality and the ability to own and control one's data (Palmer, 2019). This mindset aligns with many personal liberties that US citizens are already guaranteed, such as control over their property and protection from being forced to give up information. A recent poll by the Pew Research Center indicates that most Americans want more legislation

enacted to protect their data (Walker, 2022). US lawmakers could demonstrate commitment to their constituents by backing popular privacy laws reinforcing their rights and deeply-held beliefs of personal liberty. In supporting new regulations similar to the GDPR, US lawmakers must demonstrate courage and temperance by standing up to special interest groups that provide significant financial support to encourage lawmakers to oppose such privacy laws (Ng, 2022). US lawmakers could also demonstrate wisdom and commitment to their constituents by consulting experts who know more about technology's impacts on privacy. This would help lawmakers make informed decisions that benefit individuals rather than those serving their financial interests and corporations. Furthermore, lawmakers would show graciousness to their constituents, who voted them in, by honoring their desires and acting in their best interests instead of those who offer only financial support.

As demonstrated by the two research studies presented in this analysis, there are several ways that the GDPR could have protected the research subjects living in the US. The core principle providing the most benefit is that the GDPR focuses on individual ownership and empowers those who create data to control its storage and collection. As this principle closely aligns with long-standing American values of personal freedom and the ability of individuals to forge their own paths, the US should enact legislation that offers similar protections to its citizens as the GDPR does for the EU. However, some may object to this conclusion and argue that creating legislation in the US equivalent to the GDPR would severely inhibit sociology research, thus withholding the benefits that come from it. This concern is legitimate, but respecting individual freedoms is more important. Additionally, such regulations would not make research less effective than before the advent of the internet. Another argument critics of the GDPR may raise is similar laws could restrict US citizens' access to online resources and

services. For instance, many US-based websites were still unavailable in the EU a year after the GDPR was enacted because of compliance difficulties (Palmer, 2019). While this is true, a perceived lack of benefit from compliance may have been a more prominent driving factor since many EU-based companies are thriving after achieving compliance. As a result, the lack of motivation for companies to comply may be what restricts access, not the regulation itself.

References

Buchanan, E. (2017). Considering the ethics of big data research: A case of Twitter and ISIS/ISIL. *PloS One*, *12*(12). https://doi.org/10.1371/journal.pone.0187155

Ng, A. (2022, August 28). *Privacy bill triggers lobbying surge by data brokers*. Politico. https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958

Palmer, D. (2019, May 17). *What is GDPR? Everything you need to know about the new general data protection regulations*. ZDNET. https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Walker, K. (2022, April 25). *The urgent necessity of enacting a national privacy law*. Google. https://blog.google/outreach-initiatives/public-policy/the-urgent-necessity-of-enacting-a-national-privacy-law/

Zimmer, M. (2010). "But the data is already public": On the ethics of research in Facebook. *Ethics and Information Technology*, *12*(4), 313–325. https://doi.org/10.1007/s10676-010-9227-5