UC Law SF International Law Review

Volume 47 | Number 2 Article 5

6-2024

CCPA/CPRA: Consumers Bear the Burden as Companies Bear the Crown

Jacklin Lee

CCPA/CPRA: Consumers Bear the Burden as Companies Bear the Crown

JACKLIN LEE*

Abstract

Examining the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) is important for understanding United States privacy law. They were pioneering legislation in that the CCPA was one of the first comprehensive state-level privacy laws in the United States when it was enacted in 2018, introducing new rights for California residents regarding their personal information and imposed obligations on businesses handling data. The CPRA, passed in 2020, builds upon CCPA and further enhances privacy protections. These laws have served as models for subsequent privacy legislation at both the state and federal levels. They embody key principles that shed insight into the fundamental concepts and values that underpin privacy regulation in the United States. However, there are some inadequacies that are lacking compared to other policies such as Europe's General Data Protection Regulation (GDPR). This paper suggests that these shortcomings can be addressed by enhancing transparency to consumers and empowering consumers.

*Jacklin Lee obtained her J.D. from the University of California College of the Law San Francisco and is pursuing corporate tax law. She received her B.A. in International Studies from University of California San Diego and also holds M.A. in International Finance.

TABLE OF CONTENTS

Introduction

The California Consumer Privacy Act (CCPA) is a trailblazer for consumer privacy law in the United States because it is the first comprehensive privacy law. It allows consumers in California to find out what information a covered business is holding about them and to opt out of transfers and sales of their personal information.1 More recently in 2020, the Consumer Privacy Rights Act (CPRA), also known as Proposition 24, is a ballot measure passed by California voters that has become operative as of January 2023 that expands and modifies privacy rights to supplement the CCPA.

The CCPA and CPRA are more comprehensive and thorough than most other privacy laws that have been enacted in the United States. There are pros and cons to the CCPA that have become apparent during the few years since its enactment. Subsequently, The CPRA addresses many of the issues that have arisen as technology continues to develop and people begin to

1. Cal. Consumer Priv. Act, 105 Op. Cal. Att'y s Gen. 111 (2022).

realize the value of data privacy in the wake of incidents like the Cambridge Analytica scandal.

The CCPA and CPRA amendments provide a robust stand against flagrant and uninhibited yet surreptitious use or abuse of consumers' personal information by Big Tech companies for economic gains. Personal information goes beyond just secrets or a single right. Because it is multifaceted, the CCPA and CPRA's duties and roles become more complex. There is no doubt that the CCPA is a pioneering piece of legislation and had a seismic impact in the United States. The CCPA is not only comprehensive but also strict compared to other laws in the United States.

In fact, other states such as Colorado, Connecticut, Iowa, Virginia, and Utah have followed or are following suit in enacting their own comprehensive consumer privacy laws. Further, the CCPA and CPRA are not only relevant in California. The effects are on a national and international scale as it affects any company who does business with consumers in California. With the Bay Area being the hub of technology and business, the CCPA and CPRA are bound to be in the spotlight. CCPA protects California consumers and applies to businesses outside of California if they collect or sell any personally-identifiable information (PII) of California residents or conduct business in the state. The protection of consumer privacy in the United States is important, which is all the more reason why the shortcomings of the current CCPA and CPRA should be promptly recognized, discussed, and addressed. This paper asserts that the CCPA or CPRA is inadequate in its current form in providing vigorous privacy protection because it does not address the lack of knowledge of and meaningful choice by consumers.

Section I discusses the background of GDPR, CCPA, and CPRA, including the roots and history of the aforementioned privacy laws and how they are implemented today. Section II first addresses the shortcomings of how personal information is generally dealt with in the United States, especially with rapidly evolving development of technology. Second, Section II also surveys the background and inadequacies of the CCPA, CPRA, and the Notice and Choice regime. Section III dives into a possible solution of empowering the consumer with adequate knowledge to remedy the shortcomings of California privacy laws. Specifically, this section proposes informing consumers about the parties that are tracking their personal data and changing the roles and stances of privacy officers in companies. Section IV suggests empowering consumers with real choices as currently they are not equipped with such a luxury. Some starting points would be to change the fundamental default settings and to switch from the

current opt-out regime in the CPRA to an opt-in regime more like in the GDPR.

I. Geneses

Considering the origins of the European GDPR and the American CCPA or CPRA, it should be no surprise that they are on diverging paths. They are two remarkably different privacy laws with consequent social effects. From the beginning, the two approaches were destined to take different trajectories. The birth of the GDPR was a phenomenon that had been snowballing for years before. There was history, a sense of urgency, and a holistic recognition that played into factors – factors that are largely absent in America. The Californian laws, which are the most comprehensive set of privacy laws in the U.S., are still dominantly commercial. To more fully grasp the implications of the CCPA and CPRA, it is important to understand the fundamental differences and limitations compared to more powerful privacy laws such as the GDPR.

A. General Data Protection Regulation (GDPR)

The General Data Protection Regulation or GDPR of Europe has austere penalties and fines in the case of breaches, which is one of the reasons it was a global wake-up call. For severe violations of the law, businesses can be fined up to 20 million euros or 4% of their global turnover of the preceding fiscal year, whichever is higher.[2] Even for less severe violations, the fines can be the higher of 10 million euros or 2% of the business's entire global turnover of the preceding fiscal year.[3] For large conglomerates, a whole group can be considered an undertaking, and its total worldwide annual turnover can be used to calculate the fine for a breach.[4] As a result, the cost of fines can be astronomical for bigger companies. The gravity of these consequences is a deliberate move rooting from recognizing the grim past of German history and experiences with personal data being used to commit human rights atrocities. The stimulus for the stringent GDPR can be traced back to World War II when the Nazis would systemically use private data to

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 83(5), 2016 O.J. (L 119) [hereinafter GDPR].

3. *Id*. at art. 83(4).

