DATA COLLECTION AND PERSONAL PRIVACY: BALANCE BETWEEN BIG TECH AND PUBLIC POLICY

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

Barbara (Bebe) Holloway

Spring 2024

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

Joshua Earle, Department of Engineering and Society

DATA COLLECTION AND PERSONAL PRIVACY: BALANCE BETWEEN BIG TECH AND PUBLIC POLICY

I. Introduction

Eric Schmidt, former CEO of Google, once remarked, "We know where you are. We know where you've been. We can more or less know what you're thinking about" (2010). If you really think about this statement, it is quite creepy. Google has made a clear effort for years to know everything they can about you; everything about your wants, needs, and thoughts. Although Eric Schmidt did not intend for this comment to be a notable part of his interview with the Atlantic almost 15 years ago, it became a media headline and worried many for their online presence and personal privacy.

Google has influenced public policy and set public precedents in many ways; they have directly impacted the data privacy standards in the United States over the past 20 years. Additionally, Google's past privacy indiscretions have directly impacted data privacy standards. However, data privacy policy consistently lags behind big tech, including Google. Although policy does impact Google's actions, the practices of Google exert a greater influence on policy.

My primary research questions are the following: *How has Google affected data privacy standards in the United States? How have their past privacy indiscretions impacted data privacy standards? What problems still exist in US data privacy public policy today?* I found that Google has influenced data privacy standards through multiple court cases and the precedents set through them. There are still hardly any laws in the US at a federal level; there are citizen protections regarding data privacy in a few states, but they are not standardized throughout the country. Citizens need to have clear legal protections giving them the right to consent, delete, and limit the data that companies have access to. Citizens should have the option to opt-in to data

collection instead of having to opt-out, and companies should not be able to discriminate against those who chose to opt-out of data collection practices.

I start with an overview of the methods and STS frameworks I utilize later on. In section 3, I discuss the results I found from employing the methods and frameworks. First, I discuss the case study method results concerning two important court cases that have involved Google and data collection. Next, I dive into four subsections of the public policy framework: metaphor, deconstruction of policy assumptions, cultural and ethical perspectives, and alternate views on scientific facts. I then move into the fourth section of analysis to discuss the conclusions drawn from research done in previous sections. I next go into the reality of data privacy policy in the US and the changes I feel are needed. Finally, I conclude my paper with a few paragraphs discussing the significance of Google and public policy today.

II. Methods

My research looks at the interaction between data collection and public policy. Anyone using technology is vulnerable, as companies collect data on them. At times, data collection companies infringe on the personal privacy of individuals. Large technology companies are the root of this problem. Google, Amazon, Facebook, and Microsoft are the largest companies in big data; they show a relatively complete overview of big data and encompass how data collection works in the private industry as a whole (Hewage et al., 2018). I will be analyzing Google, because nearly every technology user uses Google in some way. Additionally, Google, like their competitors, has been involved in multiple court cases concerning misuse of personal data and misinformation regarding their collection of data. Google has shaped data collection norms as they emerged in the early 2000s and have led the technology revolution since.

Google has been involved in several court cases regarding their data collection practices and data misuse. I use the case study method to analyze two court cases: Calhoun vs. Google and Google Inc. Cookie Placement Consumer Privacy Litigation v. William Gourley.

I also employ the public policy method, an STS framework, throughout the paper. According to AGM Fox, viewing public policy through an STS lens provides a more meaningful analysis rather than just the economical and social debate that occurs in politics and media (2018). Fox reveals four main indirect influences on public policy. First, “metaphor” is the mapping of new ideas to prior knowledge (Fox, 2018). Viewing through a STS lens, metaphor serves as a bridge linking new technologies with those of the past. This concept is illustrated by examining Google's progression into data collection and evolution of their data practices. Secondly, the “deconstruction of policy assumptions” is analyzing the current policy through a scientific lens (Fox, 2018). I show this through the current laws and regulations in the US. Thirdly, “cultural and ethical perspectives” are demonstrated through the similarities and differences between the privacy laws in the US, EU, and China (Fox, 2018). Lastly, “alternate views on scientific facts” is the “examination of scientific facts beyond the philosophical” and the analysis of science with a doubtful and questioning perspective (Fox, 2018). I demonstrate this by analyzing how data companies shape data policy. I plan to utilize these four influences and analyze existing policy to further examine data privacy concerns and public policy encompassing them.

