Loyola Consumer Law Review

Volume 32
Issue 2 *2020*

Article 3

2020

Privacy or Protection: The Catch-22 of the CCPA

Diane Y. Byun
dbyun@sandiego.edu

PRIVACY OR PROTECTION:

THE CATCH-22 OF THE CCPA

*Diane Y. Byun**

ABSTRACT

On June 28, 2018, the California Legislature passed the nation's strictest data privacy law, the California Consumer Privacy Act of 2018 ("CCPA"). Although effective January 1, 2019, the provisions of the CCPA did not become operative until January 1, 2020. The CCPA enforces compliance obligations on any business that collects covered personal information about California residents ("Consumers") and exceeds one of three thresholds: (i) annual gross revenues of $25 million, (ii) collection of personal information for commercial purpose of 50,000 or more covered consumers, or (iii) 50% or more annual revenue from selling Consumers' personal information. This low threshold demonstrates the incompatibility of the CCPA's language with its alleged mission of consumer protection.

This Comment discusses the catch-22 of the CCPA—consumer data privacy versus actual consumer protection—and suggests amendments to address this conflict. In its current state, the CCPA fails to protect the Consumer as a "complex consumer." Unlike "singular consumers"—those who purchase goods and services for personal use—complex consumers hold the simultaneous role of consumer and business-owner/business-employee. This Comment suggests the following amendments to help bridge the gap between privacy and protection: (1) Restrict the scope of applicability to exclude businesses with limited financial and/or personnel resources, i.e. small businesses; and (2) Narrow the definition of "personal information" to exclude purchasing histories or tendencies and inferences drawn from the CCPA's enumerated categories. The foregoing suggestions will

---

*J.D. University of San Diego School of Law, CIPP/US. Phone: (818) 970-2522. E-mail: dbyun@sandiego.edu. I would like to thank Professor Ted Sichelman of University of San Diego School of Law for his guidance on this Comment.

provide protection for complex Consumers, resulting in actual consumer protection, while maintaining the data privacy rights provided to the Consumer by the CCPA.

I. INTRODUCTION

On June 28, 2018, the California Legislature passed the California Consumer Privacy Act of 2018 ("CCPA"), establishing the strictest data privacy law in the United States.[1] California legislators acted quickly in passing the CCPA to deter a rigid anti-business voter initiative (titled "The California Consumer Right to Privacy Act of 2018")[2] from appearing on the November 2018 ballot.[3] Several provisions of the law were amended in both 2018[4] and 2019[5] based off

---

[1] Cal. Civ. Code Div. 3, Pt. 4, Tit. 1.81.5 (Deering 2018).

[2] The California Attorney General summarized the voter initiative organized by Californians for Consumer Privacy as follows: "Gives consumers right to learn categories of personal information that businesses collect, sell, or disclose about them, and to whom information is sold or disclosed. Gives consumers right to prevent businesses from selling or disclosing their personal information. Prohibits businesses from discriminating against consumers who exercise these rights. Allows consumers to sue businesses for security breaches of consumers' data, even if consumers cannot prove injury. Allows for enforcement by consumers, whistleblowers, or public agencies. Imposes civil penalties. Applies to online and brick-and-mortar businesses that meet specific criteria." *Available at* https://oag.ca.gov/system/files/initiatives/pdfs/Title%20and%20Summary%20%2817-0039%29_0.pdf.

[3] Under California law, eligible California voters can submit the text of a new law to the California Attorney general in order to bypass the legislative process. Advocates of the new law must obtain the required minimum number of signatures to have the proposed law added to the next general election's ballot. Cal. Elec. Code § 9000 et seq.

[4] California legislature passed SB 1121 on August 31, 2018 to revise several CCPA provisions which was chaptered on September 23, 2018 with amendments such as: (i) changes to effective and enforcement dates – clarifying the CCPA will go "into effect" immediately, but operative and enforceable on January 1, 2020; (ii) elimination of a notification requirement – eliminates a Consumer's duty to notify the Attorney General when pursuing a private action under the CCPA, but maintains that a Consumer must notify a business of any potential violations 30 days before initiating an action; and (iii) clarifications as to entities exempt from the CCPA – data handled pursuant to, and covered businesses subject to, certain laws (e.g. Gramm-Leach-Bliley Act, the Driver's Privacy Protection Act, and the California Financial Information Privacy Act) are not subject to the CCPA. *See* S. 1121, 2017-2018 Reg. Sess. (Cal. 2018).

[5] Before the legislative session for 2019 ended on September 13, the California legislature passed five amendments to the CCPA (AB 25, 874, 1146, and 1564) – all

comments from stakeholders before its operative date of January 1, 2020.

The CCPA enforces compliance obligations on covered businesses to implement significant changes in the policies and practices related to covered personal information about any natural California residents ("Consumers").[6] Similar to the extraterritorial reach of the European Union's General Data Protection Regulation ("GDPR"),[7] the CCPA's scope is not limited to entities within California. As the world's fifth largest economy,[8] California will see a significant impact in the marketplace due to the CCPA.[9] While data privacy advocates may see this as a win, it is important to note that consumer data privacy does not equate to actual consumer protection.

