The Struggle over Digital Privacy in the United States

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Declan Brady

May 8, 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.

The Struggle over Digital Privacy in the United States

Digital innovation raises problems of personal privacy. In the U.S., how are privacy advocates and data collectors competing to influence digital data privacy standards? The volume of data collected online doubles about every 40 months (McAfee et al., 2012). A review of privacy advocacies and large technology companies reveals their strategies. Privacy advocacies include American Civil Liberties Union (ACLU), Center for Democracy and Technology (CDT), Electronic Frontiers Foundation (EFF), and Electronic Privacy Information Center (EPIC). Large data collectors like Meta and Google oppose privacy regulation, and create their own advocacies like the Future of Privacy Forum (FPF), and the Internet Association (Romm, 2019). In the United States, both privacy advocates and data collectors target the federal government and individual consumers. Privacy advocates demand stricter regulations and publicize data collection and usage. Data collectors lobby legislatures to prevent regulation, arguing that the responsibility lies with the user.

Review of Research

Researchers have studied privacy rights, consumers' perceptions of privacy, and consumer trust. According to Auxier et al. (2019), "81% of the public say that the potential risks they face because of data collection by companies outweigh the benefits." Many Americans distrust data collectors. Gak et al. (2022) note that personal data "can expose vulnerabilities." Data collectors promote "engagement that can facilitate unhealthy behavior" (Gak et al., 2022).

Studies attempt to understand how data affects individuals. It is also important to understand how this environment has been created. Literature into how interest groups influence privacy laws focuses on the European Union. Christou & Rashid (2021) find "lobbying by

industry together with CSOs led to a watered-down final agreement that ultimately provided more ambiguity and less stringent obligations." CSOs in Europe are similar to advocacies in the United States. They compete against large companies to influence public policy. The research investigates the European Union's General Data Protection Regulation (GDPR). Atikcan & Chalmers (2019) found that tech companies had much more influence. The resultant GDPR is much better than anything that currently exists in the United States, but CSOs want to expand regulation (Christou & Rashid, 2021). "In the EU, there has been a longstanding debate about whether U.S. law provides sufficient protections for personal information" (Schwartz & Peifer, 2017). The research surrounding EU law is extensive, as the GDPR passed in 2016. In the United States, there is still a lack of understanding of how privacy laws are influenced.

Research has been done into solutions for data privacy outside of legislation. This can be done by anonymizing data. Bayardo & Agrawal (2005) developed a methodology to perform k anonymization, removing linking data between data sets. This algorithm de-identifies data, making it impossible to link data points together across data sets. "Imagine for instance a represented individual who is the only male born in 1920 living in some sparsely populated area. This individual's age, gender, and zip code could be joined with a voter registry from the area to obtain his name, revealing his medical history" (Bayardo & Agrawal, 2005). Large companies such as Meta fund similar work, advocating for the development of stronger protocols to protect data once it is collected (Movahedi et al., 2021). These studies often deflect the responsibility of data privacy from legislation to implementation. They rely on users to trust how their data is stored and maintained, something that users are wary of (Auxier et al., 2020).

An Introduction to Data Privacy Policy in the United States

Data privacy policy is a critical issue in the United States. The collection, use, and distribution of personal data is widespread. The United States has federal legal frameworks that govern data privacy. These laws aim to grant individuals control over their personal information, and ensure data collecting and processing organizations are held accountable for its use. This is a point of contention; large corporations believe they are sufficient, while privacy advocates disagree. The Federal Trade Commission (FTC) is responsible for data privacy. The Electronic Privacy Information Center contends, "there are significant limitations in the patchwork of data protection authorities at the FTC's disposal" (EPIC, 2021). The Center for Democracy and Technology (CDT) agrees "Congress is increasingly out of touch with the privacy needs of Americans" (Null, 2023).

