

The California Consumer Privacy Act of 2018: A Sea Change in the Protection of California Consumers' Personal Information

By Sanford Shatz and Susan E. Chylik*

INTRODUCTION

Following a series of publicly disclosed data breaches, California citizens submitted a ballot proposition entitled the California Consumer Privacy Act of 2018.¹ Because ballot propositions are difficult to amend once adopted by the voters, California legislative and executive leaders reached an agreement with the ballot proposition's proponents that it would be withdrawn if a consumer privacy act became law by June 28, 2018. The proposed legislation was introduced and became law less than one week later on that date.²

The result was the nation's most far-reaching consumer protection privacy law: the California Consumer Privacy Act of 2018 ("CCPA").³ The CCPA granted Californians six new privacy rights concerning the collection and use of their personal information. The Act was intended to further Californians' constitutional right to privacy.⁴ Due to its hasty passage, the governor signed cleanup legislation in September 2018.⁵ The California legislature passed six bills to amend the CCPA at the end of its legislative session in September 2019 that remain under consideration by the governor as of this writing.⁶

* Sanford Shatz is of counsel at McGlinchey Stafford, LLP in Irvine, California. Susan E. Chylik is a member of McGlinchey Stafford, PLLC in Cleveland, Ohio.

1. See Press Release, Cal. Sec'y of State, Proposed Initiative Enters Circulation (Dec. 18, 2017), <https://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/proposed-initiative-enters-circulation39/>.

2. See CAL. CIV. CODE §§ 1798.100–.199 (added by Stats. 2018, ch. 735, § 17, effective Jan. 1, 2020) [hereinafter CCPA]; see also A.B. 375, 2017–18 Reg. Sess. (Cal. 2018) (approved by Governor June 28, 2018; filed with Secretary of State June 28, 2018), http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375.

3. CCPA, *supra* note 2.

4. CCPA, *supra* note 2, § 1798.175; see CAL. CONST. art. 1, § 1.

5. See S.B. 1121, 2017–18 Reg. Sess. (Cal. 2018) (amending Title 1.81.5 of the California Civil Code).

6. See A.B. 25, 2019–20 Reg. Sess. (Cal. 2019) [hereinafter A.B. 25]; A.B. 874, 2019–20 Reg. Sess. (Cal. 2019) [hereinafter A.B. 874]; A.B. 1146, 2019–20 Reg. Sess. (Cal. 2019) [hereinafter A.B. 1146]; A.B. 1202, 2019–20 Reg. Sess. (Cal. 2019) [hereinafter A.B. 1202]; A.B. 1355, 2019–20 Reg. Sess. (Cal. 2019) [hereinafter A.B. 1355]; A.B. 1564, 2019–20 Reg. Sess. (Cal. 2019) [hereinafter A.B. 1564]. If enacted, the proposals would amend the definition of personal information, A.B. 874, A.B. 1355; the Fair Credit Reporting Act ("FCRA") exemption, A.B. 25, A.B. 1146, A.B. 1355; the

This survey summarizes the CCPA's scope and requirements, describes how it affects consumers and businesses, discusses its enforcement provisions, and offers suggestions for implementation of its requirements.

THE SCOPE OF THE CCPA

The CCPA applies to “businesses” that collect “personal information” regarding “consumers.” The CCPA broadly defines “consumer” as a California resident⁷ who has lived in the state for at least six months and one day,⁸ regardless of where else the consumer has a home or resides. The statute is intended to be construed liberally to effectuate its purposes of protecting California citizens.⁹

The CCPA defines a “business” as a for-profit legal entity, regardless of corporate form, that collects consumers’ personal information directly or indirectly.¹⁰ To be covered by the CCPA, a business must meet one of three thresholds. The first is whether the business, in combination with its affiliates, has annual gross revenues in excess of \$25,000,000.¹¹ The statute does not state that the revenues must be earned in California or even in the United States. For example, a high-volume out-of-state lender that originated and serviced its own loans only in the state of origination would be covered by the CCPA with respect to one of its customers who had moved to California.

The second threshold is whether the business alone or in combination annually buys, receives for its commercial purposes, sells, or shares the personal information of 50,000 or more California consumers, households, or internet-connected devices.¹² Under this provision, a family with two children—each of whom has a mobile phone, a smart TV, and various internet-accessible games—could accrue ten to twenty units toward the 50,000 threshold.