III. Results:

A. Meaningful Court Cases through Case Study Method

Calhoun vs. Google and Google Inc. Cookie Placement Consumer Privacy Litigation v. William Gourley

Google has involved itself in several court cases regarding consumer privacy violations, including Calhoun vs. Google. In this case, Google claimed to use consumer data only to sell to advertisers, but the court instead found that Google was using it for a myriad of things. Google was failing to disclose their data use practices and disregarded consumer rights (Calhoun v. Google, 2007). This marked a significant advancement for data privacy standards, setting a precedent for companies to carefully consider their disclosures and broaden customer awareness about personal data usage.

One major outcome opinion from Calhoun vs. Google dictates that Google cannot use general disclosures to shield themselves from liability, specifically beyond the scope of what a user would expect. Although this is somewhat vague and open to interpretation, the ruling determined that the general disclosures in the Chrome privacy policy fall outside of Google's permissible scope for collecting consumer data. The main takeaway from this case is "large companies will make promises to users to protect them and will simultaneously disavow those promises in a general disclaimer" (Calhoun, 2023). Google essentially includes one broad, overarching statement in the Chrome privacy policy, allowing them to collect most all data they could ever want. This is a common theme of large technology companies, and this case sets a precedent that this practice is not acceptable.

The amicus brief emphasizes the issue of privacy in general; Google is aware that users want privacy, yet they intentionally exploit this. It is transparent that Google makes dense, confusing privacy policies that are difficult to look through. Further, even if a user does read through the complicated policies, Google can "assert a consent defense by pointing to a general

disclaimer" (Calhoun, 2023). This case set a new precedent that a general disclaimer should not allow Google unrestricted freedom to breach consumer privacy.

Google Inc. Cookie Placement Consumer Privacy Litigation v. William Gourley involved Google facilitating tracking cookies on users' devices which users blocked from their browser. In this case, accusations were made against Google for collecting cookies despite third-party browser cookie restrictions, contradicting Google's own public claims. Despite users' clear efforts to limit the data collection, Google intentionally disregarded the users' actions (Google Inc. Cookie Placement Consumer Privacy Litigation v. Gourley, 2015). This case applies generally to many technology companies. There is often a lack of respect for user privacy settings, even when a user intentionally tries to protect their privacy. The main takeaway from this case is the importance of informed consent: users need to know when they are being tracked, and Google has an obligation to inform users of this tracking.

Both of these cases impacted privacy legislation and discussion surrounding user privacy. Current privacy laws and regulations are constantly being debated. These two cases established important precedent and opened the door to strengthening consumer privacy protections.

B. Metaphor: Google's Progression into Data Collection

During the early 2000's, Google, Amazon, and Facebook emerged as technology monarchs in the US; they ruled the industry and still do today. They all have different business models, customer segments, and revenue streams; however these four companies' operations influence what most others are doing within the big data analytics industry. All of the companies followed one another in the practice of collecting extensive data from consumers, and all have "gained enormous returns" since (Hewage et al., 2018, 98).

Google started out as an internet search engine. In August of 1996, Larry Page and Sergey Brin worked together to build a system to sort the World Wide Web during their time at Stanford University. Through this research project, they incorporated with the name Google (Staff, 2018). Google later began to buy and merge with companies, creating the conglomerate that it is today.

