Barriers Facing Consumer Data Privacy Legislation 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

Claire Moon Cofield

Spring 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

MC Forelle, Department of Engineering and Society

Introduction

In 2018, the United States Senate Judiciary Committee conducted hearings related to the Facebook-Cambridge Analytica data scandal, after it was revealed that Cambridge Analytica – a consulting company that specialized in using data science to advise political campaigns – had been using psychological data acquired through Facebook and an app called "This Is Your Digital Life" to carry out political agendas (Meredith, 2018). At these hearings, Facebook CEO Mark Zuckerberg revealed in his testimony that only "some of" the available data that is stored and shared about users is collected "with people's permission" (Watson, 2018). This means that a lot of the data collected on users is gathered without their explicit knowledge or consent. Less than 300,000 people downloaded the "This Is Your Digital Life" app, which was designed to build psychological profiles of users. However, due to the app's ability to connect with Facebook, which collects vast amounts of personal data on users and the people they interact with online, the personal and psychological data of over 87 million people was harvested by Cambridge Analytica (Meredith, 2018). Due to the incredibly wide scope of this collection, many of the people affected would not even know their personal data had been accessed.

The personal data that Cambridge Analytica and its predecessor were able to obtain is estimated to have been used to influence over 100 campaigns in more than 30 countries world-wide (Horwitz, 2018). Of these over 87 million people, more than 70 million of them were from the United States (US) (Nieva, 2018). This scandal and others like it show that private companies - even those that a user has chosen to not interact with, such as was the case for the vast majority of people affected in this scandal - are able to collect, analyze, monetize, and distribute huge amounts of personal information about US citizens, including information that these people did

not consent to sharing. Due to the lack of any comprehensive data privacy protection laws, companies are allowed to do this relatively unchecked in the US (Klosowski, 2021).

Many Americans value their right to privacy, but there are currently no national laws in place to protect this privacy when it comes to personal data. Additionally, the vast amounts of data collected about a given person can be used to hurt them in numerous ways, such as predatory insurance rates and identity theft (Klosowski, 2021). In order to keep US citizens safe from predatory data practices, the United States Government (USG) would need to pass data privacy legislation and regulations. However, there are many barriers to the passage of such regulations at the national level. Analogous governments, such as those of the European Union (EU) and individual states in the US, which do not face these same barriers, have been able to successfully pass laws that protect consumer data privacy, so we know it is possible.

In this paper, I will argue that the lobbyist culture of the USG incentivizes politicians to cater to private companies over constituents' interest, which has hampered the passage of national consumer data privacy protection policies in the US, causing the US to fall far behind its contemporary the EU on this issue. To illustrate this point, I will first conduct a review of current literature in the field, to establish why data privacy is an issue that needs to be addressed at the national level in the US and why this has not been done already. In this review, I will examine attempts that have been made in the US, discussing why and how they have fallen short of the goal and comparing them to the much more successful attempts that have been made in the EU. I compare the US - a country - to the EU - a union of several different countries coming together - rather than comparing it to any individual country, because while the EU is able to contend with the US in terms of geographical size, population, and economic influence, none of the individual countries within it would be able to, partially due to the sheer size of the US alone (*China vs.*

E.U. vs U.S. vs. Japan, n.d.). Then, I will gather data from primary sources measuring the progression of bills through Congress and the overall attitudes of American adults, and secondary sources that offer professional analyses of these data. I combine the information provided in these sources and analyze them myself, drawing comparisons between attempts to pass data privacy legislation in the US and analogous efforts in the EU to see why such protections are dropped by governing bodies in the US but passed by those in the EU. In the end, I find that the main cause for the differences seems to be the financial structures of the lobbying and elections processes in these two different governmental bodies, which incentivize policy makers in the USG to prioritize private companies' interests. I conclude that this is the primary reason why the US does not have comprehensive laws for protecting citizens' privacy when it comes to their data and other digital information, and give suggestions for further research and ways to address this issue.

Literature Review

Many US citizens are opposed on principle to the large scale of data collected about them. This can be seen in how the American public generally reacted with anger and outrage to scandals such as the Snowden, Equifax, and Cambridge Analytica scandals, where it was revealed that their privacy had been compromised (Bellamy, 2023). Privacy allows for increased freedom and autonomy, both of which are ideals that Americans tend to highly value (Solove, 2021). Many people feel that the lack of control they have over their personal data is an affront to their dignity and sense of agency (O'Connor, 2018). Due to this morals-based opposition, approximately 70% of US adults feel the federal government should set standards for how companies collect and process personal data online ("Data privacy in America", 2022).