The third threshold applies to businesses that derive 50 percent or more of their annual revenues from selling consumers’ personal information.¹³ This threshold, and the ballot proposition giving rise to the CCPA, sought to limit the impact of data collection by technology giants such as Google and Facebook, although the breadth of the Act caught many other companies in its grasp.¹⁴

employee exemption, A.B. 25, A.B. 1146, A.B. 1355; consumer verification, A.B. 25, A.B. 1355, A.B. 1564; and privacy and training, A.B. 25, A.B. 1355, A.B. 1564. Where the bills overlap or contain contradictory requirements, the last enacted provisions would become law.

7. CCPA, *supra* note 2, § 1798.140(g).

8. CAL. CODE REGS. tit. 18, § 17014 (2018).

9. CCPA, *supra* note 2, § 1798.194.

10. *Id.* § 1798.140(c)(1).

11. *Id.* § 1798.140(c)(1)(A).

12. *Id.* § 1798.140(c)(1)(B).

13. *Id.* § 1798.140(c)(1)(C).

14. See Ben Adler, *California Passes Strict Internet Privacy Law with Implications for the Rest of the Country*, NPR.ORG (June 29, 2018, 5:05 AM PT), <https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country>.

The CCPA defines “personal information”¹⁵ expansively to include anything that identifies a consumer, relates to or describes a consumer, or could be associated or linked with a consumer or with the consumer’s household.¹⁶ The Act offers various categories as examples of personal information, including personal identifiers, personal classifications, commercial and biometric information, geolocation data, professional or employment information, and inferences from that information.¹⁷

THE CCPA’S NEW CONSUMER RIGHTS AND PROTECTIONS

The CCPA gives California consumers six strong new privacy rights with respect to their personal information that businesses collect, and it imposes significant obligations on businesses that collect that personal information, including disclosure requirements and a duty to respond to certain consumer requests.

THE CONSUMER’S RIGHT TO POSSESS INFORMATION

Consumers have a new right to know the categories and specific pieces of personal information that businesses collect about them.¹⁸ Before collecting the information, a business must disclose the fact that it collects the consumer’s personal information, the categories of information that it collects, and the purposes for collecting that information.¹⁹ A business must not collect or use this information unless it provides the advance disclosure.²⁰ When a consumer makes a verifiable request for his or her personal information, the business must provide it within forty-five days and at no charge.²¹ It may provide the information by mail or electronically in a portable form that may be shared with others.²²

THE CONSUMER’S RIGHT TO BE FORGOTTEN

Consumers have a right to ask businesses to delete their personal information.²³ Businesses must disclose this right to consumers.²⁴ When a business receives a verifiable consumer request to delete information, the business must delete the information from its records and direct its service providers to do so as well.²⁵

However, there are several exceptions to the right to be forgotten. For example, a business or service provider may retain the consumer’s personal

15. CCPA, *supra* note 2, § 1798.140(o). “Personal information” excludes information that is “publicly available,” which generally means information that is lawfully made available from federal, state, or local government records. *Id.* § 1798.140(o)(2).

16. *Id.* § 1798.140(o)(1).

17. *Id.*

18. *Id.* § 1798.100(a).

19. *Id.* § 1798.100(b).

20. *Id.*

21. *Id.* § 1798.100(d).

22. *Id.*

23. *Id.* § 1798.105(a).

24. *Id.* § 1798.105(b).

25. *Id.* § 1798.105(c).

information to complete the consumer's transaction or maintain an ongoing business relationship, such as servicing a loan.²⁶

THE CONSUMER'S RIGHT TO KNOW WHAT

A business must disclose the categories of personal information it collects, the categories of sources from which it collects the information, the business or commercial purpose for collecting the information, the categories of third parties with whom the business shares the information, and the specific personal information collected when it receives a verifiable consumer request to do so.²⁷

THE CONSUMER'S RIGHT TO KNOW WHO

A business must disclose the categories of personal information it collected, the categories of information it sold, the categories of third parties to whom it sold the information, and the categories of information that it disclosed to third parties for a business purpose when it receives a verifiable consumer request for this information.²⁸ A business that buys personal information may not resell that information unless it provides explicit notice to the consumer and gives the consumer an opportunity to opt out of future sales.²⁹

THE CONSUMER'S RIGHT TO OPT OUT OR SAY NO

Consumers have the right to opt out of the sale of their personal information at any time.³⁰ A business that sells personal information must disclose that it does so and offer consumers the right to opt out.³¹ When a consumer is between thirteen and sixteen, the consumer or the consumer's parent or guardian must affirmatively opt in to the sale.³² If the consumer is under thirteen, only the parent or guardian may opt in.³³ Once a consumer opts out, the business may not sell the consumer's information unless the consumer later opts in.³⁴

THE CONSUMER'S RIGHT TO NONDISCRIMINATION

Consumers have a right to be treated fairly and equally if they exercise any of their rights under the CCPA.³⁵ For example, a business may not charge a higher price or provide inferior goods or services to consumers who have sought copies of their personal information or opted out of information selling.³⁶ Businesses

26. *Id.* § 1798.105(d).