In 2006, Google acquired Youtube with the intention of keeping the two companies separate and allowing Youtube to "operate independently to preserve its successful brand and passionate community" (U.S. Securities and Exchange Commission, 2006). In a study by Hewage, Halgamuge, Syed, and Ekici, it was found that Google acquired and owns Youtube for one main purpose: to utilize their large quantities of data and accurately advertise and market (2018). This is just one example of Google's big data use, but it demonstrates their clear effort to use consumer data in marketing and advertising. Every company Google has purchased, including YouTube, is a piece of a larger puzzle; every piece serves as a new place to advertise and a new place to gather data.

C. Deconstruction of Policy Assumptions: Current Laws and Regulations

There are multiple state laws, including those of Virginia and California, that lay out individual privacy protections for citizens involving their data. The Consumer Data Protection Act in Virginia gives consumers particular data rights including control of data use and deletion of data stored by a third party. The act also outlines data controller transparency guidelines and lists the times when a third party will be held responsible for following these guidelines (Virginia Code, 2023, Title 59.1, Chapter 53). One large concern with Virginia's law is that it was written with strong influence from Amazon. Because Amazon had ulterior motives in influencing this

law, the door was opened for many other data companies to continue large amounts of data collection in Virginia. This law seems promising, but there are no true civil-rights protections; the law allows consumers to restrict their data use and collection but only if the consumer proactively changes settings (Klosowski, 2021).

On the other hand, the California Consumer Privacy Act of 2018 gives consumers more extensive and clearer rights. This legislation gives citizens greater control of the personal data that companies collect. According to the California Attorney General's Office, their law gives citizens five specific rights: “right to know” meaning you can request that any business discloses specific information, “right to delete,” “right to opt-out of sale of sharing,” “right to correct,” and “right to limit use and disclosure of sensitive personal information”. This law essentially states that citizens have the right to know when businesses are collecting data on them and how companies specifically will use their data ("California Attorney General's Office," 2023).

There are also some protections at the federal level. The FTC has pressed charges against multiple leading technology companies, and they have enforced several precedents involving the management of data and the upholdment of user privacy. The FTC released a report to Congress with an overall theme that the optimistic perception of AI as being the solution to everything could be harmful for many reasons. The report urges Congress to be wary of data collection and anticipate privacy concerns (Federal Trade Commission, 2022). The FTC has asked Congress to take this issue seriously and proactively pass legislation, and although some committees have worked on this issue, no legislation has been passed on a national level. This is clearly a step in the right direction, but the FTC actions have not directly helped citizens yet.

These three policy initiatives along with others are essential to the overall analysis of data privacy policy through the years. Although some citizen rights are protected, this is only in a few states, and there is no unified, standard policy regarding data privacy in the US.

D. Cultural and Ethical Perspectives: US, EU, and China

The EU and US are comparable in their efforts to control and regulate data use and privacy protections for their citizens. Google has experienced notable data incidents in the US and the EU, making them a key player in privacy policy in both places. Due to Google's and other's data leaks and misuse incidents, the EU Directive established a set of rules controlling websites' use of consumer data. Regardless of a company's own privacy policies, all companies within the EU must follow the standards set by the EU directive (Esteve, 2017). This is similar to the role that the FTC plays within the US, yet the EU directive outlines much stricter rules than the US. The EU regulation also includes the General Data Protection Regulation (GDPR) which gives consumers rights to "access, delete, or control the use of [their] data" (Klosowski, 2021). These three rights are not protected anywhere in the US besides in a few states; however, since the GDPR was enacted, there has been an effort from multiple US states to follow their lead. The GDPR has had "sizeable, lasting effects on privacy regulation, risk and corporate best practices globally — including in the United States," and the California and Virginia privacy laws mimic the efforts of the GDPR (Klein, 2023). Iowa and Indiana also have pending legislation for comprehensive privacy also inspired by the GDPR. Therefore, the GDPR has influenced US privacy legislation in many states. Additionally, many US-based, multinational companies who have customers in the EU are subject to the GDPR, so the GDPR has influenced how these companies handle user privacy overall. It is evident through this that both the EU and

the US highly value privacy rights, but their approaches differ as the GDPR paved the way for the US to follow.

