Update on the California Consumer Privacy Act and Other States' Actions

By Sanford P. Shatz and Paul J. Lysobey[*]

Introduction

California became the first state in the nation to grant its citizens new and enhanced privacy rights when it enacted the California Consumer Privacy Act of 2018 ("CCPA").[1] Since its passage, the California legislature has amended the CCPA;[2] California voters modified the CCPA when they passed ballot proposition 24, the California Privacy Rights Act of 2020 ("CPRA");[3] the California attorney general implemented final regulations;[4] and the California Department of Justice began enforcing the CCPA.[5] The CCPA has also been the subject of litigation. This survey reviews further CCPA developments during the past year and the enactment of similar consumer privacy laws in Virginia and Colorado.

Legislative Amendments to the CCPA

The CCPA defined a "consumer"[6] so broadly that it included employees, contractors, and job applicants. To limit the reach of the CCPA, the legislature amended the act to exempt employee and employment-related information through January 1, 2022.[7] The CPRA extends this deadline through January 1, 2023.[8]

Most of the bills introduced in the 2020–21 legislative session that sought to amend the CCPA failed to advance, or dealt with medical-related issues.[9]

* Sanford P. Shatz is of counsel at McGlinchey Stafford, LLP in Irvine, California. Paul J. Lysobey (CIPP/US) is an associate at McGlinchey Stafford PLLC in Cleveland, Ohio.

1. Cal. Civ. Code §§ 1798.100–1798.199 (West 2021). *See generally* Sanford Shatz & Susan E. Chylik, *The California Consumer Privacy Act of 2018: A Sea Change in the Protection of California Consumers' Personal Information*, 75 Bus. Law. 1917 (2020) (in the 2020 *Annual Survey*).

2. *See* Sanford P. Shatz & Paul J. Lysobey, *The California Consumer Privacy Act of 2018 Updated: More Protection in the Quest to Access and Protect Personal Information*, 76 Bus. Law. 685, 686 (2021) (in the 2021 *Annual Survey*).

3. *See id*. at 691–92.

4. *See id*. at 687–90.

5. *See id*. at 690.

6. Cal. Civ. Code § 1798.140(g).

7. *Id*. § 1798.145(h).

8. Cal. Civ. Code § 1798.145(m).

9. *See, e.g.*, A.B. 1436, 2020–21 Reg. Sess. (Cal. 2021) (digital health feedback systems); A.B. 814, 2020–21 Reg. Sess. (Cal. 2021) (contact tracing); S.B. 41, 2020–21 Reg. Sess. (Cal. 2021) (genetic testing).

However, one bill authorized consumers whose non-encrypted and non-redacted personal information was subject to a data breach to institute a civil action.[10] This bill provides further incentive for businesses to protect their data and to encrypt consumers' personal information.

Creation of the California Privacy Protection Agency

The CPRA established the California Privacy Protection Agency ("CPPA"),[11] which will administer, implement, and enforce the CCPA through administrative actions.[12] The CPRA empowers the CPPA to adopt, amend, and rescind regulations to carry out the purposes and provisions of the CCPA;[13] to protect the privacy rights of natural persons;[14] to promote public awareness and understanding related to consumers' personal information;[15] to provide guidance to consumers regarding their rights under the CCPA;[16] to provide guidance to businesses regarding their duties and responsibilities under the CCPA;[17] to provide technical assistance to the legislature;[18] to monitor developments related to the protection of personal information;[19] to cooperate with other agencies in California, other states and territories, and other countries to ensure consistent application of privacy protections;[20] and to otherwise implement the CCPA.[21]

The CPPA conducted its inaugural board meeting on June 14, 2021,[22] and had not taken any other public action as of this writing.