With its broad definitions of covered individuals, entities, data categories, and practices, the CCPA casts a wide net in an effort to protect Consumers through increased data privacy. However, these catch-all categorizations are counterintuitive to the CCPA's mission of consumer protection. For example, the CCPA's definition of "business" should be narrowed. Currently, a business entity is covered if it collects covered personal information about any Consumer and exceeds one of three thresholds: (i) annual gross revenues of $25 million, (ii) collection of personal information for commercial purpose of 50,000 or more covered consumers, or (iii) 50% or more annual

---

five of which were signed by Governor Gavin Newsom on October 11, 2019. The amendments are limited in scope, which means the CCPA remained largely intact on January 1, 2020. For details on the chaptered amendments, *see* Assemb. B. 25, 2019-2020 Reg. Sess. (Cal. 2019); Assemb. B. 874, 2019-2020 Reg. Sess. (Cal. 2019); Assemb. B. 1146, 2019-2020 Reg. Sess. (Cal. 2019); Assemb. B. 1564, 2019-2020 Reg. Sess. (Cal. 2019).

[6] *See* note 18.

[7] Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive 95/46/EC, 2016 O.J. L 119/1 [hereinafter "General Data Protection Regulation" or "GDPR"].

[8] Thomas Fuller, *The Pleasure and Pain of Being California, the World's 5th-Largest Economy*, N.Y. TIMES (May 7, 2018), https://www.nytimes.com/2018/05/07/us/california-economy-growth.html.

[9] *See* Forbes Technology Council, *How Will California's Consumer Privacy Law Impact the Data Privacy Landscape?*, FORBES (Aug. 20, 2018) https://www.forbes.com/sites/forbestechcouncil/2018/08/20/how-will-californias-consumer-privacy-law-impact-the-data-privacy-landscape/#6aeae802e922 (Thirteen members of Forbes' Technology Council ("FTC")—an invitation-only, fee-based organization comprised of elite CIOs, CTOs and technology executives—weighs in on how the CCPA will affect the larger data landscape) [hereinafter "FTC 2018"].

revenue from selling Consumers' personal information.[10] This low threshold ensnares more than just the data giants[11] that inspired this stringent law.[12] Consequently, businesses with limited resources ("small businesses") are further disadvantaged in the marketplace due to costs associated with compliance.[13] This overly broad approach continues as the CCPA defines "personal information" (also known as "personal data").[14] While there are eleven enumerated data categories, the CCPA's specific inclusion of "purchasing or consuming histories or tendencies" and "inferences drawn" from any of its enumerated categories presents another hurdle for complex consumers, especially small businesses.[15]

The CCPA's failure to consider the "dual consumer-business identity" presents a catch-22: consumer data privacy versus actual consumer protection. In its current state, the CCPA fails to consider the Consumer as a "complex consumer." Unlike "singular consumers"—those who purchase goods and services for personal use—complex consumers hold the simultaneous role of consumer and business-owner/business-employee. Consumers who fall under the CCPA's definition of "business" will be harmed due to increased litigation liability, vulnerability to steep fines, and additional costs

---

[10] *See infra* Part I.A.2.

[11] The legislature stated: "In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the internet. As a result, our desire for privacy controls and transparency in data practices is heightened." Assemb. B. 375§2(g), 2017-2018 Reg. Sess. (Cal. 2018).

[12] *See* Danny Allan, *California's New Data Privacy Law Could Begin a Regulatory Disaster,* FORTUNE (Oct. 23, 2018) https://fortune.com/2018/10/23/california-data-privacy-law-gdpr/, ("[T]hanks to some loose categorization of businesses to which the act applies, it has the potential to include not just organizations that sell individuals' data for financial gain, but also websites that collect IP addresses from millions of unique visitors per day").

[13] *See supra* note 7. *See also* Mario Farag, *Why Analytics Are So Important For Businesses In 2018,* DIGITALIST MAGAZINE (Feb. 12, 2018), https://www.digitalistmag.com/cio-knowledge/2018/02/12/why-analytics-are-so-important-for-businesses-in-2018-06164825, ("Small business leaders have often felt left behind by the growing acceptance of analytics, fearing that their workforce, customer base, or operations were too small to justify the cost").

[14] *See infra* Part I.A.3.

[15] *See generally* Martin Jones, *The importance of data for growing and driving small business,* Cox BLUE, https://www.coxblue.com/the-importance-of-data-for-growing-and-driving-small-business-social-media/.

associated with compliance obligations.[16] To truly protect consumers, the CCPA must be amended with consideration for the "dual consumer-business identity" and the reality of economic survival in a data-driven market. This Comment suggests the following amendments to help bridge the gap between privacy and protection: (1) Restrict the scope of applicability to exclude businesses with limited financial and/or personnel resources, i.e. small businesses;[17] and (2) Narrow the definition of "personal information" to exclude purchasing histories or tendencies and inferences drawn from the CCPA's enumerated categories.

This Comment examines the CCPA to identify provisions that harm the complex consumer and offers insight on how to remedy these harms. Part I begins by discussing the key terms and provisions of the CCPA, including its effects on existing data privacy laws. Part II then analyzes the federal government's proposed solution to consumer data privacy concerns. Part III discusses how the CCPA can achieve actual consumer protection by incorporating two amendments that take the complex consumer into consideration. Part IV provides a brief conclusion.