The United States does not have a single federal law that regulates consumer data privacy; it has a patchwork of federal and state laws instead. The most important federal law that regulates data privacy is the Privacy Act of 1974. This law regulates the collection, use, and distribution of personal data by federal agencies. It is held in high regard by the Electronic Frontier Foundation, who use the "Privacy Act's strict mandates of accountability, transparency, and privacy" in an argument against expanded data collection (EFF, 2020). The regulations notably do not extend privacy protection beyond the government's collection. Additions have been amended, but the majority of the legislation was written in 1974. This half century old piece of legislation is not enough to regulate the massive amounts of data collected today.

Other federal laws also address specific areas of data privacy, including the Health Insurance Portability and Accountability Act (HIPAA), which regulates the privacy of medical records; the Gramm-Leach-Bliley Act (GLBA), which regulates the privacy of financial

information; and the Children's Online Privacy Protection Act (COPPA), which regulates the privacy of children's personal information online. The most recently enacted was the GLBA, passed in 1999. Concerningly, no major data privacy legislation has been enacted in this millennium.

States have enacted their own data privacy laws. The most comprehensive of these is the California Consumer Privacy Act (CCPA, 2018). The CCPA gives California residents the right to know what data is collected, request that it be deleted, and opt out of the sale of their personal data. Lobbying efforts by large corporations is evident, as all initiative to exercise these rights must be taken by the consumer. Meta claims “In the Privacy Policy, we explain how we collect, use, share, retain and transfer information. We also let you know your rights” (Meta, 2023). Later in the policy, they deflect this responsibility, “You may also have other privacy rights under applicable laws” (Meta, 2023). They acknowledge that rights may exist, but don’t direct consumers to them.

Corporate Privacy Interpretation

Data-collecting corporations such as Google and Meta lobby the United States federal government to prevent consumer privacy regulations, asserting the responsibility of privacy is on the user.

User data is most used for targeted advertising, as this drives revenue for many technology companies. “Data-driven advertising is highly profitable, especially for the largest platforms such as Facebook and Google” (Crain & Nadler, 2019). Inherently, advertising is profit driven, data is a means to drive profit. Platforms profit by collecting and selling as much data as possible. It is not in their interest to protect user privacy. Crain and Nadler (2019) investigated

how data is used in political advertisements and “manipulation campaigns” in which data-guided advertising is used “to target vulnerabilities.” In such campaigns, advertisers apply user data to misinform and manipulate people. The responsibility falls back onto platforms that supply the data, and it is clear they understand the power they have. According to Crain and Nadler (2019): “Ad platforms continue to invest, expand, and fortify political buffers through lobbying.”

Google and Meta lobby against consumer privacy regulations. According to OpenSecrets (2022), Alphabet Inc, the parent company of Google, lobbied on consumer product safety in 2022. In 22 of the 24 listed instances “Privacy and data security issues” are listed as the purpose of the lobbying. Alphabet contributed $2,720,000 just to lobbying against bills “H.R.8152 /S.3195 - American Data Privacy and Protection Act / Consumer Online Privacy Rights Act S. 3663, the Kids Online Safety Act,” among others (OpenSecrets, 2022). Meta, formerly known as Facebook, lobbied in the computers and information technology category fifty times in 2022 (OpenSecrets, 2022). Consumer privacy protections impede revenue.

Large companies also create their own advocacies to promote their agendas. The Future of Privacy Forum (FPF) is one such organization. They are backed by virtually every large data collection firm, from Google, to Netflix, AT&T, and beyond (FPF, 2023a). The group works tightly with the federal government and “convenes experts to foster collaboration and promote insightful research on data protection that supports the utility of data” (FPF, 2023b). The priority is to support the utility of data, with privacy as a bonus. This is made clear in their four part belief statement:

1. Technological innovation and new uses of data can help solve big societal problems and improve lives.
2. Technological innovation must be accompanied by fresh privacy thinking.

3. It is possible to build a world where technological innovation and privacy can coexist.
4. It is possible to reach consensus on ethical norms, policies, and business practices to address new privacy challenges (FPF, 2023b).