However, even consumers who are not opposed to large scale data collection on principle alone should be wary of it. Lax data privacy regulations can harm consumers. Data collected on consumers can often be, and has famously and widely been, used against them (Kerry, 2018). The large scale collection and sale of consumer data allows for companies to profit off of the consumer, to the detriment of the consumer. This can be done through methods like raising interest rates and displaying targeted ads. Additionally, the large-scale collection requires data to be stored and transmitted, which gives attackers access points to steal this data (Klosowski, 2021). This increased attack vector has left an increased opportunity for identity theft and made it so that technological identity theft impacts more areas of life (O'Connor, 2018).

Due to these many avenues of harm that can befall citizens from data privacy invasion, many governments have passed laws, restrictions, and other regulations protecting consumer data privacy. The most notable example of governmental protection of consumer data privacy is the EU's General Data Protection Regulation (GDPR). The GDPR is a comprehensive data privacy protection law that applies to all companies that operate in the EU and service EU citizens, not just to companies located in the EU. As many companies are international, this offers much more protection to EU citizens. The GDPR covers a range of topics, but its main purpose is to minimize the amount of data collected on citizens. Under the GDPR, companies face heavy fees and other consequences for collecting unnecessary data, not securing their data storage, and not being transparent with users about what data they are collecting (Wolford, 2018). The strong protections offered by the GDPR show that it is possible to pass laws that take some effective steps to protect consumer data privacy.

However, there is no comprehensive national set of data privacy laws and enforced regulations in the US. Instead, there are several different narrow areas of regulation for distinct

subsets of personal data, and a few states that have passed overall data protection laws. Some examples of these narrowly-applicable regulations include the Video Privacy Protection Act (VPPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Family Educational Rights and Privacy Act (FERPA). VPPA only regulates the release of data pertaining to Video Home System (VHS) rental records, which most Americans no longer use. HIPAA only regulates data that is related to health or healthcare data and is collected by officially licensed practitioners. And FERPA only regulates access to student education records collected and stored by schools. These specific domains of data privacy are all kept distinct from each other and do not apply to the vast majority of consumer data that is generated on a daily basis (Klosowski, 2021). The overall data protection laws that have been passed by certain states are generally much more comprehensive and thorough than these patchwork national standards, however only five states (California, Colorado, Connecticut, Utah, and Virginia) have passed such laws (Bellamy, 2023).

Many attempts to pass comprehensive legislation for data protection in the US at the national level have been made, but none have made it through Congress, with many losing momentum and becoming completely discarded or outdated (O'Connor, 2018). The most notable such attempt was the American Data Privacy Protection Act (ADPPA), which would have covered all data that could be reasonably assumed as linkable to a specific individual. The ADPPA prohibits the collection, transfer, use, and long-term storage of data beyond what is necessary and proportionate for the services the user has requested or consented to. It also includes protections for minors, small businesses, medium businesses, and groups that may be discriminated against based on protected civil rights categories (Gaffney et al., 2022). It was introduced in the 117th Congress (2021-2022), but it did not progress from the House of

Representatives and is now on a scheduling backburner (H.R.8152). This lack of national laws means that by default the US expects the responsibility to fall on individuals.

The conceptual framework I will be analyzing this issue through is Pinch and Bijker's framework the Social Construction of Technology (SCOT). Many analysts have examined the differences between privacy laws in the US and EU, but none have done so through this lens. SCOT argues that science is socially constructed - based on culture, not objective facts - and technology is both a body of knowledge and a social system. Consequently, both science and technology are socially constructed and socially understood. This means that the issues and meanings of an object are determined by the relevant social groups, which can affect its subsequent modifications, redesigns, development, and usage (Pinch & Bijker, 1984). The framework also defines relevant social groups as "organized or unorganized groups of individuals… that all… share the same set of meanings, attached to a specific [science or technology]" (Pinch & Bijker, 1984, p. 414). I will use this framework to analyze the relevant social groups that are represented in the current literature surrounding issues of consumer data privacy in the US compared to those of the EU. For each group, I will examine their social constructions and conceptualizations of the technologies in question.

