Social Group Influence in the California Consumer Privacy Act

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

Rishika Nayak
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
MC Forelle, Department of Engineering and Society

Introduction

In an increasingly data-driven world, the evolving landscape of digital privacy raises concerns about how companies are using consumer data. A 2021 KPMG study confirms that data collection is rising, with 70% of business leaders reporting that their companies have increased consumer data collection over the past year and 33% saying that consumers should be concerned with how their company is using their personal data (*Corporate data responsibility*). The digital landscape is full of potential threats to individuals' privacy, ranging from targeted advertising to more sinister forms of exploitation. As such, the importance of safeguarding data privacy cannot be overstated. A significant incident that drew attention to consumer data privacy issues emerged with the 2018 Cambridge Analytica revelations, involving the unauthorized access and exploitation of personal data belonging to millions of Facebook users for political campaign purposes (Kozlowska, 2018). Cambridge Analytica's misuse of consumer data on such a massive scale displays the importance of robust data privacy regulations. The revelation of this scandal significantly accelerated efforts for data privacy legislation in the U.S. (Alpert, 2020, p. 1216). Data privacy is the principle that individuals should have control over their personal information (*What is privacy?*). Without adequate safeguards, personal information can be exploited for various purposes, including identity theft, manipulation, and discrimination. The rapid growth of large-scale data collection calls for attention to ethical means of handling consumer information. There are several groups, including privacy groups, businesses, and government agencies, that have the means to establish change in the way consumer data is collected and used. In my research, I will be focusing on the influence that such groups have on government-level regulation of consumer data privacy.

The General Data Protection Regulation (GDPR), put into effect by the European Union in 2018, stands as a landmark legislation in the realm of data privacy. The GDPR sets stringent standards for the collection, processing, and storage of personal data. It grants individuals greater control over their data and imposes hefty penalties on organizations that fail to comply with its provisions (*What is GDPR, the EU's new data protection law?*, 2018). Currently, in the United States there is no comprehensive federal data privacy law; however, thirteen states have enacted their own data privacy legislation. In June 2018, California became the first state to introduce consumer data privacy legislation in the United States, the California Consumer Privacy Act (CCPA). Parallel to the GDPR, the CCPA, enacted in response to growing concerns over data privacy, extends consumer rights regarding their personal information, including the right to know what data is collected and the right to opt-out of its sale (*California Consumer Privacy Act*, 2023). The CCPA represents a significant step towards enhancing data privacy protections in the United States and serves as a model for similar legislation across the nation.

By understanding the motivations, agendas, and interactions of stakeholders involved in the passage of the CCPA, we can gain insights into how data privacy legislative decisions are made and enacted. Studying the CCPA is important for four reasons: (1) The legislation applies to the most populous state in the United States, (2) the CCPA is the first data privacy legislation of its kind in the US, (3) California is home to a plethora of large technology companies, such as Amazon, Cisco Systems, Microsoft, and Meta, and (4) "California laws often serve as a model for other state legislatures" (Barrett, 2019). Stakeholders, ranging from consumer advocacy groups to industry associations, wield varying degrees of influence in the legislative process. I argue that the CCPA was shaped through a conflict of interests, where the interests of consumer-side stakeholders prevailed over those of corporate-side stakeholders. Throughout this paper, I

analyze litigation journals and public records of the CCPA rulemaking process to investigate the key stakeholders involved. In understanding how these stakeholders influenced data privacy legislation in California, I aim to provide some insight into how future data privacy legislation will be shaped in the United States. Ultimately, this research underscores the significance of stakeholder engagement in shaping consumer data privacy policy outcomes.