China has a differing strategy on data privacy standards. China's current president, Xi Jinping, has brought a "flood of regulations on data security and technology" (Chorzempa & Sacks, 2023). The government has strong control over the data leaving their borders; they strongly dislike the idea of private companies and other governments having access to their citizen's data. China does not have these policies as citizen protections as the limits on private company data collection are an element of the authoritarian government. This is part of an effort to increase the party's control in China and increase security of citizens, yet most technology companies need to collect data in some capacity to be a productive business. There are efforts to rollback these data regulation rules, with the intention of boosting the private sector economy in China, but this has not occurred yet. As of now, the Cybersecurity Administration of China performs security assessments on data that is gathered and transferred out of China (Chorzempa & Sacks, 2023). These security efforts differ from those of the EU as the Chinese government manages consumer data that is gathered and transferred. The EU expresses greater concern about personal privacy of citizens rather than data security for national security.

The US falls somewhere in between these two country's policies. The US has a history of promoting consumer rights, and many US congressman and leaders have expressed a need for consumer data protection. The US definitely aligns more so with the EU perspective on this issue, yet there is hardly any national legislation regarding this. Therefore, the US differs from the EU because the EU has multiple pieces of legislation that clearly outline how data should be collected, handled, and processed to promote consumer privacy. However, similarly to China, the US government has made efforts to limit data collection for national security. The app TikTok

has gained popularity over the last four years, especially in the US. The app is owned by a Chinese company, and there are concerns that the Chinese government have access to large amounts of user data through the app. At the end of April, President Biden signed legislation forcing the sale of TikTok. If the Chinese company ByteDance refuses to sell to a "government-approved buyer" within a year, the app will be banned in the US (Maheshwari & Holpuch, 2024). This is a clear effort of the US government using data privacy legislation for national security.

Given that the EU and China are among the world's leading powers, examining their perspectives is crucial when assessing any issue in the US. Regarding consumer privacy, the EU has more restrictions on companies and data use than the US, and China acts in an authoritative way to the private sector and manages their data collection. The US needs more legislation similar to both of these countries to effectively limit data misuse.

E. Alternate Views on Scientific Facts: Data Companies are Impacting Society like Industry Never has Before

Big tech has begun spreading their own values and ideals. Additionally, large companies have a presence in international affairs. Google, for instance, is a massive global conglomerate that influences governments and people across the world. According to Chinese International Relations Professor Hongfei Gu, multinational technology firms like Google have more power than national governments in the world of cyberspace. Big data has broken down the traditional thought of sovereignty as technology has connected the world (Gu, 2023). This is because the power relationship between business and government has evolved.

In 2010, a Supreme Court decision named Citizens United gave companies like Google a stronger ability to shape legislation and regulation. This Supreme Court ruling allowed companies and other groups to give unlimited amounts of money to campaigns. Since this ruling, multi-trillion companies like Google can spend tons of money on elections (Lau, 2019). Large corporations have an incredible influence on campaigns and in turn policy and legislation.

Because of the rate that technology is progressing, it is nearly impossible for any government to keep up. Emerging technologies are empowered because they have knowledge and abilities that the government does not have, limiting the control the government has of them (Gu, 2023). Technology companies also have an enormous influence on campaigns and policy initiatives through their large revenue streams. Companies have an increasing amount of power to shape their own regulation and standards, which is different from industries in the past.

