Differences Between the California Consumer Privacy Act and the California Privacy Rights Act

Sherry-Maria Safchuk & Garylene Javier

Sherry-Maria Safchuk is counsel and a Certified Information Privacy Professional (US) in the Los Angeles office of Buckley LLP. Garylene Javier is a litigation attorney and a Certified Information Privacy Professional (US) in the Washington, DC office of Buckley LLP. They advise clients on consumer financial services, privacy, and cybersecurity-related matters.

Sherry-Maria Safchuk

Garylene Javier

The transformation of privacy laws in California has been swift. The rapid adoption of the California Consumer Privacy Act of 2018 ("CCPA"), its regulations, and the California Privacy Rights Act of 2020 ("CPRA") has required businesses to diligently track new consumer protections across privacy statutes and regulations to ensure compliance. Since January 1, 2020, businesses have grappled with understanding and implementing the CCPA, updating processes and procedures once the CCPA regulations were finalized, and monitoring the passage of the CPRA to determine potential implications.

When the CCPA became effective, it gave California consumers robust privacy rights and control over their personal information such as the right to know, the right to access, the right to delete, the right to opt-out of the sale of personal information that businesses collect, the right to nondiscrimination, and includes additional protections for minors. The California attorney general engaged in a comprehensive rulemaking process that gathered comments from stakeholders to develop a set of regulations that provided guidance on the implementation of privacy rights and consumer protections established by the CCPA.[1] What resulted was a set of regulations that established procedures for compliance with certain requirements set forth in the CCPA, as well as clarified important transparency and accountability mechanisms for businesses subject to the law.[2] Then, in Janu-

1. *CCPA Regulations*, Att'y Gen.'s Off. Cal., https://oag.ca.gov/privacy/ccpa/regs.

2. Cal. Code Reguls. tit. 11, § 999.300 *et seq*.; *see also Attorney General Becerra Announces Approval of Final Regulations Under the California Consumer Privacy Act*, Att'y Gen.'s Off. Cal. (Aug. 14, 2020), https://oag.ca.gov/news/press-

ary 2021, the attorney general issued amendments to the CCPA regulations, which were approved in part by the Office of Administrative Law and made effective March 15, 2021.[3]

A mere three months after the CCPA regulations went into effect, California residents voted to adopt the CPRA, an initiative sponsored by Californians for Consumer Privacy. The CPRA does not deviate from the structure of the CCPA and revises the same chapter of laws in the California Civil Code—Section 1798.100 *et seq*. It is because of this that the CPRA is colloquially known as "CCPA 2.0."

As with the CCPA, the new obligations under the CPRA will similarly require additional rulemaking from the attorney general, and businesses and consumers alike should anticipate further amendments to the regulations. Understanding how the regulations currently implement the CCPA and anticipating how the regulations may change as a result of the CPRA will shed light on how businesses can better prepare their operations for the potential evolution of the law's implementation standards. This article highlights certain provisions of the CPRA that may impact financial services entities, how those provisions deviate from the CCPA and implementing regulations, and how businesses should prepare for the forthcoming changes.

I. New Rights under the CPRA

The CPRA provides consumers with additional privacy rights including the right to correct inaccurate information, the right to limit use and disclosure of sensitive personal information, and the right to opt-out of sharing for cross-context behavioral advertising.

A. Right to Correct Inaccurate Information.

The CPRA provides consumers with the right to correct inaccurate personal information.[4] To exercise this right, the consumer must submit a verifiable consumer request.[5] Aside from providing that the privacy policy must be updated to account for the additional right, the CPRA is silent as to the details for implementing this requirement.[6] Thus, businesses can expect the California Privacy Protection Agency ("California Agency"), the new agency in charge of overseeing the CPRA, to introduce regulations to further the purpose of this section.[7] However, unless the California Agency revamps the privacy policy and other notice requirements, the regulations implementing the right to correct inaccurate information should be similar

releases/attorney-general-becerra-announces-approval-final-regulations-under-california.