Literature Review

I. Shared Meanings of Data Privacy

When discussing data privacy, I focus on the governance of personal data– specifically, policies that protect the rights of individuals to control the collection, use, and sharing of their personal data *(What is privacy?).* It concerns the regulatory protection of sensitive information from unauthorized access, misuse, or exploitation. Data privacy may be characterized by a certain criterion; however, data privacy is framed differently through contrasting perspectives on the nature of personal information. From a consumer standpoint, data is often viewed as deeply personal and deserving of rigorous protection. Individuals value their privacy and expect organizations to handle their data responsibly and transparently. Personal data that businesses collect on consumers, including browsing history, location data, and purchase behavior, is viewed by consumers as valuable, personal information that must be protected (Morey et al., 2015). Therefore, consumer-side stakeholders have a shared meaning of data privacy as a human right (Smith et al., 2011, p. 994). Conversely, from a corporate perspective, data is frequently perceived as a valuable commodity (Smith et al., 2011, p. 994). Companies collect vast amounts of data to gain insights into consumer behavior, improve products and services, and target advertising more effectively (West, 2019). This perspective highlights the economic value of

data to businesses. Because of this, companies run the risk of prioritizing data collection and monetization over individual privacy concerns. With these differing frames of data privacy, there can be tensions between consumers seeking more control over their personal information and businesses seeking to leverage data for competitive advantage and profit. The central challenge in the governance of data privacy is balancing these divergent views, considering both individual rights and economic interests.

II. Governance of Data Privacy

In recent years, governments across the world have been considering how to regulate data privacy within their respective jurisdictions. In the European Union (EU), the governance of data privacy has undergone significant evolution with the enactment of the General Data Protection Regulation (GDPR) in 2018. The GDPR set precedence as the "world's first comprehensive data privacy legislation" and regulates any organization, regardless of location, that collects or processes the data of EU citizens (Perumal, 2022, p. 100; Zaeem & Barber, 2020, p. 1). It grants individuals extensive rights, such as the right to access their data, the right to rectify inaccuracies, the right to erase their data, and the right to data portability. Moreover, the GDPR imposes strict obligations on businesses, including needing explicit consumer consent for data processing, the notification of data breaches, and significant penalties for non-compliance (Bakare, et. al, 2024). With these initiatives, the GDPR marks a pivotal milestone in the global push for robust data privacy legislation and serves as a landmark for future legislation to come.

In the United States, the governance of data privacy has historically been characterized by a fragmented approach, where data privacy laws and regulations address specific sectors or states. For example, the Health Insurance Portability and Accountability Act (HIPAA) regulates

the privacy of health information, while the Gramm-Leach-Bliley Act (GLBA) regulates the handling of consumer data in the financial sector (Bakare, et. al, 2024). There is no comprehensive federal legislation akin to the GDPR in the United States. Instead, data privacy in the U.S. is defined by a "patchwork of state laws", such as the California Consumer Privacy Act (CCPA), along with legislations in a few other states including Virginia, Colorado, Connecticut, Utah, and more. Additionally, there has been ongoing pressure at the federal level to establish a comprehensive data privacy law that would set consistent standards and protections across the country (Perumal, 2022). While the EU has taken a more centralized approach with the GDPR, the U.S. has seen a more piecemeal approach, although efforts are underway to implement privacy protections at both the state and federal levels. Overall, the push for governance of data privacy in the United States reflects a growing demand from stakeholders to implement comprehensive legislation that will address their diverse needs.

III. The California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) represents a catalyst for furthering consumer data privacy rights in the United States. As the first legislation of its kind in the US, the CCPA gives Californian residents more control over the data that companies collect on them. The CCPA extends new privacy rights including the right to know about how the data businesses collect is used and shared, the right to delete personal information collected, the right to opt-out of the sale or sharing of personal information, and the right to non-discrimination (*California Consumer Privacy Act*, 2023). Crafting these provisions entailed a multi-step process that involved multiple stakeholders. Preliminary language of the CCPA was introduced as a ballot initiative in October 2017 by a privacy group known as Californians for Consumer Privacy.

Initially enacted in June 2018, the CCPA underwent a series of rulemakings overseen by the California Attorney General's office. A period of public comment then ensued from January 2019 to March 2019, where stakeholders were able to impart their influence. Amendments to the bill were drafted and officially signed into law in October 2019 and the CCPA's final regulations became effective on January 1, 2020 (*California Privacy Legislation: A Timeline of Key Events*). Since then, the rulemaking process has continued with ongoing amendments and adjustments to adapt to evolving privacy concerns. The timeline for these rulemaking activities reflects an effort to balance the interests of consumers, businesses, and regulatory authorities in safeguarding privacy rights. The consultation phase of the rulemaking process is generally a time when stakeholders have an opportunity to influence policy rules (Baik, 2020, p. 6). In my study, I focus on the period of public comments made during the rulemaking process in order to analyze stakeholders' influence.