Amendments to the Implementing Regulations

The original regulations governing compliance with the CCPA went into effect on August 14, 2020.[23] The California attorney general issued several amendments to the regulations that were effective on March 15, 2021 ("2021 Amendments").[24]

The 2021 Amendments require that businesses that sell a consumer's personal information provide the consumer an offline method with which to exercise their right to opt out and clear instructions on how to submit an opt-out request.[25]

10. *See, e.g.*, A.B. 1391, 2020–21 Reg. Sess. (Cal. 2021) (unlawfully obtained data systems).
11. Cal. Civ. Code §§ 1798.199.10–1798.199.100.
12. *Id.* § 1798.199.40(a).
13. *Id.* § 1798.199.40(b).
14. *Id.* § 1798.199.40(c).
15. *Id.* § 1798.199.40(d).
16. *Id.* § 1798.199.40(e).
17. *Id.* § 1798.199.40(f).
18. *Id.* § 1798.199.40(g).
19. *Id.* § 1798.199.40(h).
20. *Id.* § 1798.199.40(i).
21. *Id.* § 1798.199.40(j)–(*l*).
22. *See* CCPA Board Meeting Agenda and Materials (June 14, 2021), https://cppa.ca.gov/meetings/materials/20210614.html.
23. *See* Shatz & Lysobey, *supra* note 2, at 687–90.
24. CCPA Regulations, https://oag.ca.gov/privacy/ccpa/regs.
25. Cal. Code Reg. tit. 11, § 999.036(b)(3) (2021).

The amendments provide that if personal information is collected from a consumer in a brick-and-mortar store, the business may inform consumers of their right to opt out on the paper forms that collect the personal information or by posting signs where the personal information is collected.[26] Similarly, if the personal information is collected over the telephone, the consumers may be orally informed of their rights during the call.[27] Finally, the amendments created an opt-out icon for use by businesses:[28]

The 2021 Amendments require businesses to make it easy for consumers to opt out, and the opt-out method may not be designed to subvert or impair a consumer's choice to opt out.[29] The amended regulations permit a business to verify an authorized agent's authority to act on behalf of a consumer and require a consumer verify the authorized agent's ability to act.[30] The 2021 Amendments also provide disclosures to be given to consumers under age sixteen.[31]

The CPRA requires the CPPA to adopt, amend, and rescind regulations on twenty-two specified topics by July 1, 2022.[32] The CPPA has not proposed regulations as of this writing.

CCPA Enforcement

The California Department of Justice ("DOJ") began enforcing the CCPA on July 1, 2020.[33] In July 2021, the California attorney general held a press conference "announcing successful enforcement efforts [under the CCPA] and urged more Californians to take advantage" of their CCPA rights.[34] He also announced that 75 percent of businesses that had received a notice of an alleged CCPA violation cured the violation and became compliant within the thirty-day cure period provided under the CCPA.[35] The other 25 percent were still within the cure period or were under "active investigation" by the DOJ.[36] The attorney general stated that since CCPA enforcement began, the DOJ has issued cure notices to

26. *Id.* § 999.306(b)(3)(a).
27. *Id.* § 999.306(b)(3)(b).
28. *Id.* § 999.306(f).
29. *Id.* § 999.315(h).
30. *Id.* § 999.326(a).
31. *Id.* § 999.332.
32. Cal. Civ. Code § 1798.199.40.
33. *See* Shatz & Lysobey, *supra* note 2, at 690.
34. *See* Press Release, Cal. Dep't of Justice, Attorney General Bonta Announces First-Year Enforcement Update on the California Consumer Privacy Act, Launches New Online Tool for Consumers to Notify Businesses of Potential Violations (July 19, 2021), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-first-year-enforcement-update-california. The attorney general also launched a new online Consumer Privacy Tool that allows consumers "to directly notify businesses that do not have a clear and easy-to-find 'Do Not Sell My Personal Information' link on their homepage," as required by the CCPA. *Id.*
35. *Id.*
36. *Id.*

a wide range of entities, including "data brokers, marketing companies, businesses handling children's information, media outlets, and online retailers."[37]

The CCPA limited the ability of consumers to bring civil actions under the act to cases in which there was "an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."[38] The legislature also restricted the ability for a violation of the CCPA to form a basis for a claim under California's Unfair Competition Law[39] by providing that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law."[40] Accordingly, courts have quickly dismissed non-data breach claims.

For example, in one class action lawsuit alleging violations of various privacy laws, the court dismissed the claims arising under the CCPA, stating that "the CCPA has no private right of action and on its face states that consumers may not use the CCPA as a basis for a private right of action under any statute.[41] Similarly, the court granted a motion to dismiss a CCPA claim where there were no allegations of a security breach.[42] However, the CCPA claim survived a pleading challenge in a case in which the plaintiff alleged a data breach.[43]

Privacy Legislation in Other States

Two other states enacted comprehensive privacy legislation during the past year: the Virginia Consumer Data Protection Act ("VCDPA")[44] in March 2021 and the Colorado Privacy Act ("CPA")[45] in July 2021.