4. *Id*.; *Id.* at art. 83(5).

identify Jews.[5] Nazi census workers would knock door to door with punch cards forcing residents to identify their nationalities, native language, religion, and profession.[6] Even after the war, state surveillance was still rampant in East Germany especially with its secret police force, Stasi, who would screen mail, search and bug homes, torture citizens, and keep files on everything, including personal relationships and sexual habits.[7] In 1970, West Germany enacted the first modern data privacy law as a response followed by the Federal Data Protection Act in 1977 to protect people "against abuse in the storage, transmission, modification and deletion."[8] In 1983, the Federal Constitutional Court ruled that intrusive census questions were wrong and declared the right of "self-determination over personal data as a fundamental right," which became the cornerstone of the GDPR principles.[9] In a way, the GDPR is a trauma response to the state control of private data and information. This historical background naturally elicited more cooperation by the people. The reason and consequences of the GDPR are steadfast and clear.

B. CCPA & CPRA

a. General Overview

The California Consumer Privacy Act (CCPA), which was introduced in January 2018 and signed into law in June of 2018, is the first comprehensive privacy legislation in the United States which aims to give more control to consumers regarding their personal information.[10] It affects businesses that: have revenues of $25 million or more, process personal information of at least 50,000 consumers, or earn at least half of their revenue by selling personal information.[11] The California Office of the Attorney General enforces the CCPA.[12] Consumer rights under the CCPA include the right to know, the right to access information about themselves, the right to

5. Olivia B. Waxman, *The GDPR is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History*, TIME (May 24, 2018), https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/.

6. *Id*.

7. *Id*.

8. *Id*.

9. *Id*.

10. Shreya, *CCPA vs CPRA: What Has Changed?*, COOKIE LAW INFO (Nov. 11, 2022), https://www.cookielawinfo.com/ccpa-vs-cpra/.

11. *Id*.

12. CAL. CIV. CODE § 1798.155 (2020) (amended 2023).

delete, the right to data portability consumers can request a business to transfer data to another business, the right to not be discriminated against, and the right to opt out of the sale of personal information.[13] The California Privacy Rights Act (CPRA) is a ballot initiative that aims to amend and upgrade the CCPA, and it went into effect in January of 2023.[14] Under the CPRA, the enforcement authority is not the Attorney General's office but rather the California Privacy Protection Agency.[15] The scope has changed from the CCPA in that instead of the 50,000 consumer information processing threshold, businesses now must adhere to the CPRA if they process personal information of more than 100,000 consumers.[16] The concept of "sensitive personal information" was introduced as a distinguished category.[17] More rights were added as well including the right to rectify, the right to limit the use of sensitive personal information, the right to opt out of automated decision-making and profiling, and a private right of action.[18]

b. Behind the Scenes

The focus of the CCPA is undeniably commercial. The corporate entity is more of a villain in America that creeps behind us and steals our information rather than the government such as with the GDPR and Nazi Germany. One of the major purposes and benefits of the CCPA was to level the playing field between businesses and consumers to make financial transactions and the economy burgeon.[19] Before the CCPA, businesses held hegemonic power because they could collect information without consent and consumers were left vulnerable without any privacy protections or bargaining power.[20] The CCPA facilitated a more balanced and equal power dynamic by giving consumers leverage over their own information.[21] These efforts to shift to a more equal power dynamic came after legislators realized that businesses' dealings with information can become problematic if not

13. Shreya, *supra* note 10.

14. *Id*.

15. CAL. CIV. CODE § 1798.155 (effective Jan. 1, 2023).

16. *Id.* § 1798.140(d)(1)(B).

17. *Id*. (ae).

18. *Id*. §§ 1798.120-121.

19. Don Wisdom, *What is CCPA Compliance and Why It Is Important in 2023*, DATALINK NETWORKS (Feb. 8. 2023), https://www.datalinknetworks.net/dln_blog/what-is-ccpa-compliance-and-why-it-is-important-in-2023.

20. *Id*.

21. *Id*.

catastrophic if left unregulated. A pivotal moment for privacy law in the U.S. was the Cambridge Analytica fiasco where consumers were shocked to discover that tens of millions of Facebook users' personal information was accessed covertly.[22] Shortly after in 2018, a comprehensive privacy law was proposed in California when San Francisco real estate developer Alastair Mactaggart teamed up with former CIA analyst Mary Ross and finance industry executive Rick Arney to raise awareness and gather voter signatures for a ballot measure that would give California residents more protection and control over their data and allow them to request their personal information from businesses.[23] Not surprisingly, this ballot measure was met with great resistance from businesses. Silicon Valley companies opposed the ballot measure for being "too broad and unworkable."[24] Companies such as Facebook, Google, AT&T, Verizon, and Comcast contributed $200,000 in the opposing movement against the measure.[25] Mactaggart and advocates eventually withdrew their proposal and agreed to take one step back and negotiate, resulting in a legislation that placed the California attorney general as the channel of enforcement in a shambolic compromise.[26] The California State Legislature passed the law, AB 375, in 2018 known as the CCPA.[27]

Even after the CCPA was passed, however, opponents such as technology and business lobbyists immediately worked to dilute the CCPA by proposing new bills. This shed light on a new concern that CCPA protections could be undermined by the opposing forces. This issue raised a flag for the need to embed these data protections in state law. Mactaggart again led the effort for Proposition 24 that would prohibit legislators from weakening the CCPA and give people more control over how tech companies use their personal information.[28] Proposition 24 was a desperate

22. Betsy Reed, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, THE GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

23. John Myers & Jazmine Ulloa, *California lawmakers agree to new consumer privacy rules that would avert showdown on the November ballot*, L.A. TIMES (June 21, 2018), https://www.latimes.com/politics/la-pol-ca-privacy-initiative-legislature-agreement-20180621-story.html.

24. *Id*.

25. *Id*.

26. *Id*.