IV. Theory of Social Construction of Technology

In examining the factors shaping the passing of the California Consumer Privacy Act (CCPA), I will adopt Pinch & Bijker's Social Construction of Technology framework as my conceptual and theoretical lens. This framework outlines how the development and stabilization of technical artifacts is not a linear process, but rather a multi-dimensional process influenced by the competing needs of relevant social groups (Pinch & Bijker, 1984). Relevant social groups in this regard are groups that share the same set of meanings with respect to an *artefact*– in this case data privacy. The social groups that I will be investigating will be those that share the same meanings of data privacy; for example, how consumer groups may perceive data privacy as an individual right and, conversely, how companies may perceive data as a commodity. Central to this theory is the recognition that social groups play a pivotal role in shaping the design, use, and

evolution of technologies. Specifically, I will focus on identifying and analyzing the influence of various stakeholders with the same shared meanings of data privacy in the development of the CCPA. Through this framework, I aim to discover how differing interests, priorities, and understandings among these groups have shaped the trajectory of privacy legislation in California. Key to this analysis will be the identification of relevant social groups—those organizing around shared meanings of technology—and understanding their respective roles in shaping the CCPA.

Methods

To investigate the dynamics surrounding the passing of the CCPA and the influence exerted by various stakeholders, I employed a combination of primary and secondary research methods. First, I gathered primary sources, including public forums discussing the CCPA from January 2019 to March 2019 as well as comments such as letters addressed to the California legislature from concerned stakeholders during that time period. By analyzing these primary materials, I discerned the different social groups invested in the CCPA and noted the specific concerns and priorities they brought to the legislative discourse. Additionally, I complemented my primary research with secondary sources, such as literature reviews and legal journals detailing the policymaking process of the CCPA. Another secondary source I looked at will be news articles surrounding CCPA rulemaking in order to study discussions surrounding the legislation at the time. News sources I look at include the *New York Times, Los Angeles Times, and the Sacramento Bee*. Through this multifaceted approach, I sought to comprehensively uncover the nuanced interplay between consumer groups, companies, and other stakeholders in shaping the CCPA. This methodology enabled me to construct a thorough analysis of the social dynamics behind the passage of the CCPA.

Analysis

The introduction of the CCPA demonstrated a significant victory for consumer-side stakeholders in initiating data privacy legislation in the United States. The CCPA was initially proposed as a ballot initiative by the Californians for Consumer Privacy group, sponsored by Alastair Mactaggart (Luna, 2018). The proposed initiative sought to impose strict data privacy requirements on businesses, requiring them to disclose the information they collect on consumers and giving people the right to prevent businesses from selling that information (Luna, 2018). Major corporations, including Amazon, Google, AT&T, and Comcast, strongly opposed this proposed bill due to the cost of compliance and potential competitive disadvantages. Opposition to the initiative had already spent $2.2 million to remove it from the ballot, and Mactaggart expected his opponents to drop another $100 million in contestation. In a last-minute deal to avoid this costly ballot box fight, Mactaggart pledged to pull his initiative if Governor Jerry Brown signed a similar bill that Mactaggart crafted with state lawmakers and other stakeholders (Luna, 2018). Some concessions had to be made in this negotiation, as Mactaggart stated "the legislation would accomplish most but not all of what he sought in the initiative" (Luna, 2018). Specifically, the June passage of CCPA obtained many more consumer rights than the ballot initiative originally sought; it clarified a section with respect to pricing differently based on privacy choices; and it lessened the Private Right of Action but kept substantial and meaningful penalties in place to ensure compliance (*California Privacy Legislation: A Timeline of Key Events*). On June 28, 2018, the CCPA was signed into law by Gov. Brown, and the rulemaking process began (Mactaggart, 2018). Therefore, the initial push for the CCPA revealed an evident competition between consumer advocacy and corporate influence, demonstrating the challenges in balancing privacy protections with corporate interests. Despite some concessions being made

in the preliminary language of the CCPA to deter pressures from corporate giants, the CCPA's introduction highlighted a notable win for consumer-side stakeholders. This set the stage for a tug-of-war between the interests of consumer-side and corporate-side entities over what the CCPA's provisions would entail.