Virginia Consumer Data Protection Act

The VCDPA provides consumers with personal data rights, and it imposes responsibilities and duties on businesses that use consumers' personal information. The law becomes effective on January 1, 2023.[46] The VCDPA applies to persons that conduct business in Virginia or that produce products or services targeted to residents of Virginia and that during a calendar year, either control or process personal data of at least 100,000 consumers, or control or process

37. *Id.*
38. Cal. Civ. Code § 1798.150(a)(1) (West 2021).
39. Cal. Bus. & Prof. Code § 17200 (West 2021).
40. Cal. Civ. Code § 1798.150(c) (West 2021).
41. Silver v. Stripe Inc., No. 4:20-cv-08196-YGR, 2021 U.S. Dist. LEXIS 141090, at *19–20 (N.D. Cal. July 28, 2021) (citing Cal. Civ. Code § 1798.150(c)).
42. McCoy v. Alphabet, Inc., No. 20-cv-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021).
43. Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898, 924 (S.D. Cal. 2020).
44. Va. Code Ann. §§ 59.1-575–59.1-585 (2021).
45. Colo. Rev. Stat. §§ 6-1-1301–6-1-1313 (eff. July 1, 2023).
46. H.B. 2307, 2021 Leg. Sess. § 4 (Va. 2021).

personal data of at least 25,000 consumers and derive over 50 percent of their gross revenue from the sale of personal data.[47]

The term "consumer" means "a natural person who is a resident of the Commonwealth [of Virginia] acting only in an individual or household context," but does not include "a natural person acting in a commercial or employment context."[48]

The VCDPA regulates businesses acting as "controllers" and "processors," both in collecting data and in interacting with consumers, and the relationship between controllers and processors. A "controller" means "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data," while a "processor" means "a natural or legal entity that processes personal data on behalf of a controller."[49] The VCDPA defines "process" or "processing" as any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.[50]

Consumer Personal Data Rights

The VCDPA creates the following rights for consumers: (a) the right to confirm whether a controller is processing the consumer's personal data and the right to access the data; (b) the right to correct inaccuracies in personal data; (c) the right to delete personal data; (d) the right to obtain a copy of the consumer's personal data in a portable and usable format; and (e) the right to opt out of the processing of personal data for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or other significant effects concerning the consumer.[51] A consumer, or the parent or guardian of a child under age thirteen, may invoke one of these rights at any time by submitting a request to the data controller.[52]

The controller must respond to a consumer request without "undue delay" and within forty-five days, unless the controller provides a notice to the consumer to extend the time period.[53] If the controller declines to take action based on a request, the controller must inform the consumer within forty-five days, along with justification for declining to take action and with instructions for how to appeal the decision.[54] The controller must also establish an appeal process.[55] However, if a controller is unable to authenticate a request using

47. Va. Code Ann. § 59.1-576(A) (eff. Jan. 1, 2023). "Personal data" means "any information that is linked to or reasonably linkable to an identified or identifiable natural person," and "does not include de-identified data or publicly available information." *Id.* § 59.1-575.

48. *Id.* § 59.1-575.

49. *Id.*

50. *Id.*

51. *Id.* § 59.1-577(A).

52. *Id.*

53. *Id.* § 59.1-577(B)(1). Generally, a controller must provide information free of charge in response to a consumer request. *Id.* § 59.1-577(B)(3).

54. *Id.* § 59.1-577(B)(2).

55. *Id.* § 59.1-577(C).

commercially reasonable means, the controller is not required to comply with a request and may request additional information from the consumer needed to authenticate the request.[56]

Duties of Controllers

The VCDPA imposes several duties on controllers of personal data, including: (a) a duty to limit data collection to what is adequate, relevant, and reasonably necessary for the disclosed purposes; (b) a duty to establish and maintain data security practices; (c) a duty not to violate anti-discrimination laws; (d) and a duty not to process sensitive data concerning a consumer without obtaining the consumer's consent, or processing the data of a child contrary to the federal Children's Online Privacy Protection Act ("COPPA").[57]

