Cross-Cultural Analysis on the United States and the United Kingdom: The Most Feasible Methods to Improve Data Privacy Regulations in the United States

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Kavin Bapat

Fall 2023

On my Honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

In the 21st century, digital media infiltrates every aspect of society, ranging from politics and serious events all the way to lighthearted fun and entertainment. An aspect of digital media that has been significantly increasing in prevalence in recent years, globally, but particularly in the United States, is social media, with over 70% of Americans using some form of social media according to Pew Research. This number is only going to rise as social media companies begin developing more advanced and sophisticated algorithms designed to garner as much app-usage time as possible at the cost of the user's health.

In the United States, there are significantly looser data privacy laws and regulations to protect the user placed on large social media companies than in European countries. From Endpoint Protector, Christina Pop states, “Arguably the most significant difference in US legislation versus the EU is the lack of a comprehensive data privacy law that applies to all types of data and all US companies” (2023). The result of this is mounds of user data being unethically collected, used, stored, and sold to rake in billions of dollars for large media companies at the cost of the users' right to data privacy. From Statista, the US has the highest rate of companies collecting user data, at 73%, with the UK being all the way down at 43%. There is a gap in knowledge regarding the amount of data that is collected, and how exactly that data is used by social media companies. People are not aware of the potential negative effects that can result from a plethora of companies all farming and storing your data. These include third party companies having access to information you do not want them to, hackers accessing sensitive information that is improperly stored, etc. All from the Pew Research Center: approximately half of Americans believe that they do not have the ability to control who accesses their search history, most likely due to the prevalence of data privacy violations. Data breaches are not

uncommon, leaking data that has been collected and stored of hundreds of millions of users'. Nearly 30% of Americans have suffered a major form of identity theft. People feel as if their privacy is being violated online, and they are correct in feeling so.

While data privacy is not perfect in other countries, the United Kingdom is a great example of a successful country which has stricter data protection regulations. Through a cross-cultural lens, I will be analyzing the institution of data privacy in the United States and the United Kingdom to determine the most feasible solutions to alleviate the data privacy problems in the United States.

Problem Definition

Data privacy and personal information protection, while not a new concept, have become more of a concern in recent years thanks to the rapid development of social media. This is true not only in the United States but everywhere around the world. Fortunately, other countries have handled the issue of data privacy in different ways, some of which prove to be more successful at protecting users' data than the methods of the United States. The General Data Protection Regulation (GDPR) is a European Union law that dictates how personal data can be used, processed, stored, etc. The GDPR is known as one of the most strict data privacy protection laws in the world, corroborated by Lawne, a senior associate at Fieldfisher, stating, "The GDPR is one of the most comprehensive data protection laws in the world" (2022). One of the main pillars of the data privacy regulations in the European Union is how anonymization is treated. "While the GDPR applies a very high standard for "anonymisation", U.S. state laws consider "de-identified" data to be outside scope so long as the company has implemented certain technical and organisational measures" (Lawne, 2023). These strict regulations surrounding personal data result in a great discrepancy between the amount of data privacy violations in the European

Union versus in the United States. Identity theft is becoming one of the most prevalent crimes in the world, partly due to the rise in storing information digitally. The United States experienced about 13.5 million cases of identity theft in 2022, while France only experienced about 830,000 cases. Adjusting for population, the US still had a staggeringly high rate of identity theft cases in 2022 at over 4%, while France only had a rate of about 1.2% (Statista, 2022). The creation and implementation of the GDPR, a strict data privacy law, in Europe, at the same time companies in the United States are being sued for selling user data can be potentially attributed to many different reasons.

The most prominent reason for this discrepancy is the social and political environment in the different cultures. The culture one grows up in is a primary determining factor of what sets of values they have. In the United States, there is a culture of individualism, corporate rights, little government interference in the market, and fewer taxes for fewer social benefits; this leads to US citizens harboring values which results in less support for strict data privacy regulations. The GDPR is a clear display of government involvement in private corporations' business practices to protect the rights of the user, which goes against many 'American' values. In Europe, they prioritize a culture that supports its citizens, provides for the collective, and supports government intervention to protect individual well-being from rights-violating corporations. The Pew Research Center stated, "Nearly six-in-ten (58%) Americans believe it is more important for everyone to be free to pursue their life's goals without interference from the state…at least six-in-ten in Spain (67%), France (64%) and Germany (62%) and 55% in Britain say the state should ensure that nobody is in need…" (2011). These drastic differences in values are very clear contributing factors to how data privacy is handled in different cultures.