II. UNDERSTANDING THE CCPA

Understanding the CCPA and the flaws within its hastily drafted provisions will highlight the importance of addressing the dual consumer-business identity in future amendments.

A. Key Terms and Broad Definitions

1. "Consumer"

While other privacy laws often have a direct focus on information relating to specific individuals (e.g. employees, clients, children), the CCPA defines "consumer" broadly to include any

---

[16] *See* Allan 2018 *supra* note 10, ("In 2017 alone, over 1.9 billion files were leaked through security breaches. . . organizations mishandling data could be fined up to $7,500 for each violation. The financial impact to businesses could be enormous—and that doesn't even take into account the soft costs associated with loss of customer and employee confidence and damage to brand reputation").

[17] This Comment follows the legal definition of "small business" as determined by the U.S. Small Business Administration: "one which is independently owned and operated and which is not dominant in its field of operation." *See* Small Business Act, 15 U.S.C. § 632(a)(1) (1953).

natural California resident regardless of a business' relationship to the individual (e.g. employees, customers, vendors, persons associated with commercial customers who are California residents).[18] Unfortunately, it fails to address what constitutes a "household" and creates uncertainty regarding the CCPA's scope. The CCPA creates four significant data privacy rights for the Consumer:[19]

- Right to know what personal information a business has collected (annually and free of charge at the Consumer's request) and where (by category) that personal information came from or was sent.[20]

- Right to delete personal information that a business has collected from the Consumer. [21]

- Right to opt-out of the sale of Consumer personal information.[22]

- Right to receive equal service and pricing from a business upon exercising privacy rights under the CCPA, unless the difference is reasonably related to the value provided

---

[18] Cal. Civ. Code § 1798.140(g) (Deering 2018).

[19] It also includes the first mandatory "opt in" requirement in United States data privacy law, requiring an opt in prior to the sale of personal information relating to minors under the age of 16. *See* Cal. Civ. Code § 1798.120(c)-(d) (Deering 2018). Consumers between 13 and 16 years of age can provide affirmative authorization on their own behalf, but Consumers under 13 years of age can only opt in through the consent of a parent or guardian. *See* Cal. Civ. Code § 1798.120(d) (Deering 2018).

[20] *See* Cal. Civ. Code §§ 1798.100, 110, 115 (Deering 2018); *see also* § 1798.140(c) (defining "business") and § 1798.140(o) (defining "personal information").

[21] *See* Cal. Civ. Code § 1798.105 (Deering 2018). Note that the right-to-delete extends solely to personal information that a business collected *from* the Consumer while the right-to-know extends to *all* information a business has collected from the Consumer.

[22] *See* Cal. Civ. Code § 1798.120 (Deering 2018); *see also* § 1798.140(t) (defining "sale"). A Business is not required to comply to a request under section 1798.100 or 1798.105 if the Business cannot verify the Consumer making the request—based on the criteria in the draft regulations from the Attorney General. *See* Cal. Civ. Code. § 1798.140(y) (defining "verifiable consumer request"). *See also* CCPA Draft Regulations *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

to the Consumer – not to the Consumer – by the Consumer's data [23]

2. "Business"

The CCPA defines a covered "business" ("Business") as any for-profit business that collects personal information relating to Consumers, determines the purpose and means of processing that information, and either: (i) has an annual gross revenue of $25 million or more; (ii) collects, sells, or shares for commercial purposes the personal information of at least 50,000 Consumers, households or devices annually; or (iii) derives at least 50 percent of its annual revenues from selling Consumers' personal information.[24] Compliance obligations will be imposed on any business covered by the CCPA, regardless of legal residence in California.[25]

3. "Personal Information"

The CCPA broadly defines "personal information" as information (also known as "data") that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular Consumer or household, and includes name, alias, mailing address and IP address.[26] Notably,

---

[23] Cal. Civ. Code § 1798.125(a)(2); § 1798.125(b)(1) (Deering 2018).

[24] Cal. Civ. Code §§ 1798.140(c)(1)(A), 140(c)(1)(B), 140(c)(1)(C), 140(c)(2) (Deering 2018).

[25] Notably, the CCPA also applies to affiliated, co-branded entities of any businesses that meet the above criteria, whether or not the affiliate does business in California (e.g. shared name, service mark, or trademark). *See* Cal. Civ. Code. § 1798.140(c)(2).

[26] The CCPA enumerates eleven categories to demonstrate the broad scope of "personal information": (i) identifiers, such as a "unique personal identifier" and "online identifier Internet Protocol address"; (ii) "characteristics of protected classifications under California or federal law"; (iii) "commercial information," such as including records of products or services purchased and other purchasing or consuming histories or tendencies; (iv) biometric information, a defined term that means physiological, biological and behavioral characteristics and includes the traditional fingerprint and retinal scan but also keystroke and gait patterns as well as "sleep, health and exercise data that contain identifying information"; (v) "Internet or other electronic network activity information," such as browsing history or "interaction … with an advertisement"; (vi) geolocation data; (vii) audio, electronic, visual, thermal, olfactory or similar information; (viii) professional or employment-related information; (ix) education information unavailable to the public, as defined in the federal Family Educational Rights and Privacy Act; and (x) "inferences,"

personal information is not considered "publicly available" if the data was used for a purpose incompatible with the purpose for which the government maintained it has been deleted.[27] Consequently, information made legally available from federal, state, or local governments is not "personal information" under the CCPA.[28]

4. "Collect"

The CCPA defines the term "collect" as "buying, renting, gathering, obtaining, receiving, or accessing any personal information from the consumer, either actively, or passively, or by observing the consumer's behavior."[29] Just by accessing personal information (e.g. photos) from a Consumer device, a Business can risk liability. It is irrelevant to the CCPA whether the data is actually stored or retained by the Business because it has "collected" covered Consumer data.