Controllers are required to provide consumers with a privacy notice that includes specified content and information.[58] Controllers must conduct and document a data protection assessment for certain enumerated types of processing activities involving personal data.[59] In addition, other specified requirements apply to a controller when processing de-identified data.[60]

Exemptions

The VCDPA exempts the following entities from application of the act, including: any government authority, agency, or political subdivision of Virginia; financial institutions or data subject to Title V of the Gramm-Leach-Bliley Act ("GLBA"); nonprofit organizations; or institutions of higher education.[61]

The VCDPA also exempts certain types of information, including, among others: health information protected by the Health Insurance Portability and Accountability Act ("HIPAA"); certain types of personal information that are collected, maintained, disclosed, sold, communicated, or used pursuant to the Fair Credit Reporting Act ("FCRA"); personal data regulated by the Family Educational Rights and Privacy Act ("FERPA"); and data processed or maintained: (i) in the course of a person employed by or acting as an agent for a controller, processor, or third party; (ii) as emergency contact information, when used for that

56. *Id.* § 59.1-577(B)(4).

57. *Id.* § 59.1-578(A); *see* 15 U.S.C. §§ 6501–6505 (2018). "Sensitive data" means: (1) Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (2) The processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (3) The personal data collected from a known child; or (4) The personal data collected from a known child. VA. CODE ANN. § 59.1-575 (eff. Jan. 1, 2023).

58. VA. CODE ANN. § 59.1-578(C) (eff. Jan. 1, 2023).

59. *Id.* § 59.1-579. The VCDPA contains a comprehensive list of obligations that apply to controllers and processors that generally govern the relationship between them. *Id.* § 59.1-579.

60. *Id.* § 59.1-581. "De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person. *Id.* § 59.1-575.

61. *Id.* § 59.1-576(B).

purpose; or (iii) that is necessary to retain to administer benefits for an individual in certain contexts.[62]

Enforcement Authority

The Virginia attorney general has exclusive authority to enforce the VCDPA and the act has no private right of action.[63] Before initiating an action under the VCDPA, the attorney general must provide controllers or processors thirty days' notice identifying the alleged violations and allowing them to cure the violation. If they cure the violation within thirty days, the attorney general will not take action.[64] If an entity fails to cure the violation, the attorney general may seek an injunction and up to $7,500 in civil penalties for each violation.[65]

Colorado Privacy Act

Like the VCDPA, the CPA creates new privacy rights for Colorado consumers and places duties and restrictions on entities that act as controllers and processors. Most of the provisions of the CPA become effective on July 1, 2023.[66] The CPA applies to and distinguishes between controllers and processors of personal data. The CPA applies to a "controller" that conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado, and either controls or processes the personal data of 100,000 Colorado consumers or more during a calendar year, or derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.[67]

The CPA defines a "controller" as a person that, alone or jointly with others, determines the purposes for and means of processing personal data.[68] A "processor" means a person that processes personal data on behalf of a controller.[69] "Process" or "processing" means the collection, use, sale, storage, disclosure,

62. *Id.* § 59.1-576(C). *See* 42 U.S.C. §§ 1320d–1320d-9 (2018); 15 U.S.C. §§ 1681–1681x (2018); 20 U.S.C. § 1321g (2018).

63. Va. Code Ann. §§ 59.1-584(A), 59.1-584(E) (eff. Jan. 1, 2023).

64. *Id.* § 59.1-584(B).

65. *Id.*

66. Colo. Rev. Stat. §§ 6-1-1301– 6-1-1313 (eff. July 1, 2023).

67. *Id.* § 6-1-1304(7). A "consumer" means an individual who is a Colorado resident acting only in an individual or household context and does not include an individual acting in a commercial or employment context. *Id.* § 6-1-1304(6). "Personal data" means: (a) information that is linked or reasonably linkable to an identified or identifiable individual; and (b) does not include de-identified data or publicly available information. *Id.* § 6-1-1303(17).

The CPA also defines the terms "sale" or "sell" or "sold" in a way that may limit the applicability of the CPA to certain entities. These terms mean "the exchange of personal data for monetary or other valuable consideration by a controller to a third party," but the law provides several notable exclusions from the meaning of these terms. *Id.* § 6-1-1303(23).

68. *Id.* § 6-1-1303(7).