27. Dustin Gardiner, *Fight to change California's landmark consumer privacy law fizzles – for now*, S.F. CHRON. (July 21, 2019), https://www.sfchronicle.com/politics/article/Fight-to-change-California-s-landmark-consumer-14111032.php.

28. Dustin Gardiner, *California's Proposition 24 would protect data-privacy law from being weakened in Legislature*, S.F. CHRON. (Sept. 20, 2020), https://www.sfchronicle.com/politics/article/California-s-Proposition-24-would-protect-15582105.php.

struggle to help privacy protections survive as it was a matter of time before the tech and business Goliaths would use their money and power to immobilize privacy laws into becoming moot. Proposition 24, or the California Privacy Rights Act was approved by voters through the ballot measure on November 3, 2020, and became operative on January 1, 2023.[29] Whereas the CCPA was a bill passed as a state statute by the California legislature, the CPRA was a ballot measure voted by the Californians. This means that unlike the CCPA, the CPRA cannot be repealed by the California legislature.[30] This embedment is exactly what Mactaggart was aiming for and is consequently a significant progress towards robustness of privacy laws in CA.

Nevertheless, the CPRA is still inadequate in meaningfully and thoroughly protecting consumers' data privacy. The different origin stories of the GDPR and CCPA/CPRA suggest that the lawmakers must reexamine the CPRA's fundamental principles and policies, noting the aspects of the GDPR that are more enhanced and effective than with the CCPA/CPRA. Neither the GDPR nor CCPA/CPRA are perfect, but recognizing some of the shortcomings and possible remedies seems to be the appropriate first step. Because the U.S. does not have the historical backdrop and sense of urgency stemming from Nazi trauma, its best impetus and incentive for privacy law is commercial. The opponent is not the government, a player above in a vertical hierarchy, but the business, a player that is supposedly horizontally on equal fields as the consumers in a symbiotic relationship. That paved the way for great reliance on the notice and choice regime. Consumers are led to believe they are in equal standing with the business and that they can exercise meaningful consent and choice when it comes to releasing personal information to these companies. Scholars such as Ari Ezra Waldman, Professor of Law and Computer Science at Northeastern University, take it to issue the fundamental regime of notice and choice. Their arguments are valid in that there are many limitations to the notice and choice regime that call for a new approach altogether. While a radical change might be ideal, it is not realistic due to the funds, already-implemented systems, and the sheer time it would take to become reality.

29. Peter Hegel, Sundeep Kapur & Claire Blakey, *The California Privacy Rights Act (CPRA) Has Been Enacted into Law*, PAUL HASTINGS (Nov. 6, 2020), https://www.paulhastings.com/insights/ph-privacy/blog-the-california-privacy-rights-act-cpra-has-been-enacted-into-law.

30. *Id*.

II. Inadequacies

A. Personal Information in America

To thoroughly analyze the CCPA and CPRA, it is also important to grasp the fundamentals of privacy to better know what legislators should aim for. Privacy laws should serve to deter and remedy the wrongs that accompany wrongful disclosures of identifying information.

Personal information in the United States is heavily linked to identification. That is why it is oftentimes referred to as "personally identifiable information" or PII. PII becomes relevant mostly only where information reveals facts about a person.[31] This exclusive focus on identification does not fully convey the spectrum of potential privacy harms largely because there is an array of modern privacy concerns regarding manipulation and autonomy that are not captured by reducing personal data to that which identifies the data subject. Under most American privacy statutes, privacy violations can only occur when PII is improperly collected or used.[32] American privacy law generally regulates the collection, processing, and disclosure of PII, while leaving non-PII generally unprotected.[33] American privacy statutes fail to offer a uniform definition of personal data.[34]

That is not to say that privacy laws are just a newly emerging trend in America. They have come a long way in the United States, with the CCPA and CPRA being the peak moment. The Federal Privacy Act of 1974 controlled the government's handling and disclosing of PII.[35] The strictest privacy law today that rivals the CCPA/CPRA is probably HIPAA (Health Insurance Portability and Accountability Act), created in 1996, which aims to protect personally identifiable information maintained by healthcare and health insurance companies. Another federal privacy act, the Children's Online Privacy Protection Act (COPPA), specifically protects information of children under 13 years of age and their safety in online activities.[36] The

31. Maria L. Montagnani & Mark Vertraete, *What Makes Data Personal?*, 56 U.C. DAVIS L. REV. 1165, 1190 (2023).

32. *Id*. at 1188.

33. *Id*.

34. *Id*.

35. Camille Fischer, *EFF Amicus Brief: The Privacy Act Requires the FBI to Delete Files of Its Internet Speech Surveillance*, ELEC. FRONTIER FOUND. (Aug. 9, 2018), https://www.eff.org/deeplinks/2018/08/eff-amicus-brief-privacy-act-requires-fbi-delete-files-its-internet-speech.

36. *Id*.

Gramm Leach Bliley Act (GLBA) is a federal law implemented and enforced by the Federal Trade Commission that requires financial institutions to disclose how they share and protect private customers' information. The first Chief Privacy Officer (CPO) was introduced in 1999 at an internet technology firm AllAdvantage with the hiring of privacy lawyer Ray Everett. The GDPR was introduced in Europe in 2018, and the CCPA went into effect in 2020.[37]

There are different laws, but they are mostly all specific to a particular sector. CCPA/CPRA is the first comprehensive set of laws in America that triggers the reconsideration of the concept of personal information. While privacy laws should certainly consider the potential harm that comes from disclosures of private information, an exclusive focus on these types of privacy wrongs is incomplete. There is a whole aspect beyond just protection that is overlooked. "The concerns of privacy are more capacious than safeguarding private information. It's a social reflection of ideals of autonomy and freedom that transcends mere protection of private or commercial information."[38]

B. California Consumer Privacy Act (CCPA)

One of the inadequacies of the CCPA is that the heavy burden of compliance falls on the individual consumers. The current system, which relies on the consumers to request information and for businesses to respond to these requests, places the burden on the consumers to be more proactive and take initiative while companies wait to react. Naturally, companies are more reluctant to take preemptive actions, and as a result, this system is not effective in transforming corporate data practices. It is not fair to dump that burden onto consumers because frankly, there will never be strong enough motive for corporations to proactively prioritize privacy over profit.