The California Consumer Privacy Act elicited intense debate during its rulemaking process, revealing a fundamental battle between stakeholders who perceive data as a commodity and those who regard data privacy as a human right. This clash is evident across various key provisions, including 1) the Definition of "Personal Information," 2) Private Right of Action, and 3) the Right to Opt-out. Each aspect reflects divergent views on the value and control of personal data, with stakeholders advocating for positions that align with their interests and perspectives.

1. *Definition of "Personal Information"*

The amended definition of "personal information" in the 2020 CCPA showcased the prioritization of consumer-side interests, despite concessions made to appease corporate-side stakeholders. After the approval of Senate Bill 1211 in September 2018, the definition of personal information read: '"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" (SB-1121, 2018). In the public discussion during the CCPA preliminary rulemaking process, competing standpoints on this definition arose. Corporate side entities argued for more specificity within the definition of personal information, while consumer side entities advocated to keep the definition broad. Public comments made by Apple, Inc. urged the Attorney General to clarify that "personal information" excludes data identified by non-personally identifiable identifiers (Kennedy, 2019). Additionally, corporations such as Google and GitHub called for harmonization of the definition of personal

information with that defined by the GDPR, classifying data as personal information only if it is directly linked to a customer (Pantazis, 2019; Vollmer, 2019). Okta, the IT service management company, agreed, stating that personal information should be limited to data directly identifying or relating to an individual, expressing skepticism about including IP addresses, devices, households, or electronic network activity as proposed in the early CCPA version (Khan, 2019). Such corporate-side stakeholders advocated to limit the scope of "personal information" to narrow down the types of data subjected to stringent privacy regulations. Such comments reveal that corporate-side entities perceive personal information as data directly tied to an individual's identity or attributes, such as name, address, or contact details. In contrast, they are skeptical about including broader categories like IP addresses, devices, households, or electronic network activity. This indicates that they view personal information through a narrow lens, focusing on tangible identifiers rather than broader digital footprints. Furthermore, by pushing for alignment with GDPR definitions and urging for exclusions of data identified by non-personally identifiable identifiers, these corporate entities demonstrate their view of data as a commodity. They seek to limit the scope of personal information to minimize regulatory burdens and maintain control over their data assets. This approach suggests that they perceive data primarily as a resource to be leveraged for business purposes rather than as a representation of individuals' privacy rights or personal identities. In essence, by advocating for narrow definitions and exclusions within the concept of personal information, corporate-side stakeholders position data as a commodity to be used for business advantages rather than as a fundamental aspect of individual privacy and autonomy. Conversely, on the consumer-side, entities advocated to maintain the expansiveness of what personal information entails. Consumer-side entities, such as Consumer Reports, a consumer-advocacy group, and Brave Software, a private web browser

company, urged the Attorney General to keep the definition of personal information broad in order to ensure sensitive data is protected (Brookman, 2019; Ryan, 2019). Brave Software, although a company themselves, is classified as a consumer-side stakeholder due to their advocacy for all sensitive data related to individuals being adequately protected. This stance aligns with their mission to provide users with comprehensive privacy protection while browsing the web. Another consumer-advocacy group, the Consumer Watchdog, asserted that there is no valid reason to exclude IP addresses since they can easily be connected to specific individuals or households. Additionally, they argue that the CCPA should safeguard all personal information gathered by companies to encompass any data related to a person (Scow, 2019). Consumer-side social groups aimed to extend privacy rights over all data directly or indirectly linked to an individual in line with their shared meaning of "data privacy as a human right". By advocating to maintain the extension of privacy rights to cover such data, these groups aim to ensure that individuals rightfully retain sovereignty over their personal information. These competing interests resulted in a compromise– the term "reasonable" was added to the definition of personal information (i.e. the current "capable of being associated with" will become "reasonably capable of being associated with") (SB-1121, 2018). The addition of the term "reasonable" to the definition of personal information was a minor subjective concession to corporate-side stakeholders, while maintaining a generally expansive definition. Therefore, this adjustment ultimately favored the consumer-side stakeholders, indicating their greater influence over corporate interests in shaping the CCPA regulations.