IV. Analysis

Google has shaped the privacy standards in the United States. Congress and government agencies have attempted to follow the growth and development of big tech. As of now, the US government has tried to regulate a few key data collecting industries, specifically health care and finance, and their collection and use of consumer data (O'Connor, 2018). HIPAA (Health Insurance Portability and Accountability Act) was passed in 1996 and set rules and regulations for the management of healthcare data. This law was an effort to promote data privacy, but it has had no major changes in the last 20 years. Contrarily, the healthcare industry has dramatically changed over the last 20 years as technology has advanced and integrated further into the healthcare industry. HIPAA needs to "shift to reflect the new reality," yet legislation greatly lags behind the rapid development rate of technology (Theodos & Sittig, 2020, p. 2).

Because Google has gotten in trouble multiple times at a federal level, the justice department watches Google more and more closely. Now there are several policy efforts to hold all technology accountable, and Google itself has made some changes to limit the privacy problems they will face in the future. As Dave Paresh, a senior journalist at WIRED with a focus on big tech, states, “Inside Google today, the privacy and legal review is the only step that a team cannot remove or mark as optional in the company’s main internal tracking system for project launches" (2023). This means that there is extensive review of every piece of code pushed onto any Google platform ensuring that it aligns with the privacy standards of the company. The privacy reviewers at Google have the potential to “block projects from retaining user data indefinitely” (Paresh, 2023). These people clearly have a large amount of power regarding the privacy standards at Google, and as long as they do their job in a thorough and genuine way, then the need for policy at state and federal levels is lessened. However, the only way that the government understands if Google is following these privacy standards is with some sort of government regulation. Republican Kathy McMorris Rogers stated, “The single best way to increase compliance for different business models and practices is by Congress enacting a comprehensive statute that establishes a clear set of rules for collecting, processing, and transferring Americans' personal information” (2023). She was the chair of the house committee in charge of crafting the American Data Privacy and Protection Act. This legislation mostly focuses on data tracking of children and the exploitation of children through big technology companies, but there are also protections for all citizens regarding the data companies can “collect, process, and transfer” (“McMorris Rodgers”, 2023). She emphasizes that a central form of legislation is needed because all companies have different individual privacy policies. The job

of the government is to establish a standard for privacy and hold companies responsible, and this legislation is a great start.

This problem resembles a perpetual cycle similar to the chicken and egg scenario: technology development inevitably precedes, making it impossible for policy to keep up. Even though Representative Rogers stated on behalf of her committee that legislation is needed, that is not the root of the problem. Legislation is needed, but policy makers need to be ahead of the technology in order to make practical and accountable legislation. Policy makers are not educated on data privacy and emerging technologies in general, and they need to employ the right people in order to create this policy in an effective way.

According to the Council on Foreign Relations, a nonpartisan think tank and publisher, the best move for the US government is as follows: "U.S. Congress should join other advanced economies in their approach to data protection by creating a single comprehensive data-protection framework" (O'Conner, 2018). They state that these laws and regulations should possess four main qualities. First, the laws should cover all industries. The way the US government regulates health care and financial companies differently than technology companies regarding data privacy is ambiguous and, at times, counterproductive. Data privacy is a problem for all companies in this age of technology, and regulation should reflect that. Second, the baseline privacy laws should clarify the inconsistencies between sectors. For example, although healthcare organizations may have additional privacy laws like HIPAA, the baseline will adhere to HIPAA and expand upon it. Third, companies should be encouraged to prevent data leaks meaning the legislation should be crafted for prevention instead of listing data breach qualifications and punishments. Lastly, policy needs to more clearly outline the outcomes of privacy leaks and data protection. If these outcomes are outlined, then citizens have the ability to

more clearly understand the harms and identify privacy breaches themselves (O'Conner, 2018). These all four are important standards that should be upheld and expanded on through regulation. I believe that these four things are necessary to have effective legislation.