Hand-in-hand with the political and social cultures in the United States and the European Union is the education and awareness of the public on data privacy issues. More comprehensive data privacy regulations were able to be implemented in the European Union than in the United States partly thanks to awareness of the public. There is what seems to be a blind spot, or a lack of awareness, by the United States public, revolving around the violation of rights by corporations, "most people don't know how much of their activities are being tracked" (Wharton, 2019). Without the public being aware of how their data is being used, stored, collected, etc. by social media companies, there is very little incentive for the government to impose regulations on those companies to protect the data of the users. Simply knowing that their data is being collected and used is not enough for the public to push for stronger regulation for data privacy. The public needs to understand how the data they own being used solely for the profit of corporations harms themselves. This includes their data being susceptible to hackers in data breaches, their data being sold to predatory companies, and many more that should be known by the public. Feit notes, "It's a problem in my mind because the consumer doesn't necessarily know that their data is being sold to this third-party broker" (as cited in Wharton, 2019). Being more transparent with the US public about this information, as well as educating them on data privacy practices that are different and work better in other cultures, can be an effective way of bolstering support for stricter data privacy regulations in the US.

Although it is clear that there are significant issues in data privacy regulations in the United States, it is not apparent which issue is most feasibly alleviated. Rather than focus on the most effective solution, it is more productive to focus on the most feasibly implementable solution. We can pull a lot of information from the GDPR in the European Union and draw parallels to legislation in the United States, but there is no way for us to know exactly what the

effects will be as the US has a drastically different culture than the EU. Path dependency tells us that the way the media environment in both cultures was developed and how they evolved has great sway over the current state of the media environment in both cultures. This means that even if we employ, in the US, every method possible that improves data privacy in the EU, there is no guarantee that the solutions will be effective, let alone work at all. Despite the unknown, it is clear that there is a problem regarding data privacy in the United States, and there are steps that can be taken to improve the situation.

An invaluable source of information that I used when constructing my paper is Bijker's, "Differences in Risk Conception and Technological Culture". Bijker provides a comprehensive model for cross-cultural comparisons, using the United States and Netherlands as the two cultures. He thoroughly analyzes how cultural differences between the two countries result in different manifestations of the same sociotechnical system - flood prevention and coastal engineering. Furthermore, Bijker conducts research on the social and political reasons resulting in different values being held between the two countries, giving a holistic view of the sociotechnical system in question. Bijker highlights that the coastal engineer's in the Netherlands are not smarter or more advanced than in the US, but that there are prominent cultural differences with historical roots that result in different realizations of socio-technical systems in different areas. Rather than explain why the system in one country is superior to the same system in the other country, he discusses what is done well as well as the shortcomings in the coastal engineering industry in both countries. I utilize the framework in the Bijker piece to conduct a cross-cultural comparison between the United States and the United Kingdom covering the sociotechnical system of data privacy. Over the course of my research, it became clearer to me that examining how the current systems are formed is much more valuable than I previously

believed; understanding which methods have worked and which have failed is the best way to understand which methods will succeed today. The Bijker piece focuses heavily on the cultural, historical, and political reasons behind the current state of coastal engineering, giving a great template on successfully connecting culture and values to socio-technical systems for my research on data privacy. It was a very beneficial source in helping guide my research towards the right path, providing a framework for doing a cross-cultural comparison of a sociotechnical system.