3. *See* Att'y Gen.'s Off. Cal., *supra* note 2.
4. Cal. Civ. Code § 1798.106(a) (effective Jan. 1, 2023).
5. Cal. Civ. Code § 1798.106(c) (effective Jan. 1, 2023).
6. Cal. Civ. Code § 1798.106(b) (effective Jan. 1, 2023).
7. Cal. Civ. Code § 1798.185(a)(7), (d).

to the regulations implementing the right to delete or the right to know, for example.

B. Right to Limit Use and Disclosure of Sensitive Personal Information.

The CPRA also provides consumers with the right to limit the use and disclosure of sensitive personal information,[8] which it defines as (1) personal information that reveals: (a) a consumer's social security, driver's license, state identification card, or passport number; (b) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (c) a consumer's precise geolocation; (d) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (e) the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; (f) a consumer's genetic data; or (2) (a) the processing of biometric information for the purpose of uniquely identifying a consumer; (b) personal information collected and analyzed concerning a consumer's health; and (c) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.[9] The term "sensitive personal information" includes, among other things, financial account information, along with any required security or access code, password, or credentials allowing access to the account, personal information collected pursuant to the Gramm-Leach-Bliley Act ("GLBA") or shared pursuant to the Fair Credit Reporting Act but is still exempt from the CPRA.[10] Thus, for most financial services entities, the key will be how to disclose this new right while also explaining the CPRA does not apply to such information because such information is subject to the GLBA.

For sensitive personal information not subject to an exemption, consumers will have the right to direct a business that collects sensitive personal information to limit the use of such information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer.[11] A business must provide consumers with a notice disclosing that this information may be used or shared with a service provider and the consumer has the right to limit the use and sharing of such information.[12] Service providers and contractors assisting businesses also must limit their use of sensitive personal information after they have received instructions from the business and as limited by the written contract between the contractor/service provider and the business.[13]

8. Cal. Civ. Code § 1798.121(effective Jan. 1, 2023).
9. Cal. Civ. Code § 1798.140(ae) (effective Jan. 1, 2023).
10. Cal. Civ. Code §§ 1798.140(ae), 1798.145(e) (effective Jan. 1, 2023).
11. Cal. Civ. Code § 1798.121(a) (effective Jan. 1, 2023).
12. *Id*.
13. Cal. Civ. Code § 1798.121(c) (effective Jan. 1, 2023).

C. Right to Opt-Out of Sharing for Cross-Context Behavioral Advertising.

Currently, the CCPA provides consumers with the right to direct a business that sells personal information to stop selling their personal information.[14] A consumer's personal information cannot be sold if during the time the information was collected, the business did not have a notice of right to opt-out posted and did not have the consumer's authorization.[15]

The CPRA expands the scope of the right to opt-out and provides that a consumer will have the right to opt-out of the sale or *sharing* of personal information. While this is an expansion of the CCPA's requirement related to the sale of data, the definition of "sharing" is limited and includes "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party *for cross-context behavioral advertising*, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged."[16] "Cross-context behavioral advertising" means targeting "advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."[17] Thus, businesses should reach out to their service providers and other third parties to determine whether the result of sharing with such entities may result in cross-context behavioral advertising.

II. Providing Notices to Customers

The CCPA requires businesses to post a privacy policy setting forth information about consumers' privacy rights and how they may exercise their rights.[18] The CCPA also requires businesses to provide consumers with certain notices—i.e., (i) notice at collection if a business collects personal information, (ii) notice of the right to opt-out if a business sells personal information, and (iii) a notice of financial incentive if a business offers such an incentive or price or service difference (if applicable).[19] The attorney general drafted CCPA regulations to implement these privacy policy