Of course, there are some duties for businesses. First, a business must provide notice of what categories of personal information it will collect about the consumer and of the purposes for which that information will be used.[39] This notice must be provided at or before the point at which the business collects information from the consumer. If the business sells personal information, then the notice at collection must include a "Do Not Sell My Personal Information" option that allows consumers to opt out of the sale of

37. *Id*.

38. *See* Fischer, *supra* note 35.

39. CAL. CIV. CODE § 1798.100(b)-(c) (2020) (amended 2023).

their personal information.[40] Privacy policies must inform consumers of their rights to know, to delete, to opt out, and not to be discriminated against.[41] Businesses have a duty to respond to verifiable consumer requests within 45 to 90 days.[42] However, they are not obligated to respond to more than two requests for personal data by an individual consumer in a year.[43] If a business is unable to comply completely with a request, it is still obliged to provide as much information as it can. There is no private enforcement mechanism or right of action for a violation of a data access obligation.[44] Instead, the California Attorney General must first notify a business of its noncompliance and give it thirty days to cure a violation.[45]

Data is an important economic asset to companies.[46] Consumer data is coveted by companies, and consumers have instinctively grown more uneasy about how data is handled. B However, there seems to be a threshold on how to access information that companies hold. According to a survey, more than 90% of respondents felt that consumers had lost control over how companies use their data.[47] It is difficult petition against a Big Tech company when consumers don't even know how and which companies surreptitiously took our information. Consumers likely opt in or out or check a box without reading the notification. They do not give much thought when they are in a hurry to download an app or access a website and there is a pop-up. Consumers simply click and forget. While consumers may remember to request their data from Facebook, they may not know or remember to also request their data from their cell service provider who is selling their real-time location data to companies who, in turn, resell it to bounty hunters.[48] It is unfair for companies to know this and rely on this to excuse themselves from the burden and liability.

---

40. *Id.* § 1798.135(a)(1).

41. *Id.* §§ 1798.110(b), 1798.120(b), 1798.125(a)(1).

42. *Id.* §§ 1798.130(a), 1798.145(i)(1).

43. *Id*. § 1798.100(d).

44. CAL. CIV. CODE § 1798.150(c).

45. *Id.* § 1798.155(b).

46. Alexis C. Madrigal, *How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $1,200*, THE ATLANTIC (Mar. 19, 2012), https://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730/.

47. Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RSCH. CTR. (Nov. 12, 2014), https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/.

48. Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, THE MOTHERBOARD (Jan. 8, 2019, 9:08 AM), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

C. California Privacy Rights Act (CPRA)

The CPRA expanded consumer rights but also imposed a substantive obligation on businesses to collect, process, use, and retain personal information in a manner consistent with the principles of data minimization, purpose limitation, and storage limitation. It also created the California Privacy Protection Agency (CPPA) as the enforcing agency. [49]

Despite the progressive changes implemented in the CPRA, the major problem of transparency and consumers' limitations to know what kind of sensitive personal information has been collected or inferred still remains a challenge. The CCPA and CPRA purposefully give consumers a right to receive inferences, regardless of whether the inferences were generated internally by the responding business or obtained by the responding business from another source. The caveat is that its information is subject to disclosure on request. How would a consumer know whether a profile has been created, and if it has been, how extensive the inferences are? Do consumers have to regularly request this information from all companies and websites they go through, randomly poking around? This seems like an inefficient, impractical, and unrealistic process. Consumers are the ones who need to research perpetually to protect themselves.

The CPRA, though a step forward from the CCPA, is still far from perfect. It failed to dismantle the "pay for privacy" schemes which allow businesses to offer financial incentives when consumers agree to give up their data, still uses the opt-out model as opposed to the opt-in model, focuses on the businesses' purposes rather than consumers' expectations and intentions, and expands businesses' power to refuse consumers' request to deletion of data if it is to "ensure security and integrity."[50] There is no one solution to the interwoven issues present in the current privacy laws, but this paper argues that some of these issues in the CPRA specifically can be addressed by two methods – empowering consumers with knowledge and real choice.

D. Notice and Choice

Scholars point out that there is a fundamental error in the current notice and choice (also known as notice and consent) regime that the American

49. CAL. CIV. CODE § 1798.199.10.

50. Lee Tien, Adam Schwartz & Hayley Tsukayama, *Why EFF Doesn't Support California Proposition 24*, ELEC. FRONTIER FOUND. (July 29, 2020), https://www.eff.org/deeplinks/2020/07/why-eff-doesnt-support-cal-prop-24.

privacy laws including the CCPA and CPRA rely on. Ari Ezra Waldman, professor of Law and Computer Science at Northeastern University, pointed out the pessimistic destiny to failure by the current structures and systems of privacy law and regulations. Meaningful consent is a manifestation of a consumer's knowledge and subsequent choices.[51] To achieve this goal, an individual should be able to exercise control over personal information through rational disclosure decisions based on evidence.[52] However, the foundational flaws, according to Waldman, are inherent in the current notice and choice regime which lacks meaningful consent and relies on a compliance-based procedure, which means that corporate actors themselves shape the practices ultimately favoring profit over meaningful protection. Waldman argues that the "compliance procedures are easily opted to achieve corporate goals [and] legitimizes data extraction."[53] Waldman asserts that the only way to truly achieve privacy is through a radical departure from the compliance-based notice and choice regime.