Data Privacy in the UK

Data privacy regulations in the United Kingdom vary drastically from that in the United States in the sense that they are much more strict - having higher standards of data privacy to protect the individual. Although the UK left the European Union in 2020, the data privacy laws in the UK still emulate the GDPR in the EU, so the GDPR will be referred to when discussing data privacy regulations in the UK. There are many prominent elements in the GDPR that address data privacy issues which the US is lacking oversight in, one being the range of data which is protected under US data privacy legislation, as stated in the previously. Another major difference is the standards to which ‘data privacy’ as a concept is held, as the UK has a much higher threshold for adequate data privacy than the US. This is evident when looking at the higher standard for anonymization of the GDPR discussed earlier. Another major pillar of the GDPR is the control it gives EU citizens over their personal data, regardless of the fact that it is already in a company's database. If the data is no longer required for the reason it was given initially, then users can request that their data be deleted, and it must be deleted from the company database within 30 days. US data privacy legislation does not address many of these points in the GDPR. The main attributing factor for why the GDPR was successfully

implemented in the UK is the political, social, and economic culture. A table portraying the differences and similarities between the GDPR and data privacy legislation in various US states can be seen in Table 1 below.

	GDPR	CCPA	CPRA	VCDPA	CPA
Whose data is protected?					
Statutory term	Data subject	Consumer	Consumer	Consumer	Consumer
Defined as	Natural person in the EU	Natural person who is a CA resident	Natural person who is a CA resident	Natural person who is a VA resident	Individual who is a CO resident
What types of data are protected?					
Statutory term	Personal data	Personal information	Personal information	Personal data	Personal data
Defined as	Any information relating to an identified or identifiable natural person	Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household	Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household	Any information that is linked or reasonably linkable to an identified or identifiable natural person	Information that is linked or reasonably linkable to an identified or identifiable individual
Definition excludes de-identified data	GDPR uses the term "pseudonymized," rather than "de-identified." According to Recital 26, personal data that has undergone pseudonymization – which could be attributed to a natural person by the use of additional information – should be considered personal data	Yes, but see provisions regarding reidentification of de-identified information – Cal. Civ. Code §1798.148	Yes, but see provisions regarding reidentification of de-identified information. Cal. Civ. Code §1798.148. Moreover, the CPRA authorizes the attorney general to update the definition of "de-identified" – Cal. Civ. Code §l798.l85(a)	Yes, but special requirements apply to de-identified data. See Va. Code§ 59.1-581.	Yes, but special requirements apply to de-identified data. See Colo. Rev. Stat.§ 6-1-1307.
Definition excludes publicly available info	No	Yes	Yes	Yes	Yes
Definition excludes aggregate info	Not specified, but Recital 162 indicates that the GDPR applies to the processing of personal data for statistical purposes	Yes	Yes	Not specified	Not specified

Table 1: Detailed differences between the GDPR in the EU and data privacy legislation in US states (Bloomberg Law, 2023)

The UK has a drastically different culture than the US, prioritizing collectivism and the wellbeing of citizens over the rights of corporations. The overall social and political culture,

historically, in the US resulted in a society where the right of corporations to use user data trumps the right of privacy of the individual, despite highly valuing individualism. Because of this, there are very comprehensive and fully fleshed-out data privacy laws that protect the data of users in areas in which the US does not regulate or tend to side with the corporation over the individual. Corroborating my claim on cultural differences between the two countries, the Pew Research Center states, "Nearly six-in-ten (58%) Americans believe it is more important for everyone to be free to pursue their life's goals without interference from the state…at least ...55% in Britain say the state should ensure that nobody is in need…" (2011). Citizens in the UK being more favorable towards government interference allows much more action to be taken to protect the individual. A simple yet important aspect of data privacy legislation in the United Kingdom is that it is sweeping; everywhere in the UK follows the exact same guidelines. Because of this, and the values of collective wellbeing of the UK citizens, citizens are heavily motivated to ensure that their rights are adamantly protected.

Although there are many data privacy laws in the UK that would immediately improve the state of data privacy in the US if adopted, it will be exceedingly difficult to do so outright considering the current cultural and political climate of the US. This is why the best approach towards alleviating the issue of data privacy in the United States is to encourage the education of data privacy ethics and legislation, both in the US and abroad, and spread awareness of the harms that poor data privacy regulations can cause. The first step in enacting change is to garner support for the change, otherwise there will be no action. The values and culture of the EU enabled stringent data privacy regulations to be passed; this sort of culture must be created and worked towards in the US for there to be significant improvements in data protection. The most

sensible piece of legislation to advocate for is an overarching set of laws that apply blankety to every US citizen, which address data protection issues that have been ignored.