Methods

To conduct my analysis, I look at an array of both primary and secondary sources. For primary sources, I use multiple different datasets from the Pew Research Lab - known for its polls of the US population - to analyze the stance most US adults have on various privacy issues and their related policies. I also use Congress's website, which tracks all official actions taken on each proposed bill, as well as any sponsors, co-sponsors, or committees that are interested in the bill. For secondary sources, I use journalistic, humanitarian, and thinktank pieces on how privacy

regulations have been developed and implemented in the US and the EU, to examine the similarities and differences between the two regions. In my review of this literature, I examine the political policies in place in the US and other countries with similar technological developments, with a particular focus on how the social issues brought up in these political discussions are constructed within the culture of the current US.

Analysis

As I established in my Literature Review, the current solution to the problem of the US's lack of consumer data privacy protection laws is to pass the duty of all the risk assessment and protection onto the individuals, but this is not a viable solution long-term. Individual responsibility for informed consent is simply not practical in the modern world. Individuals might have been able to keep up with all of the privacy policies they were beholden to during the start of the Internet age, but as time has gone on, privacy policies have gotten exponentially longer, more complicated, and harder to read (Wagner, 2022). Many privacy policies are worded such that the average consumer is not even able to read and understand them (Savage, 2018). Even if these policies were understandable, the sheer number of policies a user must interact with causes a cognitive overload if a consumer genuinely tries to keep up with all of the privacy policies for each of their devices, the networks they connect those devices to, the software they use on those devices, and the businesses they interact with - not to mention having to keep up with policy updates as well (Quach et al., 2022). Additionally, even if a consumer were to be able to keep up with this barrage of policies, many companies do not allow for users to opt-out of the policies they find invasive (Solove, 2021). Data collection is largely automated, and thus does not allow for a consumer to voice their withholding of consent and have that be respected

(Kerry, 2018). Since individual responsibility is not a viable solution, a better option would be corporate responsibility, which depends on governmental laws and regulations.

It can be difficult for governments to pass such privacy-protecting regulations, partially due to the fact that consumer data collection and distribution can be such nebulous, fast-changing topics to begin with. Definitions and boundaries are hard to pin down as new advancements are constantly being made which completely change the fields (Sherman, 2021). Due to the speed at which laws and governmental regulations get passed, compared to the speed at which technological advancements are developed and deployed, many regulations are out of date or no longer applicable by the time they are issued (Malan, 2018). The amount of digital information collected is growing exponentially every year, and regulatory systems have largely not been able to keep up with this explosion (Kerry, 2018).

However, blaming the lack of digital privacy protection laws in the US on aspects inherent to the technology involved ignores the fact that other governments have been able to pass such laws while working with the same technologies The reason the USG does not have comprehensive digital privacy laws thus has to do with how the USG's constructions of technology policy differs from analogous governments' constructions. This is why applying the SCOT framework to this issue is helpful. Within the culture of the USG, the issues of digital privacy technology, regulation, and protection are all deeply important to one relevant social group: data brokers. These are companies that collect, trade, and/or store data on individuals. Data brokerage companies make a lot of money from these activities. The structure of the US Congress, which allows companies a lot of access to lawmakers through lobbying, affords these data brokers in particular a high degree of power and influence (Klosowski, 2021).

A large part of the reason it has been so hard to pass digital privacy protection laws in the US is because of industry pushback for financial reasons. Due to the lucrative nature of data brokerage, many companies do not want to limit it and have a strong economic incentive to hamper any governmental attempts at regulation (Klosowski, 2021). In addition to not wanting to miss out on the profits they can make from collecting and selling data, companies do not want to spend the time, resources, and manpower that are required in order to ensure compliance to new laws (Castro & Johnson, 2019). The vested interest the private sector has in hindering governments from passing regulations on this issue can be seen in how heavily companies advocate against such policies through lobbying. Amazon and other well-known tech companies spend a lot of money and resources on sending lobbyists to work against privacy protection laws when they are being deliberated on in the US at a national level (Dastin et al., 2021). In fact, in 2018, blocking US privacy legislation and regulation that would affect the Alexa devices was one of Amazon's major goals for the year (Dastin et al., 2021). In 2020 alone, data brokers spent around $25 million on such lobbying efforts (The Markup, 2021).