5. "Sale"

The CCPA defines "sale" as providing personal information to both a business and third party, sharing personal information with entities meeting the "service provider" and/or third party exception brings that disclosure outside the scope of a "sale" for both the purpose of a business' disclosure obligations as well as Consumers' opt-out rights.[30]

This broad definition includes sharing or disclosing personal information "for monetary compensation or other valuable consideration" (emphasis added), resulting in heightened requirements for Businesses that sell Consumers' personal information. [31] For

---

defined as the "derivation of information ... assumptions, or conclusions from ... another source of information," derived from data drawn from personal information to create a profile about a Consumer's "preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." Cal. Civ. Code § 1798.140(o)(1).

[27] "Publicly available" does not include de-identified or aggregate consumer information. *See* Cal. Civ. Code § 1798.140(o)(2).

[28] *See Id.*

[29] Cal. Civ. Code § 1798.140(e).

[30] Cal. Civ. Code §1798.140(t).

[31] It is worth noting that a "sale" under the CCPA need not involve monetary compensation. While it is unclear how courts will interpret "valuable consideration," a court could potentially find that a violation took place if covered data is provided to a third party in exchange for predictive solicitation or interest-based marketing. Cal. Civ. Code § 1798.140(t)(1).

example, Businesses that sell information to third parties will need to provide a clear and conspicuous link on their webpage titled "Do Not Sell My Personal Information" that enables a Consumer to opt out of the sale of personal information as well as a toll-free telephone number.[32] Businesses must also include a description of the Consumer's right to opt out within their privacy policy, whether online or offline.[33] The anti-discrimination provision of the CCPA prohibits Businesses from discriminating against Consumers for exercising their CCPA rights.[34]

B. Exceptions & Exemptions for Certain Data Categories

The CCPA's exceptions for certain data use and processing may assist (or impede) in retaining specific data or limiting its use should a Consumer instruct a business to cease using the data. Consumers will have the right to delete their personal information in certain circumstances.[35] This means a Business must delete or cease to use "personal information" upon request unless one of the enumerated exceptions applies. Businesses must determine whether they must comply with the CCPA or whether an exception or partial exception applies.

1. Non-California Commercial Conduct

The CCPA will not restrict the collection or sale of Consumer information provided every aspect of the commercial conduct takes

---

[32] Businesses that exclusively operate online will not be required to provide a toll-free number if the company has a direct relationship with a consumer from whom it collects PI. For guidance on what qualifies as a "direct relationship," *see* AB 1202 *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1202.

[33] For purposes of verifying the identity of a Consumer making a CCPA request, a Business may require any reasonable authentication of Consumer identity with consideration of the nature of the data requested. Cal. Civ. Code § 1798.130(a)(2).

[34] This provision does allow, however, for Businesses to charge a Consumer a different amount or provide a different level or quality of goods or services if the difference is reasonably related to the value provided to the Business by the Consumer's personal information. Put simply, a Consumer who chooses to opt out of the sale of his or her personal information may receive different treatment based on the value the Business would have received from selling his or her data. *See* Cal. Civ. Code § 1798.125.

[35] *See supra* note 23.

place outside of California. This means that the data was collected while the Consumer was physically outside of the state and that no part of the sale occurred within California.

2. Collection and Disclosure for a Business Purpose

The CCPA allows a business to collect and disclose personal information if it is for a "business purpose"[36]—"the use of personal information for the business' or service provider's operational purposes, or other notified purposes, provided that the use of personal information is reasonably necessary and proportionate to achieve the operational purpose for which it was collected" (emphasis added).[37]

3. Aggregate or Anonymized Data

The CCPA provides it shall not restrict the collection, use, retention, or disclosure of aggregate or anonymized Consumer information, defined as data "not linked or reasonably linkable to any consumer or household, including via a device." Businesses are likely to attempt achieving this exception through technology capable of anonymizing information (e.g. software programs that combine information sets from various sources). To fall within this exception, a Business must implement technical safeguards and business practices that specifically prohibit re-identification and the inadvertent release of anonymized data. There must be no attempt to re-identify the aggregate or anonymized data. Due to the broad scope of "personal information" under the CCPA, Businesses should proceed with caution when considering the use of aggregate or anonymized data in compliance strategies.