Their first belief does not even mention the word "privacy," this should be a red-flag coming from a privacy advocacy group, instead they are advocating for the use of consumer data. Privacy is brought up as a part of "thinking," no actionable steps are laid out. This group is a self-declared "think-tank" that attempts to advance the use of data, masked as a concern for consumer privacy.

In their efforts to collect data, corporations like Google often claim that they are protecting user privacy. In its privacy policy, Google asserts that they "work hard to protect your information and put you in control" (Google, 2023). That summarizes their entire stance on data collection and use. By default Google collects vast user data, including "Terms you search for, Videos you watch, Views and interactions with content and ads, Voice and audio information, Purchase activity, People with whom you communicate or share content, Activity on third-party sites and apps that use our services, Chrome browsing history you've synced with your Google Account" (Google, 2023). Little data is safe by default. Users can turn off some specific data collection services, but the responsibility is theirs to know their data is being collected, to know they can bar data collection, and to take the initiative to do so. Google (2023) frames such restrictive terms as empowering; as a user, you can "Decide what types of activity you'd like saved in your account."

Critics, however, argue that Google and other data-collectors do too little to protect user privacy (Woods, 2018). Data collectors claim that users are responsible for their own privacy and that regulation would degrade their experience. In describing how Google uses collected data,

Google's privacy policy uses the word "improve" 10 times (Google, 2023). For most users, however, developing a command of data collection practices and of their privacy rights is not a practical possibility.

If data collectors protected user privacy, they could be more transparent about their practices. Woods (2018) calls for data sovereignty, arguing that transparent practices are necessary to protect it. Consistent with this principle, Spain has "ordered Google to remove material at a user's request" (Woods, 2018). The United States has no equivalent regulation. Data sovereignty requires litigation to determine which country's laws a company must abide by. According to Woods (2018), when they can, companies prefer to abide by U.S. laws, as they are less strict than those in Europe.

Despite claiming to protect user privacy, corporations put the burden of privacy protection on the user. They lobby Congress to prevent privacy legislation. As corporations they strive to maximize profits, and for this purpose they commit some of their profits to averting regulations that would impede revenue streams.

Privacy Advocacies Policy Advancement

Digital privacy advocate groups act as the opposition to large corporations, asserting that digital privacy measures are not sufficient. These groups work to raise public awareness, advocate for stronger laws, and offer resources to support consumers. They advance their agenda through advocacy, lobbying, public awareness campaigns, and litigation.

Organizations such as the Electronic Privacy Information Center (EPIC), the Electronic Frontiers Foundation (EFF), the Center for Democracy and Technology (CDT), and the

American Civil Liberties Union (ACLU) advocate for digital privacy. The ACLU of California has a guide for protecting consumer privacy:

Respect your data: Limit and protect the data you use

Plan ahead: Incorporate privacy and security from start to finish

Be transparent: Give users the ability to make informed choices

Partner with users: Put users in control and stand up for their rights (ACLU, 2023).

The headers are accompanied by questions guiding data collectors on good practices. Of primary importance is the first point, and further guidelines to protect user data include "identify and collect the data you actually need, retain data only as long as you need it, minimize the links between your data and individual users" (ACLU, 2023).

Advocacies work to inform Congress, federal agencies and consumers as well. In a letter to the Department of Commerce, the CDT outlines risks of data collection. "Several prevalent data practices produce systemic, widespread patterns of harms – targeted to individual people or certain groups, or encountered by society as a whole" (CDT, 2023). The letter highlights how prevalent data sharing is: "Meta and Amazon use and share people's purchase activity, along with other data such as location and device identifiers, to tailor advertisements, measure how well products are meeting the companies' goals, and inform new products." Informing the government allows for the space for legislation to address shortcomings.

The CDT has been active in shaping data privacy policy in the United States for over 25 years, and has played a role in shaping privacy laws such as the Children's Online Privacy Protection Act (COPPA) and the Electronic Communications Privacy Act (ECPA). CDT advocates for stronger privacy protections in areas such as government surveillance, data breaches, and online tracking.