14. Cal. Civ. Code § 1798.135; Cal. Code Regs. tit. 11, § 999.306(a)(1).
15. Cal. Code Regs. tit. 11, § 999.306(e).
16. Cal. Civ. Code §§ 1798.120, 1798.140(ah)(1) (effective Jan. 1, 2023) (emphasis added). There are limited exceptions to the definition of "share." Cal. Civ. Code § 1798.140(ah)(2).
17. Cal. Civ. Code § 1798.140(k) (effective Jan. 1, 2023).
18. Cal. Civ. Code § 1798.130(a)(5).
19. Cal. Civ. Code §§ 1798.100(b), 1798.125(b)(2)–(3), 1798.135.

and notice requirements by setting forth specific disclosure requirements.[20] These regulations provide overarching guidance as to the implementation of the statute requirements, but do little to provide templates or model language for businesses to use when drafting their notices and privacy policy.

A. Notice at Collection.

The CCPA sets forth a disclosure obligation that requires businesses to provide disclosures of their collection practices at or before collection.[21] The disclosure requirement in the CCPA is a mere sentence, but the CCPA regulations provide additional guidance regarding the notice at collection disclosure.[22] Specifically, with the goal of being easy for consumers to read and understand, notices must use straightforward language, use a format that easily draws the consumer's attention, be available in languages in which the business conducts its ordinary course, and be reasonably accessible to consumers with disabilities.[23] The notice must include the categories of personal information collected and the business or commercial purposes for which the categories of personal information are used.[24] The regulations also require additional information if a business sells personal information and a link to the privacy policy.[25] The notice at collection must be "readily available where consumers will encounter it at or before the point of collection of any personal information"—e.g., introductory page of a website, all pages where personal information is collected, mobile application download page, prominent signage, etc.[26]

The CPRA amends the CCPA's notice at collection requirements to include additional disclosures. In addition to the disclosure requirements presently in the CCPA, the notice at collection must include the categories of sensitive personal information to be collected and the purposes for which the categories of personal information are collected and used, and whether that information is sold and shared.[27] Businesses are also required to indicate the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period.[28] Furthermore, businesses must use, retain, and share personal information in a manner that is reasonably necessary and proportionate to achieve the purpose for the collection or processing of personal information, or another compatible

20. Cal. Code Regs. tit. 11, § 999.304.
21. Cal. Civ. Code § 1798.100(b).
22. Cal. Code Regs. tit. 11, § 999.305.
23. Cal. Code Regs. tit. 11, § 999.305(a)(2).
24. Cal. Civ. Code § 1798.100(b); Cal. Code Regs. tit. 11, § 999.305(b).
25. Cal. Code Regs. tit. 11, § 999.305(b)(3).
26. Cal. Code Regs. tit. 11, § 999.305(a)(3).
27. Cal. Civ. Code § 1798.100(a)(2) (effective Jan. 1, 2023).
28. Cal. Civ. Code § 1798.100(a)(3) (effective Jan. 1, 2023).

purpose, and not further processed in a manner that is incompatible.[29] Thus, businesses may be required to update their notice at collection to clarify their business or commercial purpose where data is transformed so that its original purpose at collection is transformed into a subsequent purpose later in the life cycle of the data.

Several questions regarding the implementation of the notice at collection remain unaddressed by the attorney general. For example, it is unclear exactly how much detail must be provided in the notice at collection, particularly with regards to the business purpose for which the information is being collected. When questioned during the rulemaking process of whether the list of business or commercial purposes for which categories of personal information will be used was exhaustive, the attorney general referred to the definition of "business purpose" and "commercial purpose" in the CCPA but did not address the issue of whether the list of business purposes is exhaustive.[30] The attorney general advised that if businesses use the personal information outside the seven options outlined, businesses should describe the usage in very clear language, so the consumers understand the purpose for which their information is used.[31] As of the date of this article, there is no additional clarification on the issue.

It is important to note that while the CPRA is not yet effective and the CCPA's private right of action is limited to data breaches, plaintiffs have alleged "lack of notice at collection" as a violation of the CCPA in complaints filed with various courts, although it remains to be seen whether these claims survive.[32] The privacy regulations may be further amended as a result of the CPRA, but businesses should ensure that a consumer receives a timely notice at collection because, although there is no private right of action for a violation of the notice at collection requirements, plaintiffs are still alleging such violations in recent cases filed.