27. *Id.* § 1798.110(a).

28. *Id.* § 1798.115(a)–(b).

29. *Id.* § 1798.115(d).

30. *Id.* § 1798.120(a).

31. *Id.* § 1798.120(b).

32. *Id.* § 1798.120(c).

33. *Id.*

34. *Id.* § 1798.120(d).

35. *Id.* § 1798.125(a)(1).

36. *Id.*

may charge a different price or rate or provide a different level or quality of goods or services to consumers if the difference is “reasonably related to the value provided to the consumer by the consumer’s data.”³⁷ It is unknown what this provision means. However, businesses may offer financial incentives by paying consumers for the use of their personal information.³⁸

THE CCPA’S NEW DUTIES AND OBLIGATIONS FOR BUSINESSES

The CCPA imposes many duties and obligations on businesses to ensure that consumers know and can exercise their rights. For example, a business must inform consumers that it collects their personal information before it does so,³⁹ and it must inform consumers of their right to ask the business to delete their personal information.⁴⁰ It must inform consumers of their right to request the categories of personal information collected, the categories of sources of that information, the purpose of the collection, and the categories of third parties with whom the information is shared.⁴¹ It also must inform consumers of their right to request the categories of information it sells and to whom or with whom it sells or shares that information.⁴² Finally, it must inform consumers of their right to opt out of the sale of their personal information.⁴³

In response to a verifiable consumer request, businesses must do several things, as applicable. They must provide consumers with the information they collected about them,⁴⁴ and they must delete the information upon request.⁴⁵ They must disclose the categories of personal information collected, the categories of sources of that information and its purpose, and the categories of third parties with whom the information is shared.⁴⁶ They must disclose the categories of personal information the business sold, the categories of third parties to whom the personal information was sold, and the categories of personal information that were shared with third parties in response to a verifiable consumer request.⁴⁷ They must also permit consumers to opt out of the sale of their personal information.⁴⁸

To permit consumers to exercise their rights, businesses are required to designate two or more methods by which consumers can contact them, including a toll-free number and a website address.⁴⁹ They must establish and maintain an

37. *Id.* § 1798.125(a)(2).

38. *Id.* § 1798.125(b).

39. *Id.* § 1798.100(b).

40. *Id.* § 1798.105(b).

41. *Id.* § 1798.110(a).

42. *Id.* § 1798.115(a).

43. *Id.* § 1798.120(a).

44. *Id.* § 1798.100(d).

45. *Id.* § 1798.105(c).

46. *Id.* § 1798.110(b).

47. *Id.* § 1798.115(b).

48. *Id.* § 1798.120(b).

49. *Id.* § 1798.130(a)(1).

online privacy policy listing California-specific privacy rights⁵⁰ and place a “do not sell my personal information” button on their home page.⁵¹ Businesses must also update their privacy policies to include California-specific requirements.⁵² If a business operates in many states, it may set up a “California” home page to which it directs its California customers and place all its California-specific disclosures there.⁵³ Thus, consumers from other states need not be informed of the California-specific rights or have the opportunity to attempt to exercise them. Businesses are required to train their employees on CCPA rights and how consumers can exercise them.⁵⁴

While the CCPA defines a “verifiable consumer request” as a request by a consumer verified by the business to be the person “about whom the business collected personal information,”⁵⁵ businesses may want to have different tests based on the request and the risk of turning over a consumer’s information to an unauthorized person. For example, if a consumer seeks to opt out of the sale of personal information, the business should have one set of standards to verify that the request came from that consumer. However, if a consumer seeks to obtain the categories of personal information and specific information collected by a business, the business should take every reasonable step to verify the consumer’s identity to avoid releasing all the consumer’s personal information⁵⁶ to a potential identity thief.

THE CCPA’S EXEMPTIONS AND EXCLUSIONS

The CCPA has several important exclusions and exemptions.⁵⁷ Businesses must comply with existing law and legal process.⁵⁸ They may disclose information to their service providers as long as they do not have “actual knowledge or reason to believe” that the service provider will act improperly.⁵⁹

With respect to financial services companies, the CCPA states that it does not “apply to the sale of personal information collected, processed, sold, or disclosed pursuant to the federal Gramm–Leach–Bliley Act” (“GLBA”) and its regulations or the California Financial Information Privacy Act.⁶⁰ However, it is difficult to determine the scope of this exception without the attorney general implementing regulations because no information is collected, processed, sold, or disclosed

50. *Id.* § 1798.130(a)(5).