Public awareness campaigns are also used to inform. Educational materials are made available to combat resources such as Meta and Google's privacy policy. EPIC has resources outlining consumer rights (EPIC, 2023). Unlike Meta's privacy policy, which acknowledges consumers "may also have other privacy rights under applicable laws" (Meta, 2023), EPIC lays out those laws. State laws are also available on their website. This is not unique to EPIC, however, as the CDT, ACLU, and EFF all have similar resources. The EFF has a website called the "Action Center" (EFF, 2023). It lists opportunities for individuals to take action, mostly through contacting their representatives. An example being "Pass the 'My Body, My Data' Act" (EFF, 2023). This Act outlines healthcare data protection both from the government and private organizations. The Action Center encourages visitors to alert their Congressional Representatives of their support.

Litigation and legal action are actions that are also taken by organizations. These advocacies often file lawsuits on behalf of individuals or groups affected by privacy violations, and work to hold companies accountable for privacy breaches. The American Civil Liberties Union (ACLU) has been a leader in this area. They sued Clearview AI over the illegal collection of biometric data, resulting in a settlement (ACLU, 2022). The extent of the data collected is alarming: "Clearview has offered access to this database to private companies, wealthy individuals, and federal, state, and local law enforcement agencies. The company claims that, through this enormous database, it can instantaneously identify people with unprecedented accuracy, enabling covert and remote surveillance of Americans on a massive scale" (ACLU, 2022). The ACLU sued on behalf of the residents of Illinois, alerting the public to this breach in privacy.

The goal for data privacy advocates is to solidify protections inside of legislation, and uphold those regulations via litigation. They do this by raising public awareness and interacting with government organizations. In the combat for online privacy, they are fighting for the rights of individuals.

California Case Study: The California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) is a piece of legislation that seeks to protect the online privacy rights of Californians. It is the first comprehensive privacy law in the United States and has been hailed as a significant step towards protecting consumer privacy rights (Klosowski, 2021). Significant lobbying efforts led to the final bill. This legislation sheds a light on how federal policy could be received. "California's race to regulate the tech industry stands in stark contrast to the federal government, where lawmakers long have failed to adopt a national privacy law of their own" (Romm, 2019).

Data collectors funded significant lobbying to oppose many provisions in the bill. Google, Meta, and Amazon argued that legislation would be burdensome, stifle innovation, and create confusion for businesses operating in multiple states that have their own privacy laws. Advocacies created by tech companies such as California Chamber of Commerce (CalChamber) and the Internet Association perform the lobbying. "Last year, CalChamber helped spearhead a $2.2 million coalition that tried to scuttle the ballot initiative that predated the state's privacy law…Facebook and Google donated to that campaign" (Romm, 2019).

Consumer advocacy groups were initially concerned that the CCPA would be weakened by the tech industry's lobbying efforts. However, they were ultimately able to secure significant concessions in the legislation, including the right for consumers to request that their personal

information be deleted, the right to know what personal information companies are collecting about them, and the right to opt-out of the sale of their personal information (Cowan & Singer, 2020).

The passage of the CCPA was the result of a contentious legislative process that involved competing lobbying interests. The CCPA was enacted into law and became the leading privacy legislation in the country (Cowan & Singer, 2020). The CCPA has since become a model for other states seeking to pass their own privacy laws, and it has spurred renewed interest in federal privacy legislation (Klosowski, 2021).

Protections extend from consumers to employees as well. “For the first time, the California law requires employers to tell employees the categories of personal information the company has collected about them and the purposes for which it will be used. Categories of employee information may include online activity data and mobile phone location-tracking information” (Cowan & Singer, 2020).

These protections are “the floor, not the ceiling” (Romm, 2019). Privacy advocates argue rights need to be expanded to:

> Opt-in consent: A company should have to ask you if it may share or sell your data to third parties. You shouldn’t have to spend hours opting out of the collection of your private data through every service you use.
>
> Data minimization: A company should collect only what it needs to provide the service you’re using.
>
> Nondiscrimination and no data-use discrimination: A company shouldn’t discriminate against people who exercise their privacy rights (Klosowski, 2021).