B. Privacy Policy.

The CCPA requires businesses to disclose certain information in their online privacy policy or their websites, and must be updated at least once every 12 months.[33] The goal of the privacy policy per the CCPA regulations is "to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and

29. Cal. Civ. Code § 1798.100(c) (effective Jan. 1, 2023).
30. *See* Att'y Gen.'s Off. Cal., FSOR Appendix A: Summary and Response to Comments Submitted During 45-Day Period 46 (2020), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf (Response 155).
31. *Id.*
32. *See, e.g.*, *In re* Ring LLC Privacy Litigation, No. 2:19-CV-10899 (C.D. Cal. filed Dec. 26, 2019); In re: Zoom Video Communications, Inc. Privacy Litigation, No. 5:20-CV-02155 (N.D. Cal. filed Mar. 30, 2020).
33. Cal. Civ. Code § 1798.130(a)(5).

sale of personal information and of the rights of consumers regarding their personal information."[34] The regulations set forth instructions for how to draft and post the privacy policy such as including information related to formatting, type of language used, languages, the manner in which the policy must be given, and accessibility to consumers with disabilities.[35] The regulations build on the requirements in the CCPA and provide business with more direction on how to draft a privacy policy and the disclosures that must be included.[36]

The CPRA incorporated some of the privacy policy provisions in the regulations into the statute itself, which appears intended to align the requirements in the statute and regulations.[37] While the CPRA did not set forth additional requirements for the privacy policy, the CPRA added additional consumer rights as discussed above, which must be incorporated in a business's CCPA policy.[38] Further, the questions raised with respect to how certain disclosures should be made in the notice at collection are applicable to the privacy policy as well. Notwithstanding, the CPRA regulations may require businesses to include additional disclosures in its privacy policy and thus, businesses should monitor developments regarding the CPRA regulations.

In the interim, the attorney general's commentary and the current CCPA regulations remain useful guidance to draft privacy policies.[39] In addition, businesses should review FTC guidance and enforcement actions for direction on how to draft privacy policies and get a sense of what regulators are looking for to determine whether a representation made in the policy may be considered unfair or deceptive.[40]

III. Consent and Dark Patterns

Under the CCPA, the term "consent" is used in the context of consent for research purposes in the exceptions to the right to delete, to sell minor information, and for purposes of entering a consumer into a financial in-

34. Cal. Code Regs. tit. 11, § 999.308(a)(1).
35. Cal. Code Regs. tit. 11, § 999.308(a)–(b).
36. *Compare* Cal. Civ. Code § 1798.130(a)(5), *with* Cal. Code Regs. tit. 11, § 999.308.
37. *See* Cal. Civ. Code § 1798.130(a)(5) (effective Jan. 23, 2023); Cal. Code Regs. tit. 11, § 999.308.
38. Cal. Civ. Code § 1798.130(a)(5) (effective Jan. 1, 2023).
39. Attorney General commentary regarding the CCPA regulations can be found in the *Initial Statement of Reasons*, the *Final Statement of Reasons*, and addendums to the *Final Statement of Reasons*, found at: https://oag.ca.gov/privacy/ccpa/regs.
40. *See Protecting Consumer Privacy and Security*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security.

centive program, but the term is undefined.[41] The CPRA addresses this issue and adds the following definition for "consent":

> [A]ny freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.[42]

Most consumer finance entities will not be subject to the consent requirements under the CPRA, but the definition of "consent" is informative in a number of ways:

- The definition of "consent" is limited to the CPRA, but other regulators and courts may look to the definition of "consent" under the CPRA to inform their view of how consent should be obtained in other contexts.
- The CPRA makes clear that consent must be "freely given, specific, informed, and unambiguous indication of the consumer's wishes . . . including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose." As such, businesses should consider reviewing "consent" language for purposes of the CPRA to ensure that the language is clear, specific, unambiguous, and for a narrowly defined particular purpose. Further, businesses may consider reevaluating how they obtain consumer consent and whether the manner in which consent is obtained would be considered "a clear affirmative action."
- The CPRA expressly provides that "acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent." Thus, it appears that the Agency will expect to see compliance with the "consent" requirements as separate from a terms of use or similar lengthy document.
- The CPRA introduces the concept of "dark patterns" and provides that agreements obtained through use of dark patterns do not constitute consent. First used in 2010, the term "dark patterns" was developed

41. Cal. Civ. Code §§ 1798.105(d)(9), 1798.120(d), 125(b)(3).
42. Cal. Civ. Code § 1798.140(h) (effective Jan. 23, 2023).

> to define "user interface design patterns that are 'crafted with great attention to detail, and a solid understanding of human psychology, to trick users into do[ing] things they [would not] otherwise have done."[43] Rohit Chopra, when at the Federal Trade Commission, noted that "dark patterns are design features used to deceive, steer, or manipulate users into behavior that is profitable for an online service, but often harmful to users or contrary to their intent . . . [and] are the online successor to decades of dirty dealing in direct mail marketing."[44] The CPRA attempts to incorporate this concept in California privacy laws and defines "dark patterns" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice . . . ."[45]

The CCPA regulations appeared to refer to "dark patterns" in its 2021 amendments in the context of the right to opt-out, requiring that methods for submitting requests to opt-out must necessitate minimal steps to allow the consumer to opt-out and are not designed with the purpose or have the substantial effect of subverting or impairing a consumer's choice to opt-out.[46] In other words, examples of dark patterns may include an opt-out request requiring more steps than the process for a consumer to opt-in to the sale of personal information after having previously opted out, using confusing language such as double negatives, and requiring the consumer to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.[47]

IV. Service Providers, Contractors, and Third Parties

The CCPA also sets forth requirements for service providers and third parties. The definitions of "service providers" and "third parties" are similar in the sense that both definitions contemplate that a business will have a contractual relationship with the "service provider" or "third party" that limits the service providers' and third parties' use of personal information.[48] The CCPA regulations further outlined when an entity is considered a "service provider" under the CCPA and sets forth requirements for "service providers."[49] For example, a service provider must not retain, use, or

43. Justin Hurwitz, *Designing a Pattern, Darkly*, 22 N.C. J. L. & Tech. 57, 67 (2020).
44. Rohit Chopra, Commissioner, Fed. Trade Comm'n, Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc., Fed. Trade Comm'n File No. 1723186 (Sept. 2, 2020), https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.
45. Cal. Civ. Code § 1798.140(l) (effective Jan. 23, 2023).
46. Cal. Code Regs. tit. 11, § 999.315(h).
47. *Id*.
48. Cal. Civ. Code § 1798.140(v), (w).
49. Cal. Code Regs. tit. 11, § 999.314.

disclose personal information obtained while providing services except in limited instances (such as processing personal information in compliance with a written contract for services under the CCPA)[50] or sell data on behalf of a business when a consumer has opted out of the sale of their personal information with that business.[51]

The CPRA revises the definition of "service provider" to include additional restrictions and adds a new "contractor" category of recipients who receive and process personal information in accordance with a written agreement with a business.[52] The CPRA also sets forth similar contract requirements for "contractors,"[53] however, contractors must certify they understand and will comply with the imposed contractual commitments and must permit the business to monitor the contractor's compliance with the contract (although this requirement appears permissive with service providers).[54] The CPRA requires contractors and service providers to notify businesses if they engage their own service provider or subcontractor and ensure those parties adhere to the same written obligations arranged between the businesses and the service providers.[55] Both service providers and contractors must be contractually prohibited from combining any personal information received from the business with personal information from other sources or collected on its own behalf.[56]

The CPRA does not provide further clarity regarding the difference between a "service provider" and a "contractor." Based on the additional certification requirement, "contractor" may be referring to persons generally considered independent contractors as opposed to more traditional vendors, which are often considered service providers. Notwithstanding, businesses should reevaluate their relationships with third parties to determine whether such persons would be considered a "service provider," a "contractor," or some other third party, and whether the agreements with such persons should be updated.