51. *Id.* § 1798.135(a)(1).

52. *Id.* § 1798.135(a)(2).

53. *Id.* § 1798.135(b).

54. *Id.* §§ 1798.130(a)(6), 1798.135(a)(3).

55. *Id.* § 1798.140(y).

56. This includes the consumer’s social security number, account information, and other financial or personal information that could cause a consumer havoc if delivered improperly. *Id.* §§ 1798.100, 1798.140(o).

57. *Id.* § 1798.145.

58. *Id.* § 1798.145(a).

59. *Id.* § 1798.145(h).

60. *Id.* § 1798.145(e); see Pub. L. No. 106-102, tit. V, 113 Stat. 1338, 1436-43 (1999) (codified as amended at 15 U.S.C. §§ 6801-09 (2018)); CAL. FIN. CODE §§ 4050-60 (2018).

pursuant to the GLBA. This exemption does not apply with respect to the CCPA's data-breach provisions.⁶¹

CCPA DATA BREACH, ENFORCEMENT, AND REGULATION PROVISIONS

UNAUTHORIZED ACCESS OF PERSONAL INFORMATION

Under the CCPA, a business may be liable for a data breach if it fails to implement and maintain reasonable security procedures.⁶² The CCPA provides affected consumers with a private right of action, including the right to recover statutory damages between \$100 and \$750 per consumer per incident or actual damages, whichever are greater, plus injunctive relief and any other proper relief.⁶³ The consumer must give the business thirty days to cure before initiating an action for any uncured breach.⁶⁴ While no other private rights of action are granted by the CCPA,⁶⁵ California's unfair-competition law permits a consumer to use other laws such as the CCPA as a basis for an action for an injunction, restitution, and attorneys' fees.⁶⁶

ENFORCEMENT

The attorney general may bring an enforcement action for a violation of the CCPA after giving thirty days' notice and an opportunity to cure.⁶⁷ The attorney general may seek penalties of \$2,500 for each violation or \$7,500 for each intentional violation, plus an injunction against the business.⁶⁸ The attorney general cannot bring an enforcement action under the CCPA until the earlier of July 1, 2020, or six months after the publication of final regulations.⁶⁹

CCPA REGULATIONS

The CCPA requires the attorney general to solicit broad public participation to adopt regulations on or before July 1, 2020.⁷⁰ Those regulations must, among other things, address categories of personal information, the definitions of identifiers, exceptions to comply with other laws, rules for complying with the CCPA, and monetary-threshold adjustments.⁷¹ As of the date of this writing, the proposed regulations had not been published.

61. CCPA, *supra* note 2, § 1798.145(e); *see id.* § 1798.150.

62. *Id.* § 1798.150(a)(1).

63. *Id.*

64. *Id.* § 1798.150(b).

65. *Id.* § 1798.150(c).

66. CAL. BUS. & PROF. CODE § 17200 (2018).

67. CCPA, *supra* note 2, § 1798.155(b).

68. *Id.*

69. *Id.* § 1798.185(c).

70. *Id.* § 1798.185(a).

71. *Id.* § 1798.185(a)(1)–(5).

PREPARING FOR THE CCPA

The provisions of the CCPA discussed above, which became effective on January 1, 2020,⁷² suggest a number of steps that businesses should take to prepare for it. Businesses should determine what personal information they collect and store about consumers and where they store that information. Information may be stored on central servers, cloud servers, individual desktops, separate files maintained by loan officers or customer-service representatives, and other locations. It may also be stored in daily backups, weekly backups, off-site backups, and other archival systems. The CCPA is not clear as to whether only the most current information or all information must be identified and produced.

After locating the personal information they collected, businesses should review it to determine why they collected it and whether they need to retain it. Periodic data purges will help reduce potential privacy risks. For retained information, businesses should map their data so that they can locate it when needed.

Businesses should also review and update their privacy notices to include the disclosures required by the CCPA. They should update their websites to include the information required by the CCPA and consider setting up a home page for California consumers. They also should set up separate portals for consumers to use to exercise their CCPA rights, including establishing new toll-free telephone numbers, new web addresses or portals, new post office boxes, and other means by which consumers can establish contact as needed.

Businesses should train their personnel on how to respond to consumer requests and questions to comply with the CCPA's requirements, including how to produce the personal information that consumers will request.

Businesses should review their contracts with third-party service providers and others with whom they share consumers' personal information. The contracts must be updated to satisfy the new requirements under the CCPA—particularly regarding sharing, selling, and deleting personal information.

Finally, businesses should update their testing, verification, and monitoring procedures that apply to how they collect, maintain, use, and produce consumers' personal information.

72. *Id.* § 1798.198(a).