The structure of the political systems in the USG incentivizes politicians to prioritize these companies' desires above those of the general public or constituent individuals. In the EU, politicians are sponsored by their parties, and political parties are sponsored by the parliament itself, with each registered party getting a small baseline amount of a shared pot of funding, and the rest of the funding being distributed proportionally based on the number of currently serving elected members of parliament that each party has (*Funding European Political Parties*, 2023). However, in the US, politicians must fund their own campaigns. The winner-take-all systems and the need to fund re/election campaigns combine to require politicians to spend a considerable amount of time and effort trying to secure funding, and lobbyist organizations are often an easy

source to get this funding from In the US, it is typical for companies to fund electoral campaigns for various politicians, whereas in the EU such conduct is seen as unethical (Mahoney, 2009). In fact, in the EU, members of parliament are expressly forbidden from engaging in lobbying related to current political decisions and from entering into any agreements that might give the appearance of bribery or external influence through direct or indirect financial gain (European Parliament Committee on the Conduct of Members, 2017). On the other hand, US politicians' prioritization of campaign financing means that, compared to the EU, in the US a lobbyist organization's influence on policy is much more closely related to how much money they can provide their politicians with, leading to people-led organizations having less power. The consequences of this are that in the US, success rates for company lobbying campaigns are around 71% while those for citizens' rights groups is only around 39%. Meanwhile in the EU, companies succeed around 59% of the time while citizens' rights groups do around 62% of the time (Mahoney, 2009).

People may argue that the reason the US doesn't have national protection laws like the EU does is due to the cultural differences between the two, with the EU placing more trust in their governmental systems and the US placing more trust in their companies and corporations. This cultural difference does exist. Approximately 60% of Americans trust businesses while only 41% trust the government (McCarthy, 2015). And, in a more specific area of trust, only 49% of Americans trust the USG to protect their data, while 60% trust the companies they do business with to do this (Olmstead & Smith, 2017). However, arguing that this cultural difference has more impact than lobbying and financial incentives ignores a few key facts. Firstly, there is a long history of cooperation and information-sharing between the USG and private companies who hold Americans' data, so protecting consumers against companies will also help protect

them against the government abusing their data, as was seen in the Snowden scandal of 2013 (Beens, 2020). Secondly, and more to the point, the vast majority of data collected on individuals these days is collected, held, and aggregated by private companies, not governmental organizations (Dastin et al., 2021). Thus, although the degree to which US citizens trust their government is significantly lower than the degree to which EU citizens trust their government, this cultural difference is not enough to justify the USG's lack of any comprehensive legislation to protect consumer data privacy. Indeed, by taking action to pass legislation that protects US consumers, the USG may even be able to increase the trust its people have in it.

Conclusion

Americans tend to value privacy and protection. The lack of national data privacy laws in the US undermines both of these values, and causes harm to US citizens. The main reasons for the lack of such protections is due to lobbying and the deep impact that financial incentives have on elections and politicians, as companies do not want to lose access to the lucrative yet exploitative market that big data affords them. The political forces at issue here provide an area that is ripe for future exploration. I hope this paper can serve as a contribution to further research in key areas of US privacy policies and legislative approaches. One avenue future research could take is looking into how much influence the American people feel lobbyists and the market should have on laws that protect citizens' wellbeing.

While Americans are currently vulnerable to data privacy violations in many ways, this does not have to remain true. If national-level representatives read research such as that conducted in this paper, they could be encouraged to pass laws that protect consumer privacy, for the good of their constituents, regardless of the desires of lobbyists. Additionally, if more Americans become aware of the way that the financial systems embedded in US politics can

work against citizens' welfare, they might be encouraged to challenge and change the design of political systems that give more power to companies than to people.

References

Beens, R. E. G. (2020, July 29). *Council post: The privacy mindset of the EU vs. The US.* Forbes; Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/07/29/the-privacy-mindset-of-the-eu-vs-the-us/

Bellamy, F. D. (2023, January 12). U.S. data privacy laws to enter new era in 2023. *Reuters*. https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/

Castro, D., & Johnson, A. (2019, December 13). *Why can't congress pass federal data privacy legislation? Blame California*. ITIF; Information Technology & Innovation Foundation. https://itif.org/publications/2019/12/13/why-cant-congress-pass-federal-data-privacy-legislation-blame-california/

China vs. E.U. vs U.S. vs. Japan: Population and GDP comparison. (n.d.). Worldometers; Worldometer. Retrieved April 6, 2023, from https://www.worldometers.info/population/china-eu-usa-japan-comparison/