Consumers are too vulnerable. They don't have much power, and the companies shamelessly rely on the consumers' lack of knowledge. Waldman points out that Mark Zuckerberg mentioned giving users more control 53 times during his 2018 testimony before the U.S. Senate.[54] Ostensibly, this sounds legitimate, but shows that Zuckerberg does not feel threatened by giving consumers more control. Companies do not doubt that "control" to consumers is futile under the current system where people do not have the knowledge to make rational decisions where finance and convenience incentives would sway them into giving up their information anyway.[55] In fact, advocating for more "control" to consumers is a frivolous way of shifting the burden on to the consumer. Waldman proposes "radical" changes that redistribute power away from the companies and dismantle the notice and choice system.[56]

This paper agrees with Waldman's view that there are many fallacies that root from foundational errors. However, this paper also asserts that the

---

51. Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617, 641 (2021).

52. Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 129, 151 (2018).

53. Bill Echikson & Grace Endrud, *Europe's Grand Privacy Experiment Gets a Gentleman's C*, CTR. FOR EUR. POL'Y ANALYSIS (June 17, 2022), https://cepa.org/article/europes-grand-privacy-experiment-gets-a-gentlemans-c/.

54. Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 733, 812 (2020).

55. *Id.* at 811.

56. Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CAL. L. REV. 1221, 1276 (2022).

CCPA and CPRA give us some valuable takeaways. Addressing some of the specific negatives of the CCPA may place consumers in a better position than before and help privacy law in California and the U.S. advance. When proposing changes and improvement to the CCPA/CPRA, the United States does not have a collective trauma of Nazi genocide or state surveillance to the degree of Europe that triggered the GDPR without much resistance. This means that the United States must depend on a different force, and that is likely commercial. Second, although many scholars point out the shortcomings of the notice and choice regime, and however deficient it is, there is not a better alternative. This paper suggests that the CPRA can be improved if we go back to the basics and troubleshoot some building blocks to ensure more meaningful consent. Generally, this can be achieved by two ways, first, empowering the consumers with knowledge, and second, empowering the consumers with a real, non-illusory choice.

III. Empower with Knowledge

One of the major issues with the CCPA and CPRA is that the lack of transparency inhibits consumers from full utilization of the intended privacy protections. The playing field is skewed towards the businesses, since they have much more information about the data than the owner of the data themselves, causing an asymmetry. The most pressing solution to this lingering problem of information asymmetry would be enabling consumers to know the sources that are collecting, using, or sharing their information. Businesses have a great deal of funds and resources. There is pronounced information asymmetry between businesses and consumers in the online arena because consumers are left in the dark regarding businesses practices and handling of personal data.[57] Informed consent is the "process by which a fully informed user participates in decisions about his or her personal data."[58] The elements of informed consent are disclosure, competence, comprehension, voluntariness, and agreement.[59] None of these elements are fully or meaningfully achieved when there is a lack of transparency. Sometimes, it is difficult to even find out whether a company holds one's personal information because companies intentionally make accessing one's data convoluted and tedious. If we inspect the two Big Tech companies

57. Masooda Bashir, Carol Hayes, April D. Lambert & Jay P. Kesan, *Online Privacy and Informed Consent: The Dilemma of Information Asymmetry*, 52 PROC. ASS'N INFO. SCI. & TECH. 1, 1 (2016), https://asistdl.onlinelibrary.wiley.com/doi/epdf/10.1002/pra2.2015.145052010043.

58. *Id*. at 2.

59. *Id*.

Apple and Facebook, a consumer is able to access their data by first logging in to the online service, navigating to the data portal, and downloading their personal data from the settings.[60] According to trials by scholars, it took a whopping four days to download personal data on Apple.[61] It is not an exaggeration to say that this four day process itself is a deterrent for consumers and widens the gap between the consumer and business' information. On Facebook, the process is equally egregious as the consumer must rummage through twenty-four folders before accessing the information.[62] Basically, a consumer would be likely to find this information only if they knew what they were searching for and exactly where to look for it.[63] This is blatant elitism taking advantage of the disinformation of the layperson. Only people who are educated in the fields of privacy or technology would understand the meaning of privacy policy implications, the consequences of data sharing, and how to even request businesses for their information. It is woeful that even then, information about third-party advertisers to which Facebook shared information with is unavailable.[64] The lack of transparency leaves consumers blind to the fate of their own personal information.

A. Tracking the Trackers

The first practical way to remediate the lack of transparency is to equip users with information about who is tracking them. "Tracking" by websites and companies allows the storage of user activity on a website whenever they visit the site, and the information is relayed to either the company that hosts the website or may be shared to third parties. Tracking occurs through "cookies" which are small pieces of data that are created during a visit of a website, much like a trail. The site can transfer the data to different parties, and the data consist of information about the user's interaction with the website. Two different types of cookies exist. The first type is the first-party cookies that are created by the website, and the second type is the third-party cookies which are created by advertisers and other websites, such as through social media plugins or web analytics tools. Through these cookies,

60. Zach Whittaker, *How to Download Your Data from Apple*, TECHCRUNCH (Oct. 17, 2018), https://techcrunch.com/2018/10/17/how-to-download-your-apple-data/.

61. David Alpert, *Beyond Request-and-Respond: Why Data Access Will Be Insufficient to Tame Big Tech*, 120 COLUM. L. REV. 1215, 1233 (2020).

62. *Id*.

63. *Id*.

64. *Id*.

companies can track users' activities across websites and devices, and with more visits and cookies accumulate more information about the user.[65]

Under the current CCPA and CPRA, consumers often do not even know what kind of information the businesses are collecting. The CCPA requires consent to collect cookies if the data include personal information, such as unique personal identifiers that can track the user over time and across different services.[66] All third-party cookies fall under the umbrella of personal information and some first-party cookies do as well, but it is more ambiguous and determined on a case-by-case basis.