2. *Private Right of Action*

While the final provisions concerning private right of action for CCPA violations didn't fully address consumer-side concerns, they did preserve some rights in this regard. The early

version of the CCPA mandated consumers to give businesses a 30-day written notice of alleged violations before taking legal action, allowing businesses a chance to fix the issues. A proposed amendment, Senate Bill 561, would have removed this provision, allowing consumers to sue a company for violations of the CCPA without such notice. Social groups with vested financial interests, such as GitHub and the American Property Casualty Insurance Association, explicitly objected to S.B. 561, especially "given the complexity of implementing CCPA while it is still being finalized during the rulemaking period" (Vollmer, 2019; Kammerer, 2019). By opposing Senate Bill 561, these corporate stakeholders sought to protect their interests in maintaining control over data assets and minimizing regulatory burdens, reflecting their overarching view of data as a valuable commodity. On the other side of the dispute, consumer-side entities supported S.B. 561. The County of Santa Clara Privacy Office argued that "the CCPA should be amended to explicitly allow consumers a private right of action for any violations of the law's provisions" (Shapiro, 2019). Other groups including Consumer Attorneys of California and Consumer Watchdog also advocate for private right of action for consumers whenever their rights are violated under the CCPA (Blood, 2019). With the view of data privacy as a human right, consumer-side social groups promote enhanced consumer rights and enforcement mechanisms. By pushing for the removal of the requirement for prior notice before legal action, these groups emphasize the necessity of swift and effective protection of individuals' privacy rights without unnecessary bureaucratic hurdles. Their argument for immediate access to legal recourse for CCPA violations demonstrates their view that data privacy is a human right deserving of protection. As a result of this debate, Senate Bill 561 ended up being rejected, and the 30-day cure period was signed off on (Golden Data Law, 2020). While consumer-side advocates didn't achieve their desired outcome, the final version of the CCPA still allowed for private right of

action without prior notice in cases of data breaches. Thus, although corporate interests were prioritized regarding the 30-day notice period, consumer-side interests were still safeguarded concerning more severe violations of data privacy.

3. *Right to Opt-out*

Finally, the 2020 CCPA provisions regarding the right to opt-out reflected the desires of consumer-side stakeholders over those of corporate-side stakeholders. The CCPA provided the right for consumers to opt-out the sale of their information by requiring businesses to include an opt-out button on their sites (5). Social groups viewing data as a commodity advocated for more opt-out choices, whereas social groups viewing data as an extension of identity advocated for a holistic opt-out button. A corporate-side stakeholder, an attorney at Loeb & Loeb, expressed that the CCPA "doesn't explicitly permit a business to allow a consumer a choice of what they are opting out of," and suggested a provision of more choices to consumers, (Lee, 2019). Another attorney argued that more opt-out choices, as opposed to an all-or-nothing opt-out would give consumers more flexibility and greater control over their privacy (Cohen, 2019). Providing more opt-out choices potentially allows corporations to selectively collect some data from consumers who opt-out, rather than none at all. This approach allows companies more leverage and access to consumer data, aligning with their interests in maximizing data collection for profit. Although both parties reasoned that more opt-out choices would foster more flexibility for the consumer, their motivations were drawn from the data-as-commodity perspective. This is because even though more opt-out choices would offer more flexibility, consumers would lose some control through the difficulty of having to navigate through multiple opt-out decisions. For this reason, consumer-side groups advocated for a universal opt-out option. An activist representing Consumer Reports argued that it is impractical to have multiple opt-outs for different sites as it

would be difficult to navigate and use (Brookman, 2019). Consumer-side advocates such as Consumer Reports suggest a universal opt-out button because it provides a simpler and more comprehensive way for individuals to assert control over their personal information. By prioritizing simplicity and comprehensiveness in data control mechanisms, consumer-side groups aimed to enable individuals greater control over their personal information, aligning with their view of data privacy as a human right. In the January 2020 enactment of the final version of the CCPA, it mandated that businesses incorporate a universal opt-out button (5). Ultimately, in this regard, the CCPA right to opt-out provision was shaped to protect the interests of consumer-side stakeholders.

