

A Social Analysis of the California Consumer Privacy Act

Michael Greene

Old Dominion University

CYSE 425W

March 19, 2023

## A Social Analysis of the California Consumer Privacy Act

The California Consumer Privacy Act or CCPA can be attributed to an increase in society's awareness of consumer privacy online within the United States. Before the enactment of the CCPA, there had been a limited amount of transparency between online organizations and consumers. Online organizations would often take the information obtained from consumers and sell it to third parties, often without the consumer's consent or knowledge. This information could be utilized in a variety of ways ranging from targeted marketing to possibly furthering a political agenda. The Cambridge Analytica incident which influenced the creation of the CCPA utilized consumer data for political advertising. Once the incident had been uncovered and brought to public attention, lawmakers in California attempted to appease the privacy concerns by introducing the CCPA. Through the combination of a platform with a massive user base and obtaining user information. The issue of privacy on the internet has come to the forefront in the United States. This analysis will examine the social factors that motivated the creation of the CCPA and the future societal implications of the CCPA.

The introduction of the internet changed society by bringing individuals from across the world closer to one another. In this modern age, society has increasingly grown more dependent on the internet by interacting with others on social media, consuming entertainment, and purchasing goods. What once required extensive effort can now be accomplished from the comfort of a person's own home. With this increase in online usage, many within society have become complacent when handling their information. The excessive number of requests made by each site, combined with the information requested often viewed by the consumer as insignificant has reinforced complacent online habits. Consumers have a higher probability of foregoing security to prioritize convenience (Saquella, 2020). Take for example the social media

platform Facebook, a platform for users to connect and share information. Although the information most users share on this platform may not initially appear to have any significant value, organizations are capable of piecing together this seemingly insignificant information to create their profile for a user. This information could be valuable for third-party organizations wanting to appeal to individual users. By having ads tailored to individual users, some may simply interpret this as another convenience provided by the site. However, in 2018 it would be discovered that the political data firm Cambridge Analytica would use this information and platform to influence the 2016 presidential campaign increasing awareness for privacy online.

During the 2016 presidential campaigns, social media platforms became an appealing target to reach a massive audience. Cambridge Analytica would be discovered to have information on millions of Facebook users, utilizing this information in favor of Presidential candidate Donald Trump (Alpert, 2020). By targeting specific users based on information they obtained through Facebook, Cambridge Analytica would be able to encourage users to vote for Donald Trump. Not only would they be capable of influencing individual users, but those within the user's network of close family and friends. The incident resulted in a loss of trust in Facebook and brought attention to the market of selling and purchasing user data with third-party entities. Legislators in California responded by unanimously passing the CCPA in June 2018 to give California residents more transparency, control, and protection over their data (Alpert, 2020). Having a culture heavily dependent on the internet such as the United States, the response to the incident in creating the CCPA can be justifiable. However, upon further examination, some may wonder why it took so long for a society with such a massive internet culture to begin protecting users' privacy.

In Europe, the regulation governing user data is referred to as the European General Data Protection Regulation or GDPR and existed before the introduction of the CCPA. This regulation gives consumers more protection and authority over their data similar to the CCPA (Illman & Temple, 2020). However, the GDPR was introduced in response to growing concerns over user privacy in general, as opposed to the CCPA which was introduced in response to an incident. It's concerning for some that a nation with a prominent internet culture would be behind other countries in implementing protections for online consumers. One theory could be attributed to the influence of American culture. Americans are often viewed as advocates of freedom, especially when it comes to freedom of speech. Organizations could argue that they have a right to the first amendment granting freedom of speech. Since the information obtained on users may qualify as publicly available information, they have the right to disclose user information to other parties (Saquella, 2020) With many major tech companies headquartered within the United States, the fear of these companies leaving in response to harsher regulations is a possibility. Another theory could be attributed to society's increasing complacency as mentioned before. Until an incident affecting a large number occurs such as the Cambridge Analytica incident, it appears the majority will continue to choose security over convenience. Regardless, the response by California legislators to enact regulations governing consumer privacy in the future is promising.

With an ever-increasing society adopting the Internet, the concern for consumer privacy will continue to expand well into the future. In its haste to provide consumers with some amount of protection, the CCPA admittedly will need to be continuously amended to keep up with technology and new trends. As a result, in 2020 the California Privacy Rights Act was introduced expanding upon the CCPA. The CPRA adds to the CCPA more control for the

consumer by allowing users to correct inaccurate information and limit the disclosure of user information to organizations (Shatz & Lysobey, 2022). This amendment demonstrates a need for constant reevaluation of regulations protecting society from abuses of technology. As new technology emerges such as wearable tech, the threat to society's privacy will only continue to grow.

In summation, due to the increasing prominence of the internet in society's everyday life. Society runs the risk of becoming complacent, and a culture prioritizing convenience is beginning to emerge. Social media encourages society to relinquish privacy by giving users a platform to share information with others. The CCPA provides California consumers with a means of protecting their privacy and holding organizations responsible. Just as the GDPR inspired the development of the CCPA. Hopefully, the CCPA can inspire states or even the federal government to take measures in regulating consumer data online. However, these regulations are only as effective as the society it is intended to protect. It is ultimately up to each individual to ensure that their respective information is protected and that organizations are held responsible for violating a person's privacy.

## References

Alpert, D. (2020). BEYOND REQUEST-AND-RESPOND. *Columbia Law Review*, 120(5), 1215-1254. [https://odu-primo.hosted.exlibrisgroup.com/permalink/f1ucqpjv/TN\\_cdi\\_proquest\\_journals\\_2435125344](https://odu-primo.hosted.exlibrisgroup.com/permalink/f1ucqpjv/TN_cdi_proquest_journals_2435125344)

Illman, E., & Temple, P. (2020). California Consumer Privacy Act: What Companies Need to Know. *The Business Lawyer*, 75(1), 1637-1646.  
<http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/california-consumer-privacy-act-what-companies/docview/2350105509/se-2>

Saquella, A. (2020). Personal Data Vulnerability: Constitutional Issues with the California Consumer Privacy Act. *Jurimetrics* (Chicago, Ill.), 60(2), 215-245. [https://odu-primo.hosted.exlibrisgroup.com/permalink/f1ucqpjv/TN\\_cdi\\_proquest\\_journals\\_2426140307](https://odu-primo.hosted.exlibrisgroup.com/permalink/f1ucqpjv/TN_cdi_proquest_journals_2426140307)

Shatz, S., & Lysobey, P. (2022). Update on the California Consumer Privacy Act and Other States' Actions. *The Business Lawyer*, 77(2), 539-547. [https://odu-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN\\_cdi\\_proquest\\_reports\\_2791357392&context=PC&vid=01ODU\\_NUI&lang=en\\_US&search\\_scope=Everything&adaptor=primo\\_central\\_multiple\\_fe&tab=everything&query=any,contains,Update%20on%20the%20California%20Consumer%20Privacy%20Act%20and%20Other%20States%27%20Actions&offset=0](https://odu-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_cdi_proquest_reports_2791357392&context=PC&vid=01ODU_NUI&lang=en_US&search_scope=Everything&adaptor=primo_central_multiple_fe&tab=everything&query=any,contains,Update%20on%20the%20California%20Consumer%20Privacy%20Act%20and%20Other%20States%27%20Actions&offset=0)