The CPRA enables the consumer to know the categories of personal information collected about the consumer in the preceding twelve months.[67] How the information was collected is undisclosed to the consumer. The methods by which businesses collect personal information is not a mandated disclosure provision. "For example, a business may simply disclose that it collects information about which websites a consumer visits but fail to disclose whether it collects this information by examining packet headers or by collecting DNS (domain name system) queries. The latter information about the method used could have informed a consumer about whether adopting a different DNS provider would change the collection of personal information."[68]

Disclosing the more specific source and the methods by which businesses have collected would be the first big step towards transparency. The source is important because as in the DNS example, it empowers consumers with a real choice. Knowing the source of data collection can provide consumers with the knowledge of when and where their information was collected and even weigh alternatives. We know this is technically feasible because the GDPR already requires a controller that collects personal data to disclose the source of origination and whether the source was public or not.[69]

The disclosure of the third parties that possess a user's data should be mandatory. CPRA only requires the disclosure of categories of the recipients that businesses share information with. Without knowing whether

65. Cynthia J. Cole, Travis Wofford & Katherine Burgess, *Tracking the Trackers: Cookies Are Subject to Opt-In Under GDPR and a Sale Under the CCPA*, CPO MAG. (Aug. 26, 2020), https://www.cpomagazine.com/data-protection/tracking-the-trackers-cookies-are-subject-to-opt-in-under-gdpr-and-a-sale-under-the-ccpa/.

66. *Id*.

67. Scott Jordan, *Strengths and Weaknesses of Notice and Consent Requirements under the GDPR, the CCPA/CPRA, and the FCC Broadband Privacy Order*, CARDOZO ARTS & ENT. L.J. 1, 18 (2021).

68. *Id*.

69. *Id*.

information was shared with a third party or not, it is difficult for consumers to exercise ownership of their own personal information. Once a piece of information is injected into one business, that information is left free to wander anywhere without the knowledge of the consumer. Sharing information with one party should not equate to sharing information with the whole world, yet the CCPA and CPRA enable exactly this result, leaving the owner of information vulnerable and stripped of control power. It might be alleviating if the consumer can at least know for what purpose the information is being shared for. The CPRA does require a business to disclose in the privacy policy the business or commercial purpose for selling personal information.[70] However, the sheer lack of detail is almost tantamount to useless. If, for example, a business shared both the address and browsing history, separately disclosing that it shares personal information both for advertising and to improve insurance rate-setting, the "separate disclosures fail to indicate whether the business shares your browsing history for advertising or for insurance rate-setting" which would have very different results and implications that had the consumer known, would affect their choice-making.[71] Disclosure of parties that have tracked and acquired data of users would exponentially increase transparency and effectiveness of the CPRA.

B. Privacy Officers

A second way to promote transparency and empower consumers with substantive knowledge is to appoint more privacy officers that can assume the role of informants to both the businesses and consumers. Privacy officers are not required in California. Neither the CCPA nor the CPRA has a provision that mandates privacy officers for businesses. Even if businesses do have privacy officers, currently, many in-house counsel lawyers or chief privacy officers (CPOs) work exclusively for the interest of companies. These individuals have different nuances in roles and responsibilities compared to a Data Protection Officer (DPO) in Europe. The European Union requires businesses to appoint a DPO as of May 2018.[72] Although similar to the privacy officers in America in that DPOs also mainly strive for compliance, there are other duties that set them apart. DPOs are able to promote transparency because they are not solely affiliated with the company

70. CAL. CIV. CODE § 1798.110(b).

71. Jordan, *supra* note 67, at 19.

72. *Data Protection Officer (DPO)*, EUR. DATA PROT. SUPERVISOR, https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en (last visited Apr. 11, 2024).

and are rather like liaisons between different interest parties. The EU has many formal instruments that ensure the independence of the DPO such as Data Protection Coordinators, investigatory power invested by the EU, and terms and strict conditions for appointment.[73] To date, an estimated 500,000 organizations have registered DPOs across the EU.[74] On the other hand, not only is there no such provision in the CCPA or CPRA, there is no general requirement in appointing a formal data security or privacy officer in any part of the United States aside from HIPAA.[75] The use of data protection or privacy officers should become more widespread, if not embedded in the CCPA or CPRA, because these officers can exercise independent judgment and stand on the side of consumers as well. They can be facilitators of transparency just as in Europe.

The simple appointment of privacy officers, however, is not enough. If the privacy officers are simply another appendage to the corporate entity, they would serve no great good to the consumers' interests. Waldman points out that currently, companies simply hire privacy officers as a symbol of compliance without consideration for the substance.[76] He asserts that comprehensive privacy programs and privacy officers are merely symbolic because their duties are broad and vague.[77] In fact, sometimes their roles can erode to becoming even harmful because as affiliates of the company, they contribute to the managerialization of privacy law by describing privacy as a compliance-based checklist that they make up for themselves.[78] Companies assign privacy officers to protect themselves from liability with vague, unspecific language to maximize their objectionable practices and profits.[79] The wrongfully misplaced focus on records and documentations as opposed to substantive goal of consumer privacy protection is a practice that is not just neutral, but harmful to the consumers.[80] When companies immediately excuse themselves from liability by pointing to their "compliance" demonstrated by the assessments and internal documents, consumers are dissuaded from mobilizing their rights and investigative powers no matter

73. *See Data Protection Officer (DPO, supra* note 72.

74. Caitlin Fennessy, *Study: An estimated 500K organizations have registered DPOs across Europe*, INT'L ASS'N OF PRIV. PRO. (May 16, 2019), https://iapp.org/news/a/study-an-estimated-500k-organizations-have-registered-dpos-across-europe/.

75. *Data Protection Officers — United States*, DLA PIPER (Jan. 29, 2023), https://www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=US.

76. Waldman, *supra* note 54, at 776.

77. *Id*.

78. Waldman, *supra* note 56, at 1232.

79. Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE L. REV. 307, 380 (2020).

80. Waldman, *supra* note 54, at 814.

how real the privacy problems were.[81] The stances of the privacy officers need to change.