Currently, the only opt-in provision is “Opt-In for Data Sales Related to Minors”, everything else must be opted-out of (Goldman, 2020).

An important caveat in the law pertains to deidentified data. This type of data has much more limited restrictions as it is not considered “personal information.” “Information is personal information if it’s capable of being associated with an individual, but it’s free to use so long as it’s not ‘reasonably’ capable of that association” (Goldman, 2020). Stallings (2020) considers whether these technical protections are well-defined enough and whether they are effective. This perspective is what company funded research like Movahedi et al. (2021) advocate for. It is an important distinction inside a piece of legislation that was advocated for by tech companies (Romm, 2019).

The CCPA is the baseline of what consumer advocacy groups are advocating for (Cowan & Singer, 2020). It is being used as a basis for many other state legislation such as in Colorado and Virginia (Klosowski, 2021). These laws were also lobbied to great effect. “‘A lot of the provisions are business-model affirming. [VCDPA] essentially allows big data-gathering companies to continue doing what they have been doing.’ - Kate Ruane, senior legislative counsel, American Civil Liberties Union” (Klosowski, 2021). The Virginia Consumer Data Protection Act (VCDPA) is not considered as strong by advocacy groups like the ACLU.

Conclusion

Data privacy policy in the United States is a complex issue with many parties attempting to influence public opinion and policy. Despite several federal and state laws that regulate data privacy, there is no comprehensive federal law in place that governs data collection, usage, and distribution by private entities. This has led to a patchwork framework that allows corporations

to go under the radar and lobby the federal government to prevent consumer privacy regulations. These lobbying efforts are driven by profit motives, and while “data-driven” advertising is the claim made, profit is inherently the goal of any corporation.

The lack of comprehensive data privacy regulations has far-reaching implications for individuals, as their personal data is being collected and used without their knowledge or consent. Companies have successfully changed the narrative to put the impetus of privacy on the user. It is critical that federal lawmakers take action to address these concerns and implement comprehensive data privacy regulations that protect the rights of individuals. The passage of the California Consumer Privacy Act in 2018 was a step in the right direction, but it should not fall to individual states to create their own regulations.

Consumers must be careful where they turn to seek information. Meta, Google, and other large tech firms do not offer comprehensive policy outlines. In addition, while advocacies like the ACLU, EFF, EPIC, and CDT have useful resources, think tanks like FPF appear similar but are funded by data-collecting organizations. FPF deflects the responsibility of data privacy by highlighting the benefits brought about by data collection.

As we move forward, more legislation is necessary to protect consumers. We rely on bills that are decades old, and a meaningful online privacy bill has not been passed since 2008 (EPIC, 2023). A balance needs to be struck between data collection, profit, and a right to privacy.

References

ACLU (2022, May 11). American Civil Liberties Union. ACLU v. Clearview AI. https://www.aclu.org/cases/aclu-v-clearview-ai

ACLU (2023). American Civil Liberties Union; It's Good for Business. Privacy & Free Speech. https://www.itsgoodfor.biz/

Atikcan, E. Ö., & Chalmers, A. W. (2019). Choosing lobbying sides: The general data protection regulation of the European Union. *Journal of Public Policy*, 39(4), 543-564.

Auxier, B. (2020, May 4). How Americans see digital privacy issues amid the COVID-19 outbreak. Pew Research Center. https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bayardo, R. J., & Agrawal, R. (2005, April). Data privacy through optimal k-anonymization. In 21st International conference on data engineering (ICDE'05) (pp. 217-228). IEEE.

California Consumer Privacy Act of 2018, 1.81.5 § 1798.100 *et seq.* (2018).

CDT (2023). Center for Democracy and Technology. Re: Request for Comments on Privacy, Equity, and Civil Rights, NTIA-2023-0001. https://cdt.org/wp-content/uploads/2023/03/CDT-Comments-to-NTIA-2023-0001.pdf

Christou, G., & Rashid, I. (2021). Interest group lobbying in the European Union: privacy, data protection and the right to be forgotten. *Comparative European Politics*, 19, 380-400.