Results

It is clear, after conducting a cross-cultural analysis of data privacy regulations in the United States and the United Kingdom, that the most feasible path towards improving the state of data protection in the US is to increase education and awareness surrounding data collection by corporations and to unify data privacy regulations.

First and foremost, before attempting to implement legislation, it is paramount to increase education on what, when, and how much data is collected; otherwise, there will not be enough public support for the policies, and no meaningful change is likely to occur. The numbers of US citizens that do not truly understand the magnitude of their personal data that is being collected, stored, and sold are considerably high, as mentioned previously. This is because corporations are not required to make this information obvious to the user. Focusing on pushing for legislation to require corporations to provide this information clearer is not beneficial, however, because of the culture surrounding protecting the rights of corporations over the individual in the US. What follows is that the only logical course of action to increase education on data usage of corporations is a public awareness campaign. It will be beneficial to publicize and disseminate information on data privacy that would encourage people to worry about their personal information's protection. Discussing exactly how companies are handling user data and how frequent it is sold to other companies or used to deploy predatory advertisements would be greatly beneficial. Spreading information on cases where sensitive data was unethically used and highlighting the harm that followed, as well as data breaches where a higher standard of anonymity would have prevented major consequences would help bolster support for the

campaign If people do not know what data of theirs is being sold, it is impossible for them to understand the potential harms that could follow. Without understanding the potential harm of lax data privacy regulations, people will not push for stricter data privacy legislation. The culture in the United States is at a state where unless there is a significant increase in support for governmental regulations being imposed on corporations to protect user data privacy rights, such legislation will not be passed.

The reason it is important to focus on increasing education and awareness surrounding data privacy is because of how much influence that the culture and values of a citizenry has on its governing principles. The culture in the United States discourages supporting data privacy legislation that would involve the government placing restrictions on corporations. On the other hand, we can see how easily the government in the United Kingdom is willing to pass legislation to impose restrictions on corporations. Furthermore, the UK citizenry is very comfortable with supporting legislation that protects their personal data at the expense of corporate freedoms to do as they please with user data. Values are deeply rooted in a culture which stems from hundreds of years of historical context. Decisions that were made at the genesis of digital media, and even prior to that, have lasting effects on the state of data privacy legislation today. Although the introduction of digital media occurred at similar times in history in the United Kingdom and in the United States, they have followed significantly different paths in its use. In the first half of the 20th century, the UK created a public-funded network to provide quality, truthful, and unbiased information known as the British Broadcasting Corporation (BBC). At the same time, the government of the United States, for various reasons, decided it was important to keep private ownership of all major media corporations and keep its involvement in the media space at a minimum. This is a phenomenon known as path dependency. Because of this, even though we

know what works in the United Kingdom, we cannot expect the same results using the same methods in the United States. Also, this highlights the significance that culture and the values held highly by citizens has on socio-technical systems such as data privacy. Since the government imposing data privacy regulations on corporations is starkly against the typical values and culture of the US, it is important to dedicate time, energy, and resources towards shaping the overall culture of the US and the minds, values, and beliefs of its citizens.

In terms of legislation, the first step towards improving the data privacy rights of individuals should be unifying regulation involving data privacy. The current system of states having different sets of data privacy regulations makes it difficult for users to understand what data of theirs is vulnerable, and easier for corporations to find loopholes and sidestep data protection laws. A company can behave differently and treat users' data differently whether they are residents of Texas, where there are laxer data protection laws, versus residents of California, where they have much more stringent data protection laws. We have seen, when looking at the United Kingdom's data privacy legislation, sweeping regulations that are standardized across the entire country, which have proven to be effective. This is a preliminary basic step the US must take before introducing stricter and more comprehensive data privacy regulations. This can only be done through passing federal legislation, so the federal government cannot remain complacent and leave this issue up to the states. Without committing to standardizing data protection regulations across the US, people are left vulnerable in states with less proactive legislators. Implementing a federal piece of legislation that applies to every US citizen lays the groundwork to more easily implement more robust data protection laws in the future. If the piece of legislation is not controversial, complex, or too harsh on corporations initially, then it will be

more feasibly passed into law, beginning the process of implementing strong data protection laws.