4. Employee Data

"Employees" are provided a limited employee exemption for the first year of the CCPA's implementation, which gives the

[36] A business could deny a Consumer's request for deletion if the data is found necessary for the business to: Complete the transaction for which the data was collected; detect or protect against security incidents or illegal activity, or prosecute individuals responsible for illegal activity; identify and repair errors that impair intended functionality; exercise free speech or ensure the right of another to exercise free speech; comply with federal, state, or local laws and legal obligations; exercise or defend legal claims; engage in public or peer-reviewed research; or for internal purposes. Cal. Civ. Code § 1798.140(d).

[37] *Id.*

California legislature a one-year deadline to pass a separate privacy bill for employees.[38] Under the CCPA, "employees" include job applicants, employees, owners, directors, officers, medical staff, and independent contractors.[39] This exemption will cover personal information collected from those who qualify as employees under the CCPA, including emergency information and information regarding beneficiaries.[40] To qualify for this exemption, employees' personal information must be collected and solely used for employment purposes.[41] This leaves information that is received in any other context from a Consumer employee within the scope of the CCPA (i.e. whenever the Consumer employee otherwise interacts with the Business outside of the employment relationship). [42]

5. Business-to-Business Data

Until January 1, 2021, Businesses have an exemption for personal information collected in business-to-business transactions.[43] Data from such a transaction is exempt only when it reflects communications and transactions solely within the context of due diligence and situations where a product or service is provided or received between a Business and a Consumer, where the Consumer is acting as an "employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency."[44] Notably, this amendment does not seem to include information collected from cold-calling or other marketing communications.

---

[38] Cal. Civ. Code § 1798.145(h).

[39] Cal. Civ. Code § 1798.145(h)(1)(A).

[40] Cal. Civ. Code § 1798.145(h)(1)(B).

[41] For example, data collected in the course of a Consumer acting as a job applicant, employee, officer, director or contractor of a Business, but only to the extent that the Business uses such information in the context of the Consumer's role (or former role) as an applicant, employee, etc. *See* Cal. Civ. Code § 1798.145(h)(1)(C).

[42] This exemption does not remove the notice requirement under section 1798.100(b) and does not exempt employee data from consumer private right of action under section 1798.150. *See* Cal. Civ. Code §§ 1798.100(b); § 1798.150. Employers should still conduct the due diligence necessary to revise the employee privacy notices to include employees' right to request disclosure and deletion of information the Business collects outside the employment relationship.

[43] Cal. Civ. Code § 1798.145(n).

[44] *Id.*

6. Vehicle Information

Vehicle and ownership information can be shared between new motor vehicle dealers and the vehicle manufacturer if the information is shared "for the purpose of effectuating, or in anticipation of effectuation, a vehicle repair covered by a vehicle warranty or recall" and for no other purpose.[45]

C. Effects on Existing Data Privacy Laws

Many data privacy regulations already in place focus on specific categories of personal information. The CCPA does not provide detailed guidance on how it will fit in with existing data privacy laws but does include several clear exemptions for businesses already in compliance with certain laws.[46]

1. HIPAA and FCRA

The CCPA does not apply to health information governed by Health Insurance Portability and Accountability Act ("HIPAA")[47] nor does it affect the sale of information to or from a consumer reporting agency covered by the Fair Credit Reporting Act ("FCRA").[48]

2. Gramm-Leach-Bliley Act

The CCPA does not apply to nonpublic personal information pursuant to the Gramm-Leach-Bliley Act ("GLBA").[49] This exemption homes in on information, not entities, subject to or otherwise handled pursuant to the GLBA.[50] Thus, the exemption protection would only apply to nonpublic personal information about consumers by financial

---

[45] Cal. Civ. Code § 1798.145(g).

[46] *See supra* note 4.

[47] Health Insurance Portability and Accountability Act of 1996, Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996. *See* Cal. Civ. Code §§ 1798.145(c)(1)(A), (c)(1)(B) (Deering 2018).

[48] Fair Credit Reporting Act, 15 U.S.C. § 1681. *See* Cal. Civ. Code § 1798.145(d) (Deering 2018).

[49] The revised GLBA exemption eliminates the original requirement that it would apply only if the CCPA was in conflict with the GLBA (it would now apply even if there was no conflict). *See supra* note 4.

[50] Cal. Civ. Code § 1798.145(d) (Deering 2018).

institutions. Title V, Subtitle A of the GLBA[51] defines "nonpublic personal information" as any information that is not publicly available and that: (i) a consumer provides to a financial institution to obtain a financial product or service from the institution; (ii) results from a transaction between the consumer and the institution involving a financial product or service; or (iii) a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.[52]

3. Existing California Data Privacy Laws

In its current form, the CCPA does not directly address how it will affect or interact with California's existing privacy laws. California Civil Code section 1798.175 acts as a potential remedy for this absence prescribing that where conflict arises between California laws, the law that affords the greatest privacy protections shall control. California Civil Code section 1798.194 instructs courts that the new law "shall be liberally construed to effectuate its purposes."[53]

D. Enforcement and Penalties

1. Private Right of Action (Consumers)

The CCPA gives Consumers a private right of action against Businesses with respect to data security breaches.[54] Currently, a Consumer can only pursue a private action in the event that his or her unencrypted personal data is subject to unauthorized access, exfiltration, theft, or disclosure as a result of a covered business' violation of its duty to implement and maintain reasonable security

---

[51] Gramm-Leach-Bliley Act, Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999.