Since we know the limitations of the current privacy officer roles, their positions and duties can be altered to be less allied with the businesses, taking on a more neutral role. For starters, CPRA can implement policies modeled after the DPO requirements in the GDPR. California can also have the instruments that ensure the independence of the privacy officers such as not being solely affiliated to the company, having investigatory power, and having strict terms and conditions for appointment. Current privacy officers in California only exist to make sure companies' financial risks are contained through compliance and serve no bigger role aside from that. The CPRA currently doesn't remedy this problem and should reconsider including an approach which allows privacy programs and officers to go beyond the "aesthetics" of law by focusing on the achievement of the affirmative goal of consumer protection rather than avoidance of a problem.[82] Implementation of an actor with a role similar to an ombudsman that can take on a more intermediary and neutral role would be helpful in empowering people with knowledge.

IV. Empower with Choice

Businesses are also oddly taking a back seat in the CCPA and CPRA, and the ball is in the consumer's court to request, deny, or delete information. This asymmetry is augmented by the lack of knowledge by the consumers. Notice and choice regimes place the burden of data governance on individual consumers who do not have the full capability or knowledge of privacy laws to make informed decisions.[83] Because businesses are the entities that have more information, it is only fair for them to be more proactive with informing controlling personal information. Presently, the businesses are in the default state of entitlement to personal information. It is an easy strategy for shifting the burden of privacy from the company who is at a better position to make intelligent and efficient privacy decisions, to the user, who is inevitably not.[84] During Facebook's motion to dismiss of hearing amidst Cambridge Analytica, the judge questioned Facebook about whether their invasion of privacy by sharing users' information with third parties was a violation of a reasonable expectation of privacy, to which their counsel responded that the

81. Waldman, *supra* note 54, at 814.
82. *Id*.
83. Bietti, *supra* note 79, at 396.
84. Waldman, *supra* note 54, at 811.

users evidently consented to giving up control of the data.[85] Google also claimed that the mere use of their search engine is sufficient to consent to the data collections.[86] Big Tech is grossly placing the burden on the consumers instead of taking the wheel in the front seat.

Moreover, the default state of opting in to collection of data unless one actively clicks the "opt-out" button is only advantageous to the business, and never to the consumer. Privacy in the US operates on opt-out regimes where data collection is presumed lawful unless individuals actively withdraw their consent.[87] This is grim because it means when a user clicks "Agree," on a website, they are not just granting access to a platform, but is partaking in a routinization and repetition of normalizing effects of making this phenomenon seem ordinary.[88] Also, the Non-discrimination prong of the California laws is impractical because people have accepted the fact that there are always financial advantages of giving up information to businesses. Further, one of the differences between the California laws and the GDPR is that the GDPR is more granular regarding requirements of the businesses yet more open-ended in terms of where responsibilities of those businesses end. The CPRA on the other hand is the opposite. It is akin to simply checking boxes. Waldman calls these no more than an "insubstantial privacy checklist."[89] The CCPA and CPRA should be more like the GDPR in that the privacy rules should not simply be a laundry list of minimums.

A. Foundations

Explicitly, there are two basic foundational differences – who the privacy laws apply to and what kind of information it applies to. A major difference between the two laws is that the CCPA and CPRA use the term "business" whereas the GDPR uses the term "controller." The term "controller" is broader and encompasses more entities beyond just a business or company. Therefore, the CCPA and CPRA do not apply to non-profits, governmental organizations, or other non-commercial entities. However, the GDPR applies to anyone and any entity that handles personal information of EU residents - business or not. Even starting from the actors to whom the set of laws apply to, there is a clear boundary between the CCPA and CPRA. In fact, it is very specific and applies to only one type of data controller – the

85. Waldman, *supra* note 56, at 1257.
86. *Id*.
87. *Id*.
88. *Id*.
89. Waldman, *supra* note 54, at 778.

business. The GDPR, however, refuses to contain the set of laws to a specific actor and makes it essentially boundless, applicable to anyone as long as they handle data.

The second foundational difference is regarding the type of information the laws apply to, or more specifically the type of information that is "exempt" from the bounds of the privacy law. One critical piece of difference that is often overlooked is the extent of exemption of "publicly available" information from the definition of "personal data" under the CCPA or CPRA. While many of the newer provisions in the CPRA are stricter compared to the CCPA, the definition of "publicly available" information that is exempt from the privacy laws became wider. Under the CCPA, only government records are exempt from the definition of "personal information" that is subject to the regulation.[90] This means that information retrieved from government records are "up for grabs" by companies. However, the CPRA expanded this definition to include information about a consumer that he/she made publicly available or disclosed to a third party if the consumer didn't.[91] So now, there are even more classes of information that are "up for grabs" by the companies. The GDPR, however, does not have such a provision for exemptions. It does not discriminate between public or private data. Even data that is obtained from public or government sources are included under the aegis of personal data and are subject to the same protection under the GDPR. The only small exception under the GDPR is "personal data which are manifestly made public by the data subject.[92] This huge exemption of the expansive category of "public" information is problematic. Just because an individual has given consent to a certain party at an earlier time does not mean it is free for all. Facebook in fact audaciously stated.[93] The district court judge[94] Businesses are brazen in avoiding liability and impudent in claiming it's fair game for them to use "publicly available" information however they want.

Third, the business-mandated collection and use of personal data are laxer for businesses in California. The standard for mandatory processing is lower for the CPRA compared to the GDPR. The CPRA allows mandatory processing if it is "reasonably necessary and proportionate" to the operational purpose while the GDPR allows mandatory processing only if it

90. Jordan, *supra* note 67, at 12.

91. *Id*.

92. *Id*.

93. *In re Facebook, Inc., Consumer Priv. User Profile Litig.,* 402 F. Supp. 3d 767, 782 (N.D. Cal. 2019).