There are many data privacy regulations that can be adopted from the GDPR, including the user's "right to be forgotten", higher standard of anonymization, wider scope of data protection, and many more prominent laws. Until the data privacy guidelines are regulated across the entire United States, it is futile to attempt to improve the state of data privacy. Before any attempts at standardizing data privacy regulations in the United States, there must be a significant shift in culture in the US and values held by its citizens. To most feasibly improve the state of data privacy protection in the US, education and awareness must be increased, and data privacy laws must be standardized across the entire country.

Conclusion

The importance of strong data privacy regulations in the United States is currently overlooked, as the US is far behind other developed countries. Looking at the United Kingdom, we can see that it is possible for stricter regulations involving data privacy to be popular and successful. Looking at related research done on data privacy in the US, most sources discuss what the effective solutions could be by looking at what works in other countries. This research, oftentimes, ignores the cultural and political nuances of the US, which are very important to observe when determining which solutions make sense to pursue. I hope that my research can act as a stepping stone for others to look at this issue from a cultural perspective. I believe analyzing the issue through this lens will prove to be much more effective at garnering real change and improvements, as you cannot look at policies in a vacuum. After conducting a thorough comparison of the institution of data privacy in both countries, it became clear that the state of data privacy protections for citizens in the United States, although not very robust currently, has

multiple reasonable avenues to pursue to improve it. The first of which being increasing education and awareness on data protection regulations abroad, and the amount of data being collected and how it is being used. We know that many Americans do not truly understand the importance of proper data protection regulations and the extent to which their data is being used. The culture in the US is deeply rooted and works against increasing government interference in private corporations, so increasing awareness to foster a shift in public opinion is a necessary first step. When looking at the United Kingdom, we see the success in having standardized legislation across the entire country. The differing privacy laws between the 50 states can result in American citizens' data being at risk just for living in the wrong state. Standardizing regulations on data protection across the board lays a strong foundation for implementing more stringent and robust legislation in the future. There are many other potential avenues to pursue to strengthen data protection in the United States, but increasing education and standardizing regulations are the important options to focus on to have the best odds of success.

References

Auxier, B. (2019, November 15). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bijker, W. E. (2007). American and Dutch Coastal Engineering: Differences in Risk Conception and Differences in Technological Culture. Social Studies of Science, 37(1), 143-151. https://doi.org/10.1177/0306312706069437

Comparison charts: U.S. state vs. EU Data Privacy Laws. Bloomberg Law. (2023, July 11). https://pro.bloomberglaw.com/brief/privacy-laws-us-vs-eu-gdpr/

Knowledge at Wharton Staff. (2019, October 28). *Your data is shared and sold... what's being done about it?* Knowledge at Wharton. https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/

Lawne, R. (2023, March 2). *GDPR vs U.S. state privacy laws: How do they measure up?*. Fieldfisher. https://www.fieldfisher.com/en/insights/gdpr-vs-u-s-state-privacy-laws-how-do-they-measure#:~:text=Scope.,a%20narrower%20range%20of%20organisations

Pew Research Center. (2011, November 17). *The American-Western European Values Gap*. Pew Research Center's Global Attitudes Project. https://www.pewresearch.org/global/2011/11/17/the-american-western-european-values-gap/

Pew Research Center. (2021, April 7). *Social Media Fact Sheet*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/fact-sheet/social-media/

Pop, C. (2023, November 22). *EU vs US: What are the Differences Between Their Data Privacy Laws?*. Endpoint Protector Blog. https://www.endpointprotector.com/blog/eu-vs-us-what-are-the-differences-between-their-data-privacy-laws/

Statista. (2023a, May 15). *Share of companies worldwide that collect personal data in 2021, by data subject region*. https://www.statista.com/statistics/1172965/firms-collecting-personal-data/

Statista. (2023b, June 7). *Number of adults in selected countries who have ever fallen victim to identity theft in 2022*.

https://www.statista.com/statistics/1389318/identity-theft-victims-in-selected-countries/#:~:text=In%202022%2C%20India%20ranked%20first,encountered%20identity%20theft%20that%20year.