[52] Nonpublic personal information may include a consumer's name, address, phone number, social security number, income, credit score, and information obtained through Internet collection devices (i.e. cookies). *See* GLBA Title V, Subsection A, Sec. 509(4)(A).

[53] Cal. Civ. Code §1798.194.

[54] In an attempt to address the scope of the private right of action, SB-1121 states, in relevant part: "The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." Cal. Civ. Code § 1798.150(c) (Deering 2018).

measures.[55] For purposes of the private right of action, "personal information" is restricted to traditional identifiers included in California's data security statute (e.g. name, social security number, credit card information) rather than the broad definition used prevalently in the CCPA.

A Consumer does not have a duty to notify the Attorney General when pursuing a private action under the CCPA but must notify a business of any potential violations 30 days before initiating an action. Consumers can seek either statutory damages between $100 and $750 per incident or actual damages, whichever is greater.56 The CCPA provides the judiciary with a long list of considerations for determining the amount of statutory damages to award including, inter alia, "the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth."57 It

---

[55] Notably, California Attorney General Xavier Becerra expressed his support in protecting the singular consumer in a letter urging California legislature to expand the private right of action to allow Consumers to protect all of their CCPA's privacy-related rights: "Finally, the CCPA does not include a private right of action that would allow consumers to seek legal remedies for themselves to protect their privacy. Instead, the Act includes a provision that gives consumers a limited right to sue if they become a victim of a data breach. The lack of a private right of action, which would provide a critical adjunct to governmental enforcement, will substantially increase the [Attorney General's Office's] need for new enforcement resources. I urge you to provide consumers with a private right of action under the CCPA." *Available at* https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/08/ag-becerras-letter-re-california-consumer-privacy-act.pdf. Data privacy advocates are likely to push for this recommendation to be incorporated, but this would be a mistake in true consumer protection. Again, the focus here lies on the singular consumer rather than the complex. Should the Attorney General's recommendation actually see fruition, the CCPA will flood the courts with privacy-related lawsuits, taking up the judicial system's precious time and resources and further increasing liabilities for complex consumers. Privacy professionals must keep an eye on the California Privacy Rights Act ("CPRA") which has qualified for the November 2020 ballot. *See* CPRA, https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf. If the CPRA passes, it will become effective January 1, 2023 and move California's privacy framework closer to that of the GDPR. *See id.*

[56] Cal. Civ. Code § 1798.150(a)(1)(A) (Deering 2018). Further, a Consumer's ability to pursue statutory damages is in addition to seeking injunctive or declaratory relief. Cal. Civ. Code. § 1798.150(a)(1)(B)-(C).

[57] Cal. Civ. Code § 1798.150(a)(2).

is unclear whether the calculation of statutory damages will be based on a single data breach or the number of data breaches (and multiplied by) each impacted Consumer. Either method of calculation significantly increases a Business' liability for failure to maintain adequate security for Consumers' personal information.

2. Civil Actions (California Attorney General)

Civil penalties for violations of the CCPA will be exclusively assessed and recovered in civil actions brought by the California Attorney General.[58] Notably, the stringent statute considers arbitration clauses and class action waivers to be unenforceable and contrary to public policy. For actions commenced by the Attorney General, the CCPA allows imposition of penalties for intentional violations of any provision of the CCPA of up to $7,500 per intentional violation in cases of breach or violation of the CCPA not cured within 30 days after being notified of noncompliance.[59] While covered businesses will have an important right to cure alleged noncompliance, it remains unstated and untested what might constitute a cure.[60]

III. THE FEDERAL APPROACH: A CONSUMER PRIVACY BILL OF RIGHTS

The Consumer Privacy Bill of Rights is a term that describes the federal government's attempts to regulate how electronic personal data is processed within the U.S. These proposed "Privacy Bill of Rights" would manifest consumer data privacy as a fundamental American right. None of these proposed measures have become law. Most notable is the Obama administration's Consumer Privacy Bill of Rights Act of 2015. This set the tone amongst businesses and data privacy advocates as a disapproving one due to its lack of consideration for economic effects and inadequate consumer safeguards. In 2015, the White House drafted its own bill after the Obama administration's 2012 blueprint receive little interest: the Consumer Privacy Bill of

---

[58] The California Office of the Attorney General proposes to adopt sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations concerning the CCPA. *See* Proposed Text of Regulations *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

[59] Cal. Civ. Code § 1798.155(b).

[60] For further details on the Attorney General's enforcement of the CCPA, *see* CCPA Regulations *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.