94. *Id*.

is indubitably necessary.[95] The CPRA allows a business to mandate processing of personal information for the purpose of improving a service while the GDPR does not. Because these terms are written in the terms and conditions, many consumers overlook this. The problem with this is that while the minimum requirements and checkboxes are clear for the business, the power endowed to them in subjectively judging whether processing information is "mandatory" or not, or "reasonably necessary" or not, are limitless. This kind of ambiguous language is catch-all phrases that can become a loophole for businesses. If they deem something is "reasonably necessary," then it must be so, and consumers have no say or way to dispute this.

It is so easy for businesses in California to check off boxes by performing the minimum requirements clearly laid out in the CCPA or CPRA. All they have to do is stay within the four corners. The GDPR, by being more boundless in terms of responsibility of the data controller, essentially makes the default state more consumer-friendly and keep the businesses on their toes.

B. "Opt-Out" to "Opt-In"

One of the most prominent differences between the GDPR and the CCPA or CPRA is that in the GDPR, the default is to "opt out" of collection of data while under CCPA/CPRA, the default is to "opt in" unless one actively decides to "opt out." This single function under the CCPA/CPRA is not an accident nor is it insignificant. This single function reflects the immensely different ideals and fundamentals behind the GDPR and the CCPA/CPRA.

The GDPR requires that consent be specific and be "by a statement or by a clear affirmative action."[96] This is the difference in ideals between the two laws. The CPRA not requiring specific and affirmative consent takes advantage of the layperson who is uninformed. Consumers are not experts in privacy or the algorithm behind the data processing. people do not know the impact and implications of opting in or out. If the default is to be opted in, not many people are going to dispute that.

Not only are the average consumers untrained in privacy laws, it is quite impractical to opt out even if one were educated. In theory, people may seem free to opt out. It's a take-it-or-leave-it system. However, in many cases, there are not sufficient alternatives and "leaving it" is far too inconvenient.

95. *Id*.

96. GDPR, *supra* note 2, art. 4(11).

If ,say, a consumer has a cell phone, they must go off the grid in order to protect their privacy and their rights.[97] Helen Nissenbaum argues that people often do not have much of a choice but to agree to the collection: "While it may seem that individuals freely choose to pay the informational price, the price of not engaging socially, commercially, and financially may in fact be exacting enough to call into question how freely these choices are made." [98] Further, the cost of opting out is many times not worth it because the cost itself is inexact and unclear.[99] The decision to give up my information is made in a matter of seconds through a click of a button whether it be "opt out" or "opt in." The benefits of simply remaining to opt in lead to tangible gains, whether it be a discount that the business is offering or a subscription to a mailing list. The risks, however, are not immediate and hence easily forgotten, and also unclear. The cost is murky is undeterminable because the cost is in the future and the potential harms are inconceivable whereas the benefit is immediate, and decision-making happens fast.[100] People cannot spend considerable time contemplating it.[101] The "accept cookies" is clicked in a matter of seconds, and the opt-out regime optimally takes advantage of this exact phenomenon. These instantaneous benefits, as a collateral result, go so far as to have the effect of people trading in their personal data for a discount or convenience. This is also known as "pay-for-privacy" schemes where businesses are allowed to withhold discounts or require users to pay a premium unless they surrender their data.[102] Although the California privacy laws have a nondiscrimination clause, it is unclear and broad, and even under the CPRA pay-for-privacy schemes are not hampered.

To weigh the pros and cons of opting in versus opting out more accurately, consumers need additional information including information about the complex algorithms that shed light onto the flow of how our information will be processed, used, and shared. However, "the algorithm is far too complex for most lay people to understand."[103] Further, as this paper has established above, the information asymmetry and lack of transparency

97. Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law.*, 104 B.U. L. REV. 593, 608 (2023).

98. Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 35 (Sept. 29, 2011).

99. Solove, *supra* note 97, at 606.

100. *Id*.

101. *Id*.

102. Adam Schwartz, *The Payoff From California's "Data Dividend" Must Be Stronger Privacy Laws*, ELEC. FRONTIER FOUND. (Feb. 15, 2019), https://www.eff.org/deeplinks/2019/02/payoff-californias-data-dividend-must-be-stronger-privacy-laws.

103. Solove, *supra* note 97, at 621.

remains a big barrier. Consumers are not in a position with choice because they do not know or comprehend their choices. Consumers are basically choosing among options of "wildly speculative hunches or uninformed gut feelings."[104] People often cannot imagine what could go wrong. Choice exists when there is more than one viable option to choose from. "Individual choice becomes utterly meaningless as increasingly automated data collection leaves no opportunity for any real notice, much less individual consent."[105] The lack of knowledge by the lay consumer coupled with the opt-in default taking advantage of the passivity of human nature make the CPRA less effective than it could be compared to the GDPR.

V. Conclusion

The CCPA and CPRA are pivotal privacy policies in the United States that is so far the only equivalent we have to the GDPR. Despite its trailblazing and ambitious statutes, there are some inadequacies that are apparent from the GDPR during the three years it has been in effect. The CPRA is a more detailed and progressive set of amendments, yet the difference is not groundbreaking enough and fails to address the former shortcomings. The CCPA and CPRA are ineffective in its current form in providing robust privacy protection because it does not address the lack of knowledge of and meaningful choice by consumers. Some specific measures to rectify this would be by giving transparency to consumers on which parties are tracking their personal data and to change the roles and stances of the privacy officers in the companies. Another way is to empower consumers with real choices such as by changing the fundamental default settings and switching from the current opt-out regime in the CPRA to an opt-in regime more like in the GDPR. The CCPA and CPRA are works in progress and the need to address consumer empowerment with knowledge and real choices is imperative.

104. *Id*.

105. Cameron Kerry, *Why Protecting Privacy is a Losing Game Today – and How to Change the Game*, BROOKINGS (Apr. 15, 2022, 5:00 PM), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.