Conclusion

Therefore, the CCPA enacted in January 2020 showcased the prioritization of consumer-side interests to protect data privacy as a human right. Throughout its legislative journey, the CCPA presented a battleground where stakeholders clashed over competing views of data—as either a valuable commodity or a fundamental aspect of human rights and privacy. Despite facing opposition from corporate entities, the CCPA ultimately highlighted consumer-side interests in protecting consumer data. Even through there were some victories for corporate interests, such as retaining the 30-day notice period for private right of action, the CCPA ultimately emphasized consumer-side interests, as seen in provisions like the expansive definition of personal information and the universal opt-out button. In essence, the CCPA's enactment marked a significant milestone in the ongoing evolution of data privacy governance as a potential model for future legislation. By prioritizing the protection of personal data as a fundamental human right, the CCPA set a precedent for comprehensive data privacy laws in balancing the needs of consumers and businesses. As other state and federal governments strive

for data privacy regulation, the CCPA's rulemaking process provides valuable insights into the complexities of stakeholder engagement and the need for upholding consumer rights. Outside the scope of this paper includes how similar stakeholders influenced other state data privacy legislation as well as considering the influence of other stakeholders apart from consumer-side and corporate-side. In this regard, future research in this area could explore the rulemaking process of other data privacy legislations or analyzing the influence of other stakeholders. Studying the rulemaking processes of other data privacy laws offers comparative insights into similarities, differences, and factors shaping governance at state and federal levels. Additionally, analyzing the influence of diverse stakeholders, such as government agencies, healthcare professionals, and legal scholars, adds to the understanding of data privacy policymaking dynamics. By continuing to examine the evolving landscape of data privacy regulation, researchers can contribute to the ongoing dialogue surrounding the protection of consumer data rights.

References

Alexander, C. B. (2019). The General Data Protection Regulation and California Consumer Privacy Act: The Economic Impact and Future of Data Privacy Regulations. *Loy. Consumer L. Rev.*, *32*, 199.

Alpert, D. (2020). Beyond Request-and-Respond: Why Data Access Will Be Insufficient to Tame Big Tech. *Columbia Law Review*, *120*(5), 1215–1254.

Baik, J. S. (2020). Data Privacy Against Innovation or Against Discrimination?: The Case of the California Consumer Privacy Act (CCPA). *Telematics and Informatics*, *52*. DOI:10.1016/j.tele.2020.101431

Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS. *Computer Science & IT Research Journal*, *5*(3), Article 3. https://doi.org/10.51594/csitrj.v5i3.859

Barrett, C. (2019). Are the EU GDPR and the California CCPA Becoming the De facto Global Standards for Data Privacy and Protection?. *Scitech Lawyer; Chicago*, *15*(3), 24-29. *ARE THE EU GDPR AND THE CALIFORNIA CCPA BECOMING - ProQuest*. (n.d.). Retrieved April 5, 2024, from https://www.proquest.com/docview/2199825726?fromopenview=true&pq-origsite=gscholar&sourcetype=Scholarly%20Journals

Blood, T. (2019, January 14). PUBLIC FORUM OF THE DEPARTMENT OF JUSTICE CALIFORNIA CONSUMER PROTECTION ACT/CONSUMER PRIVACY ACT [Transcript]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-sd-011419.pdf

Brookman, J. (Consumer Reports). (2019, February 5). PUBLIC HEARING ON THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA) [Transcript]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-sac-020519.pdf

California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General. (2023, May 10). California Department of Justice. Retrieved October 27, 2023, from https://oag.ca.gov/privacy/ccpa