Rights Act of 2015.[61] The bill was drafted with the intent to provide a set of conditions governing the processing of personal data. The bill included conditions that favored consumer protection including but not limited to the following stipulations: Process personal data in a manner consistent with the context in which consumers provided the data.[62] Allow consumers to opt out if personal data is used unreasonably for the context.[63] Delete and de-identify personal data in a reasonable amount of time. [64] Implement reasonable security for personal data. Develop a code of conduct for handling personal data (in some industries). [65] This bill was harshly criticized by both businesses and data privacy advocates.[66] Companies argued that the bill presented undue burdens, hindering corporate innovation, and less competition.[67] Privacy advocates argued the bill did not go far enough, expressing the concern that the bill would allow businesses to write their own rules rather than allowing the government the power to establish and enforce regulations. An additional point made by activists is that a federal law would undermine state laws that provided better protections. Even the Federal Trade Commission ("FTC") was concerned that the bill did not provide consumers with enforceable protections.[68]

The question of whether a national law would be better than a state data privacy regulation has come back into play with the CCPA. Given the harsh nature of the CCPA, one could argue that it should be eradicated, so the federal government can just have one overarching law. While that may be the case for some areas of law, each state should have the option to make its own data privacy law, within reason and as far as legally allowed, because of the state's interests in having a say on the business conducted within its borders. For example, although there is a federal minimum wage requirement, each state is

---

[61] Consumer Privacy Bill of Rights Act of 2015, *available at* https://www.congress.gov/bill/114th-congress/senate-bill/1158/text.

[62] *Id.* at 1.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *See* Brendan Sasso, *Obama's 'Privacy Bill of Rights' Gets Bashed from All Sides,* THE ATLANTIC (Feb. 27, 2015), https://www.theatlantic.com/politics/archive/2015/02/obamas-privacy-bill-of-rights-gets-bashed-from-all-sides/456576/.

[67] *Id.*

[68] James Denvil and Patrick Kane, *Insights on the Consumer Privacy Bill of Rights Act of 2015,* HOGAN LOVELLS (Mar. 3, 2015), https://www.hldataprotection.com/2015/03/articles/consumer-privacy/insights-on-the-consumer-privacy-bill-of-rights-act-of-2015/.

given the power to decide whether they would like to enact stricter ordinances within its borders. Additionally, each state has its own code that governs corporations, e.g. Delaware. A significant downside to the federal approach is the inability to provide a fair compliance threshold nationwide. For example, a compliance threshold provided for businesses covered by California are not going to be the same for states with less than thriving economies. It just isn't practical. Lastly, as evidenced by the slew of failed attempts by the federal legislature, e.g. Obama administration, CONSENT Act, the issue of regulating the processing of personal information is better left to the states because state laws provide stronger protections for its consumers.

IV. BRIDGING THE GAP: HOW TO PROTECT THE COMPLEX CONSUMER

To truly protect consumers, the CCPA must be amended with consideration for the dual consumer-business identity and the reality of economic survival in a data-driven market.[69]

A. Narrowing the Scope of Applicability

With its current scope of applicability, the CCPA harms the consumers it aims to protect by including small enterprises with limited resources in its definition of a Business. A particularly negative effect of focusing on the singular consumer is the likelihood of a decrease in corporate innovation in small businesses. Businesses with fewer resources will peter out, leaving only large businesses in the marketplace.[70] The dilemma of small businesses competing with

---

[69] Alexandro Pando, CEO of Xyrupt Technologies, expresses a view that seems to be in favor of the singular consumer: "Allowing people to opt out of having their information used for purposes they do not intend will bring new understanding and trust to tech companies." FTC 2018. One must question whether the benefit of gaining this "trust" outweighs the burdens and risks associated with CCPA compliance. If a covered business lacks the resources to comply with the CCPA, it is likely to fail, leaving only large businesses in the market. With him is Alan Price, CTO of VisionCritical.com: "As these transparency standards are backed by legislation, it's increasingly important for brands to remain honest with their customers if they want to retain their loyalty." *Id.* Again, this support for the singular consumer is coming from the perspective of someone who belongs to a business that has the necessary resources to not only comply with the CCPA, but also put costs toward strategizing how to survive in the new CCPA-regulated economy.

[70] Brent Chapman, CIO of RoundPoint Mortgage Servicing Corporation, succinctly articulates this concern: "[T]his increased regulatory compliance will

established entities has been an ongoing issue, as evidenced by the creation of the U.S. Small Business Administration.[71] To remedy this issue, the CCPA should amend the definition of "business" to exclude small businesses. The current definition of Business[72] creates such a broad scope of applicability that a business can be covered even if it is not an entity selling Personal Information for money. For example, a business can be covered by the CCPA if it engages in or generates income through interest-based marketing and has at least 50,000 unique Consumers visiting its website. The law can also apply to traditional brick-and-mortar institutions that conduct business in California. Thus, a small business with less than $25 million in revenue could become a Business by "collecting" an annual total of 50,000 unique Consumer credit card sales. The costs associated with increased liability are potential costs to a covered business, but a definite cost that must be made will be time, money, and labor spent on changing the infrastructure of one's business to achieve CCPA compliance. Although larger businesses will also feel the impact of the CCPA's financial burdens, they are better equipped to adapt and survive due to incumbent advantages such as established consumer brand loyalty and sufficient financial and personnel resources to comply with the CCPA's requirements. Small businesses either lack or simply do not have the resources available to compete with larger businesses without data.

---

begin to suffocate companies. And when companies suffocate, consumers suffer. Prices go up, jobs are lost and we could experience negative economic impact in those regions. . . The CCPA will only fuel the activist fire on how personal data is being handled, especially by the larger global internet companies. What will further escalate the cost and complexity of doing business in the U.S. is the compounded effect of having to manage consumer and data privacy in up to 50 varied ways across the 50 states." *Id.*

[71] In the Small Business Act of July 30, 1953, Congress created the Small Business Administration, whose function is to "aid, counsel, assist and protect, insofar as is possible, the interests of small business concerns." *See* Small Business Act, *available at* https://www.sba.gov/sites/default/files/2019-03/Small_Business_Act.pdf.