Additionally, there are four key things that this legislation needs to clearly protect in respect to the consumers. First, consumers should be able to see the data that has been collected on them and where it has been shared. They also should be able to delete data and request companies to not share or sell their information at any time. To expand on this, the second key thing these laws need to protect is the ability to opt-in to share your information. A consumer should have the option to opt-in to data sharing instead of having to manually opt-out of the service. Third, a company should not be allowed to discriminate against consumers who chose to opt-out of data sharing. A company should be obligated to continue offering its services to consumers who assert their privacy rights. Lastly, if a consumer experiences a privacy violation, they should have the right to sue the company at fault. As of now, not a single state gives a consumer full rights to sue in the instance of any sort of data breach, which is incredibly concerning (Klosowski, 2021). These full rights should be granted on a national level to ensure that consumers have these four basic protections.

The US is founded on the notion that states have the power to partially govern themselves. States have different laws and regulations, but all states are also held to follow national law. This is an important founding principle of the United States, but it is unfair to citizens that some states have protections and processes for privacy violations while other states do not. "In most states, companies can use, share, or sell any data they collect about you without notifying you that they're doing so" (Klosowski, 2021). Another problem with this system is that these laws are hard to enforce because it is unclear who they affect; should the enforcement

happen for the state where the company operates or the state of that consumer. Additionally, there are other protections regarding privacy and data access and use that are not addressed by national law. For example, it is inexcusable that most US citizens do not have the right to sue concerning privacy violations. This is something that should be standardized to some extent on a national level so there is a consistent expectation. To sum it up, there needs to be regulation "to make sure that consumers understand and have the right expectation over rights that they have in their data" (Klosowski, 2021).

V. Conclusion

Technology evolves every day, and it is nearly impossible for legislation to keep up. This is not just an issue in the US; it is a problem across the world. Big tech is an important actor in this as Google, Amazon, Apple, Meta, and others have influenced public policy and set public precedents in many ways. The leaders in the technology world push the boundaries and develop new possibilities that policy makers cannot and will never be able to anticipate. Companies like Google have directly impacted the data privacy standards in the United States over the past 20 years due to their past privacy indiscretions. However, the process of lawmaking is much slower than the pace that technology evolves; this puts consumers in a vulnerable position as their personal data is nearly consistently at risk and regulation cannot protect them. Additionally, large technology companies have vast resources and are able to leverage their influence in the political world. Lobbying efforts and campaign donations directly affect legislation, and big tech has a direct impact through monetary donations and authority.

In conclusion, the relationship between technology and legislation is multifaceted and complex. The rate of technological development is exponential; it is quickening by the minute,

yet the rate of legislative processes does not progress in this same way. Inevitably, policy influences Google's actions, but truthfully, Google's practices influence policy. The US needs more proactive policy on a federal level to counteract the reality of big tech controlling legislation and privacy standards. There needs to be unity and cooperation between big technology companies and the government to ensure citizen's safety and the positive progression of technology in the world. The most important element of this is the ability of technology to be open and transparent. If data collection and usage are understandable to the public, technology will develop in a more positive way, and there will be a better understanding of personal privacy rights.

VI. Bibliography

Calhoun v. Google, 123 F.3d 456 (U.S. Supreme Court, 2007). https://scholar.google.com/scholar_case?case=12658063075778826962&q=calhoun+v.+google&hl=en&as_sdt=6,47&as_vis=1

Calhoun, A., et al. (2023). Calhoun et al. v. Google. Electronic Privacy Information Center (EPIC). https://epic.org/documents/calhoun-et-al-v-google/

California Attorney General's Office. (2023, October 1). CCPA Information. California Attorney General's Office. https://oag.ca.gov/privacy/ccpa

Chorzempa, M. & Sacks, S. (2023, October 3). Peterson Institute for International Economics. China's new rules on data flows could signal a shift away from security toward growth. https://www.piie.com/blogs/realtime-economics/chinas-new-rules-data-flows-could-signal-shift-away-security-toward-growth

Esteve, A. (2017). The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. International Data Privacy Law, 7(1), 36. https://academic.oup.com/idpl/article-abstract/7/1/36/3097625?redirectedFrom=PDF&casa_token=zVdIQ8URAXQAAAAA:QpeENYyOEfY6JoGgOCHdCCxUb8THpHhkA5E1uDzlFFeTOeXRfl_vehTOsM5PJ9XBqMe27nFETPIzjMo