California Consumer Privacy Act of 2018, SB-1121, 2017-2018 Cong. (2018). *Bill Text—SB-1121 California Consumer Privacy Act of 2018.* (n.d.). Retrieved April 5, 2024, from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

California Privacy Legislation: A Timeline of Key Events - Future of Privacy Forum. (n.d.). *Https://Fpf.Org/*. Retrieved April 5, 2024, from https://fpf.org/blog/california-privacy-legislation-a-timeline-of-key-events/

Cohen, A. (2019, February 5). PUBLIC HEARING ON THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA) [Transcript]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-sac-020519.pdf

Corporate data responsibility: Bridging the consumer trust gap. (n.d.). KPMG. Retrieved April 5, 2024, from https://kpmg.com/us/en/articles/2023/bridging-the-trust-chasm.html

Golden Data Law. (2020, November 20). *Keeping track of CCPA amendments (2018–2020)*. Medium. https://medium.com/golden-data/keeping-track-of-ccpa-amendments-2018-2020-941dc7bf4653

Kammerer, S. (2019, March 8). [Comments on CCPA (APCIA)]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf

Kennedy, K. (2019, March 8). [Apple Inc Comments to the California Department of Justice re CCPA]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf

Khan, F. (2019, March 8). [CCPA Written Comments (Okta)]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf

Kozlowska, I. (2018, April 30). *Facebook and Data Privacy in the Age of Cambridge Analytica*. Jackson School of International Studies. Retrieved October 27, 2023, from https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/

Lee, J. (2019, February 13). PUBLIC FORUM OF THE DEPARTMENT OF JUSTICE CALIFORNIA CONSUMER PROTECTION ACT CONSUMER PRIVACY ACTS [Transcript]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-fresno-021319.pdf50. Public comments of ccpa

Luna, T. (2018, June 22). There's a deal to pull consumer privacy measure from the California ballot. *The Sacramento Bee*. https://www.sacbee.com/news/politics-government/capitol-alert/article213608964.html *CA consumer privacy deal could end ballot initiative | Sacramento Bee*. (n.d.). Retrieved April 5, 2024, from https://www.sacbee.com/news/politics-government/capitol-alert/article213608964.html

Mactaggart, A. (2018, November 9). [Developing the Administration's Approach to Consumer Privacy .] Retrieved from https://www.ntia.doc.gov/files/ntia/publications/11_9_18_ntia_rfc_californians_for_consumer_privacy_final_.pdf

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, *93*(5), 96-105.

Pantazis, C. (2019, February 8). [Google/CCPA]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf

Perumal, V. (2022). The Future of U.S. Data Privacy: Lessons from the GDPR and State Legislation Notes. *Notre Dame Journal of International & Comparative Law*, *12*(1), ii–123.

Pfeifle, S. (2018, June 28). *California passes landmark privacy legislation*. The Privacy Advisor. https://iapp.org/news/a/california-passes-landmark-privacy-legislation/

Pinch, T. J., & Bijker, W. E. (1984, August). The Social Construction of Facts and Artefacts: On How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science, 14*(3), 399–441. http://www.jstor.org/stable/285355

Ryan, J. (2019, March 8). [Comments on preliminary rulemaking for the California Consumer Privacy Act (Brave Software)]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf

Scow, A. (2019, March 8). [Consumer Watchdog Comments on CCPA]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf

Shapiro, M. (2019, March 8). [Response to Request for Comments for California Consumer Privacy Act (County of Santa Clara Privacy Office)]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Vollmer, A. R. (2019, March 8). [California Consumer Privacy Act (CCPA) rulemaking (GitHub)]. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

What is GDPR, the EU's new data protection law? (2018, November 7). GDPR.Eu. https://gdpr.eu/what-is-gdpr/

What is Privacy. (n.d.). IAPP. Retrieved April 5, 2024, from https://iapp.org/about/what-is-privacy/

Zaeem, R. N., & Barber, K. S. (2020). The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. *ACM Transactions on Management Information Systems*, *12*(1), 2:1-2:20. https://doi.org/10.1145/3389685