Cowan, J., & Singer, N. (2020, January 3). How California's New Privacy Law Affects You. *The New York Times.* https://www.nytimes.com/2020/01/03/us/ccpa-california-privacy-law.html?searchResultPosition=5

Crain, M., & Nadler, A. (2019). Political Manipulation and Internet Advertising Infrastructure. *Journal of Information Policy*, *9*, 370–410.

EFF (2020). Electronic Frontier Foundation. Comments of the Electronic Frontier Foundation Regarding System of Records Notices. https://www.eff.org/files/2020/08/17/2020-08-17_-_eff_comments_re_hhs_regs_re_covid_data.pdf

EFF Action Center. (2023). EFF Action Center; Electronic Frontier Foundation. https://act.eff.org/

EPIC (2021, June). Electronic Privacy Information Center. What the FTC could be doing (but isn't) to protect privacy.

EPIC (2023). Electronic Privacy Information Center. U.S. Privacy Laws. https://epic.org/issues/privacy-laws/united-states/

FPF (2023a). Future of Privacy Forum. About the Future of Privacy Forum. https://fpf.org/about/

FPF (2023b). Future of Privacy Forum. Supporters. https://fpf.org/about/supporters/

Gak, L., Olojo, S., & Salehi, N. (2022, April). The distressing ads that persist: Uncovering the harms of targeted weight-loss ads among users with histories of disordered eating. *Association for Computing Machinery*, 1(9). https://arxiv.org/pdf/2204.03200.pdf

Goldman, E. (2020). An introduction to the California consumer privacy act (CCPA). *Santa Clara Univ. Legal Studies Research Paper.*

Google. (2023). Google Privacy Policy. Google. https://policies.google.com/privacy

Klosowski, T. (2021, September 6). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *The New York Times*. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/?searchResultPosition=7

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data: the management revolution. *Harvard business review*, *90*(10), 60-68.

Meta. (2023). Privacy Policy. Meta. https://www.facebook.com/privacy/policy

Movahedi, M., Case, B.M., Honaker, J., Knox, A., Li, L., Li, Y.P., Saravanan, S., Sengupta, S., & Taubeneck, E. (2021). Privacy-Preserving Randomized Controlled Trials: A Protocol for Industry Scale Deployment. *Proceedings of the 2021 on Cloud Computing Security Workshop*.

Null, E. (2023, January 23). On This Year's International Data Privacy Day, Let's Keep Pushing for National Privacy Protections. Center for Democracy and Technology. https://cdt.org/insights/on-this-years-international-data-privacy-day-lets-keep-pushing-for-national-privacy-protections/

OpenSecrets. (2022). Client Profile: Alphabet Inc lobbying on Consumer Product Safety, 2022. https://www.opensecrets.org/federal-lobbying/clients/issues?cycle=2022&id=D000067823&spec=CSP&specific_issue=Consumer+Product+Safety#specific_issue

OpenSecrets. (2022). Client Profile: Meta lobbying on Computers & Information Tech, 2022. https://www.opensecrets.org/federal-lobbying/clients/issues?cycle=2022&id=D000033563&spec=CPI&specific_issue=Computers+%26+Information+Tech#specific_issue

Privacy Act of 1974, 5 U.S.C. § 552a (1974)

Romm, T. (2019, February 19). "There's going to be a fight here to weaken it": Inside the lobbying war over California's landmark privacy law. *Washington Post*. https://www.washingtonpost.com/technology/2019/02/08/theres-going-be-fight-here-weaken-it-inside-lobbying-war-over-californias-landmark-privacy-law/

Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic data privacy law. Geo. LJ, 106, 115.

Stallings, W. (2020). Handling of personal information and deidentified, aggregated, and pseudonymized information under the California consumer privacy act. *IEEE Security & Privacy*, 18(1), 61-64.

Woods, A. K. (2018). Litigating Data Sovereignty. *Yale Law Journal*, *128(2)*, 328–406.