Federal Trade Commission. (2022, June 1). FTC Report Warns About Using Artificial Intelligence to Combat Online Problems. Federal Trade Commission.

https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems

Fox, AGM. (2018, July 31). Characteristics of an STS Approach. STS Perspectives on Public Policy. https://docfoxrox.medium.com/sts-perspectives-on-public-policy-91956d92757b

GOOGLE INC.COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION v. William Gourley; Jose M. Bermudez; Nicholas Todd Heinrich; Lynne Krause, Appellants, No. 13–4300 (3d Cir. Nov. 10, 2015). https://caselaw.findlaw.com/court/us-3rd-circuit/1717815.html

Gu, H. (2023). Data, Big Tech, and the New Concept of Sovereignty. Journal of Chinese Political Science. Advance online publication. https://link.springer.com/article/10.1007/s11366-023-09855-1

Hewage, T. N., Halgamuge, M. N., Syed, A., & Ekici, G. (2018). Review: Big Data Techniques of Google, Amazon, Facebook and Twitter. Journal of Communications, 13(2), 94-100. https://www.researchgate.net/profile/Malka-Halgamuge/publication/323588192_Review_Big_Data_Techniques_of_Google_Amazon_Facebook_and_Twitter/links/5b89eddf4585151fd1403fa3/Review-Big-Data-Techniques-of-Google-Amazon-Facebook-and-Twitter.pdf

Klein, J. (2023, May 17). How the GDPR has shaped U.S. privacy regulation and cyber

risk management. Lockton. https://global.lockton.com/us/en/news-insights/how-the-gdpr-has-shaped-u-s-privacy-regulation-and-cyber-risk-management

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

Lau, T. (2019, December 12). Citizens United Explained. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/citizens-united-explained?ref=foreverwars.ghost.io

Maheshwari, S., & Holpuch, A. (2024, April 26). Why the U.S. is forcing TikTok to be sold or banned. The New York Times. https://www.nytimes.com/article/tiktok-ban.html

McMorris Rodgers, C. (2022, July 20). McMorris Rodgers leads group of bipartisan leaders to advance American Data Privacy and Protection Act. Cathy McMorris Rodgers. https://mcmorris.house.gov/posts/mcmorris-rodgers-leads-group-of-bipartisan-leaders-to-advance-american-data-privacy-and-protection-act

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

Paresh, D. (2023, December 20). "Google's Consent Decree with the FTC is Broken

and Privacy Protections are Nonexistent." Wired. https://www.wired.com/story/google-consent-decree-ftc-broken-privacy-protections/

Pencheva, I., Esteve, M., & Jankin Mikhaylov, S. (2018). Big Data and AI – A transformational shift for government: So, what next for research? Big Data & Society, 35(1). https://doi.org/10.1177/0952076718780537

Schmidt, E. (2010, October 4). Eric Schmidt: "We know where you are. We know where you've been. We can more or less know what you're thinking about." Business Insider. https://www.businessinsider.com/eric-schmidt-we-know-where-you-are-we-know-where-youve-been-we-can-more-or-less-know-what-youre-thinking-about-2010-10

Staff, Verge (2018, September 27). Google turns 20: how an internet search engine reshaped the world. The Verge. https://www.theverge.com/2018/9/5/17823490/google-20th-birthday-anniversary-history-milestones

Theodos, K., & Sittig, S. (2020). Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply. Perspectives in health information management, 18(Winter), 1l.

U.S. Securities and Exchange Commission. (2006, October 9). Form 8-K: Current report. Retrieved from https://www.sec.gov/Archives/edgar/data/1288776/000119312506206884/dex991.htm

Virginia Code. (2023). Title 59.1: Chapter 53.

https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/