[72] *See* Cal. Civ. Code §§ 1798.140(c)(1)(A), 140(c)(1)(B), 140(c)(1)(C), 140(c)(2) (Deering 2018); *supra* note 22.

B. Excluding "Purchase Histories" and "Inferences Drawn"

Although not as comprehensive as the GDPR's definition,[73] the CCPA includes categories of personal information rarely expressly stated in US privacy laws such as "commercial information," including "purchasing or consuming histories or tendencies";[74] internet activity, such as browsing or search history or a consumer's "interaction" with a website, application, or advertisement; and "inferences drawn" from any of the CCPA's enumerated categories to "create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.".[75] Whether singular or complex, Consumers will be harmed by the conflicting interests of consumer expectations and data privacy concerns.[76] Gigya, a customer identity management provider, found that consumers have two consistently conflicting desires: more personalization and increased data protection.[77] While singular consumers will be grappling with not receiving goods and services that meet their personalized needs, complex consumers will suffer from trying to assess and meet consumer expectations with substantially less data.[78] Without the

---

[73] GDPR Article 1(1) defines personal data as any information "relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier."

[74] Cal. Civ. Code § 1798.140(o)(1)(D) (Deering 2018).

[75] Cal. Civ. Code § 1798.140(o)(1)(K) (Deering 2018).

[76] *See* Philip Kushmaro, *How Privacy and Personalization Intersect in Our Data-Filled World*, CIO IDG CONTRIBUTOR NETWORK (Nov. 30, 2016), https://www.cio.com/article/3145469/security/how-privacy-and-personalization-intersect-in-our-data-filled-world.html ("While consumers demand privacy, it's not likely they'll become long-term customers without some type of personalization").

[77] Gigya, *The 2015 State of Consumer Privacy & Personalization*, *available at* http://info.gigya.com/rs/672-YBF-078/images/Gigya_WP_2015PrivacyPersonalization%20(1).pdf

[78] *See Selligent Marketing Cloud Study Finds Consumer Expectations and Marketer Challenges are Rising in Tandem,* Selligent Marketing Cloud (Aug. 23, 2018), https://www.selligent.com/press/selligent-marketing-cloud-study-finds-consumer-expectations-and-marketer-challenges-are-rising-in-tandem ("Thirty-three percent of the respondents expect brands to anticipate needs before they arise and a whopping 70 percent agree that it's important that brands understand a consumer's individual situation (e.g. marital status, age, location, etc.) when they market to them and not just use every communication as a means to make a sale"). *See also* Kimberly Collins, *As Consumer Expectations Rise, Brands Find New Data to Personalize Experience,* CLICKZ (Sept. 17, 2018), https://www.clickz.com/as-consumer-expectations-rise-brands-find-new-data-to-personalize-

ability to track consumer responses or predict consumer expectations, it is nigh on impossible for a small business to compete with incumbents like Google or Facebook.[79] Thus, the CCPA should be amended to narrow the definition of "personal information" to exclude purchasing histories or tendencies and inferences drawn from the CCPA's enumerated categories to assist businesses, small and large, to address the demands of a consumer-driven market.

V. CONCLUSION

California has effectively set the stage for change in how Businesses engage with Consumers and personal information. Given the heavy stakes involved, Businesses will seek to make amendments, which are expected to provide some clarification and reasonableness to this sweeping legislation. While the proposed amendments address the issue of the CCPA's neglect for the complex consumer, it is by no means a cure-all. Regardless of the content of data privacy regulations, businesses must take it upon themselves to refrain from misuse of consumer information. Just as the CCPA must consider the dual consumer-business identity of Consumers, so must any business entity handling personal data.

---

experience/216842/ ("We have high expectations for personalized customer experience, yet are quite uncomfortable with sharing personal data that makes personalization possible"). *See For information on artificial intelligence and data privacy, see Emily Alford, In the Age of AI, Do Consumers Still Care About Privacy?,* CLICKZ (Aug. 2, 2018), https://www.clickz.com/in-the-age-of-ai-do-consumers-still-care-about-privacy/216162/.

[79] *See* Christina Donnelly, *Small Businesses Need Big Data, Too, Harvard Business Review (Dec. 5, 2013), https://hbr.org/2013/12/small-businesses-need-big-data-too ("Big Data threatens to create a deep divide between the have-datas and the have-no-datas, with big corporations gaining advantage by crunching the numbers and small firms left to stumble in the dark"); Christina Donnelly, Digital loyalty card 'big data' and small business marketing: Formal versus informal or complementary?, International Small Business Journal Vol. 33(4), 422-442 (2015), available at https://journals.sagepub.com/doi/pdf/10.1177/0266242613502691. See also Ginni Rometty, We need a new era of data responsibility, World Economic Forum Annual Meeting (Jan. 21, 2018), https://www.weforum.org/agenda/2018/01/new-era-data-responsibility. ("[O]nly 20% of the world's data is searchable — which means 80% of the data out there is sitting on private servers, most of them in businesses").*