69. *Id.* § 6-1-1303(19).

analysis, deletion, or modification of personal data and includes the actions of a controller directing a processor to process personal data.[70]

Consumer Personal Data Rights

Like the CCPA and the VCDPA, the CPA creates new personal data rights for Colorado consumers.[71] These include: (a) the right to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or certain profiling that produces legal or other significant effects; (b) the right of access to confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data; (c) the right to correct inaccuracies in personal data; (d) the right to delete personal information; and (e) the right to data portability.[72]

Consumers may exercise these rights by submitting a request to a controller at any time specifying which rights the consumer wants to exercise.[73] The controller must inform the consumer of the action taken on a request without "undue delay," and notification requirements are substantially similar to those of the VCDPA.[74]

Duties of Controllers

The CPA provides a list of specific duties applicable to controllers, including: (a) a duty of transparency, including the requirement to provide a specific privacy notice; (b) a duty to specify why the personal data is collected and processed; (c) a duty of data minimization, meaning that a controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary; (d) a duty to avoid secondary use; (e) a duty of care, meaning that a controller must take reasonable measures to secure personal data from unauthorized acquisition during both storage and use; (f) a duty to avoid unlawful discrimination against consumers; and (g) a duty regarding sensitive data, meaning that a controller must not process a consumer's sensitive data without first obtaining the consumer's consent, or without the parent's or guardian's consent in the case of a child under age thirteen.[75]

Other duties under the CPA apply to controllers when they conduct "processing that presents a heightened risk of harm to the consumer." In such circumstances, controllers must conduct and document a data protection assessment for each of its processing activities that involve a heightened risk of harm.[76]

70. *Id.* § 6-1-1303(18).
71. *See id.* § 6-1-1306.
72. *Id.* § 6-1-1306(1)(a)–(e).
73. *Id.*
74. *Id.* §§ 6-1-1306(2)(a), 6-1-1306(2)(d). *See* text accompanying *supra* notes 53–56.
75. *Id.* § 6-1-1308. "Sensitive data" means: "(a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition, sex lift or sexual orientation, or citizenship or citizenship status; (b) genetic or biometric data processed for the purpose of uniquely identifying an individual; or (c) personal data from a known child." *Id.* § 6-1-1303(24).
76. *See id.* § 6-1-1309. The CPA also contains a comprehensive list of obligations that apply to controllers and processors that generally govern their relationship. *Id.* § 6-1-1305.

Additional duties and provisions apply when controllers process de-identified data.[77]

Exemptions

The CPA provides a list of exempt persons and information.[78] The list is extensive, but includes: (a) health information protected by HIPAA; (b) certain de-identified information; (c) certain activities regulated by the FCRA done by a consumer reporting agency, furnisher of consumer report information, or a user of a consumer report; (d) data collected, processed, sold, or disclosed pursuant to the GLBA; (e) data regulated by the COPPA; (f) data regulated by FERPA; (g) data maintained for employment record purposes; (h) data maintained by a financial institution or an affiliate as defined by the GLBA; and (i) other data and entities enumerated under the CPA.[79] The CPA also provides limitations on processing data pursuant to an exemption.[80]

Enforcement Authority

The CPA provides that the Colorado attorney general and district attorneys have exclusive authority to enforce the CPA by bringing an action on behalf of the state or on behalf of persons residing in Colorado.[81] There is no private right of action.[82]

Before bringing an enforcement action, the attorney general or a district attorney must issue a notice of violation to the controller and give a sixty-day opportunity to cure, if a cure is deemed possible.[83] In addition, for purposes only of enforcement by the attorney general or a district attorney, any violation of the CPA is considered a deceptive trade practice under Colorado law.[84]

77. *Id.* § 6-1-1307. "De-identified data" means "data that cannot be reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data: (a) Takes reasonable measures to ensure that the data cannot be associated with an individual; (b) Publicly commits to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and (c) Contractually obligates any recipients of the information to comply with the above requirements regarding de-identified data." *Id.* § 6-1-1301(11).
78. *See id.* § 6-1-1304(2).
79. *Id.* § 6-1-1304.
80. *See id.* § 6-1-1304(4).
81. *Id.* § 6-1-1311(1)(a).
82. *Id.* § 6-1-1311(1)(b).
83. *Id.* § 6-1-1311(1)(c).
84. *Id.* § 6-1-1311(1)(d); *see id.* § 6-1-105(1)(nnn).