Dastin, J., Kirkham, C., & Karla, A. (2021, November 19). *The Amazon lobbyists who kill U.S. consumer privacy protections.* Reuters. https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/

Data privacy in America. (2022, February 3). Senate Republican Policy Committee. https://www.rpc.senate.gov/policy-papers/data-privacy-in-america

European Parliament Committee on the Conduct of Members. (2017). *Code of Conduct for members of the European parliament with respect to financial interests and conflicts of interest* (Code of Conduct Annex I). European Parliament.

http://www.europarl.europa.eu/pdf/meps/Code%20of%20Conduct_01-2017_EN.pdf

Funding European political parties. (2023, April 19). European Parliament Contracts and Grants Website; European Parliament. https://www.europarl.europa.eu/contracts-and-grants/en/political-parties-and-foundations/european-political-parties

Gaffney, J. M., Linebaugh, C. D., & Holmes, E. N. (2022). *Overview of the American Data Privacy and Protection Act, H.R. 8152* (No. 10776; Legal Sidebar, pp. 1–6). Congressional Research Service. https://crsreports.congress.gov/product/pdf/LSB/LSB10776

Horwitz, J. (2018, April 5). *Outside the US, the Philippines saw the most Facebook user data go to Cambridge Analytica*. Quartz. https://qz.com/1245355/outside-us-philippines-saw-most-facebook-user-data-go-to-cambridge-analytica

H.R.8152 - 117th Congress (2021-2022): American Data Privacy and Protection Act. (2022, December 30). https://www.congress.gov/bill/117th-congress/house-bill/8152

Kerry, C. (2018, July 12). *Why protecting privacy is a losing game today—And how to change the game*. Brookings; Brookings Institute. https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

Klosowski, T. (2021, September 6). The state of consumer data privacy laws in the US (And why it matters). *Wirecutter: Reviews for the Real World*. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Mahoney, C. (2009, June 4). *Why lobbying in America is different*. Politico; Politico. https://www.politico.eu/article/why-lobbying-in-america-is-different/

Malan, D. (2018, June 21). Technology is changing faster than regulators can keep up—Here's how to close the gap. *World Economic Forum*.

https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/

The Markup. (2021, April 2). The data broker industry is spending big bucks lobbying Congress. *The Next Web; The Financial Times*. https://thenextweb.com/news/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress-syndication

McCarthy, N. (2015, February 5). *Americans trust business more than government [infographic]*. Forbes*; Forbes*. https://www.forbes.com/sites/niallmccarthy/2015/02/05/americans-trust-business-more-than-government-infographic/

Meredith, S. (2018, April 10). *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*. CNBC. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Nieva, R. (2018, June 13). *Most Facebook users hit by Cambridge Analytica scandal are Californians*. CNET. https://www.cnet.com/tech/tech-industry/most-facebook-users-hit-by-cambridge-analytica-scandal-are-californians/

O'Connor, N. (2018, January 30). *Reforming the U.S. Approach to data protection and privacy.* Council on Foreign Relations. https://www.cfr.org/report/reforming-us-approach-data-protection

Olmstead, K., & Smith, A. (2017, January 26). Americans and cybersecurity. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Pinch, T., & Bijker, W. (1984). The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science, 14*, 399 - 441.

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Savage, L. (2018, September 14). Why we must remember where informed consent comes from. IAPP; International Association of Privacy Professionals. https://iapp.org/news/a/why-we-must-remember-where-informed-consent-comes-from/

Sherman, J. (2021, April 8). *Federal privacy rules must get "data broker" definitions right*. Lawfare; The Lawfare Institute in cooperation with Brookings. https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right

Solove, D. (2021, December 1). *Why privacy matters: An interview with Neil Richards*. Teach Privacy. https://teachprivacy.com/why-privacy-matters-an-interview-with-neil-richards/

Wagner, I. (2022). *Privacy policies across the ages: Content and readability of privacy policies 1996-2021*. https://doi.org/10.48550/ARXIV.2201.08739

Watson, C. (2018, April 11). The key moments from Mark Zuckerberg's testimony to Congress. *The Guardian*. https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments

Wolford, B. (2018, November 7). *What is GDPR, the EU's new data protection law?* GDPR; Horizon 2020 Framework Programme of the European Union. https://gdpr.eu/what-is-gdpr/