V. Conclusion

The introduction and subsequent adoption of the CCPA, its regulations, and the CPRA, has made consumers more aware of what personal information they are providing businesses and are prioritizing the security and confidentiality of their personal information. This means that consumers may pay particular attention to a business's privacy policies and practices and may be inclined to reach out to the business with questions about their

50. Cal. Code Regs. tit. 11, § 999.314(c).
51. Cal. Code Regs. tit. 11, § 999.314.
52. Cal. Civ. Code § 1798.140(j)(1), (ag)(1) (effective Jan. 1, 2023).
53. *Id*.
54. Cal. Civ. Code § 1798.140(j)(1)(C), (ag)(1)(D) (effective Jan. 1, 2023).
55. Cal. Civ. Code § 1798.140(j)(2), (ag)(2) (effective Jan. 1, 2023).
56. Cal. Civ. Code § 1798.140(j)(1)(A)(iv), (ag)(1)(D) (effective Jan. 1, 2023).

privacy practices. In addition, consumers may engage third-party companies to assist them with exercising their rights under the CCPA and businesses should have processes in place to respond to such requests.

As California implements the CPRA, we can anticipate future revisions of the regulations to account for the changes made by the CPRA, which will require business to be able to quickly adopt new requirements to satisfy compliance obligations.

As privacy laws evolve, businesses should consider focusing their efforts in two areas—businesses must know what personal information they possess, how they collect it, and how they use it (i.e., data mapping discussed further below); and businesses must have mechanisms in place to ensure that consumers are able to exercise their rights. In addition, for businesses to remain flexible to the shifting privacy landscape, they should consider implementing the following best practices:

- **Engage in data mapping.** Businesses should readily have access to information outlining the data they collect, the reason for collecting the data, how they collect the data, how they use the data, with which entity they share data, the duration they keep the data, and where it is housed. While many businesses have engaged in data mapping to understand their obligations under the CCPA, businesses would benefit from enhancing or revisiting their data mapping in light of the CPRA and other state privacy legislations that have been introduced and are pending across the country.
- **Regularly update privacy policies and procedures:** Businesses are required to update their CCPA privacy policy every 12 months. As such, if a privacy policy includes a "last updated" date of 2019, it may be a target for regulators. However, merely changing the date likely is not sufficient to satisfy the requirement. Rather, when updating a privacy policy, a business also must ensure that its data mapping is up to date and its procedures have not changed if it receives new information regarding the collection of personal information. As noted above, if a business's privacy policy does not match its procedures internally, the business could face allegations of unfair or a deceptive acts or practices. Further, businesses should look for ways to further clarify their privacy policy to ensure it is concise and easy to read by consumers.
- **Establish appropriate compliance mechanisms.** When the CCPA passed, businesses were required to create processes and procedures to provide consumers with mechanisms for submitting requests and for responding to requests. These processes and procedures should be reevaluated to determine whether any updates should be made to current practices to account for the CPRA amendments. This is particularly important when working with third parties, such as service providers, contractors, affiliates, and non-affiliates, where the business must ensure that its written agreement includes certain limitations.

- **Be aware of enforcement and private right of action priorities.** Although the private right of action in the CCPA is limited to data breaches, plaintiffs have filed complaints that raise other alleged deficiencies under the CCPA including lack of notice at collection. In addition, the California attorney general and likely federal regulators, such as the FTC, remain keenly focused on privacy disclosures provided to consumers. As such, businesses should monitor litigation and enforcement actions in this space to determine how regulators and plaintiff's counsel are focusing on privacy violations.

By adopting these best practices, businesses will remain ready for any subsequent changes to the privacy regulations as it implements the principles in the CPRA or any subsequent evolution of the California privacy law.