The California Privacy Rights Act:

CCPA Amendments, New Requirements and Recommendations

New requirements now apply to employee and business information

by Michael Plumleigh & Meera Patel

The California Consumer Privacy Act of 2018 ("CCPA") was recently amended by the California Consumer Privacy Rights Act ("CPRA").[1] In previous client alerts, we provided an overview of the CCPA and an update regarding subsequent amendments and enforcement by the California legislature. We encourage our readers to review those alerts, as well as the text of the law itself.

This Alert, while not exhaustive, describes many of the recent amendments to the CCPA that will be enforced starting on July 1, 2023*, including those that now apply to employers and businesses, and provides information regarding:

- the CPRA changes and requirements enacted into law following our previous client alerts, including expanded coverage to employers and businesses, adding requirements for employee personal information and B2B information and adding a new category of "sensitive personal information" requiring additional protections;
- our recommendations for our clients that are covered entities under the CCPA. In addition, while not all companies meet the California consumer and/or revenue requirements of the CCPA, we recommend that companies implement website and privacy policies that comply with the new law given the growing trend for similar protections in many states and outside the U.S.

For additional information and guidance, please contact one of the attorneys listed below.

Covered Businesses

All businesses that are covered by the CCPA are required to comply with the expanded statutory requirements enacted under the CPRA. A "covered business" is any for-profit entity that (A) collects the personal information[2] of California consumers or (B) does business in California, and meets at least one of these criteria: (i) had an annual gross revenue in excess of $25 million in the preceding calendar year, (ii) alone or in combination, annually buys, sells, or shares the personal information of more than 100,000 California consumers, households or devices for commercial purposes (previously only 50,000), or (iii) derives 50% or more of its annual revenues from "selling" or "sharing" consumers' personal information.

Legislative Background

In November 2020, California voters approved Proposition 24, the CPRA, which supplemented the CCPA with additional consumer privacy protections and transferred rulemaking and enforcement authority from the California Attorney General to the California Privacy Protection Agency ("CPPA"), a newly established agency. The CPRA took effect on January 1, 2023, but many of the new obligations include a 12-month look-back that allows consumers to request that businesses provide

* ***Update***: On June 30, 2023, the Superior Court of California, County of Sacramento, ruled that enforcement of the final regulations issued under the CPRA to date is delayed until March 29, 2024. Enforcement of any regulations regarding cyber-security audits, risk assessments and automated decision-making technology will not begin until a year after the CPPA finalizes such rules.

certain information dating back to January 2022. The CPPA approved a penultimate draft of the CPRA on February 3, 2023, which subsequently underwent a final round of public comments and additional revisions. The final draft of the revised CCPA, which incorporates the CPRA, was approved by California's Office of Administrative Law and became effective on March 29, 2023. As originally reported, the CPPA would have begun enforcing the revised CCPA through administrative enforcement actions on July 1, 2023, however that has now been delayed until March 29, 2024.[3]

CPRA Requirements

This section provides a brief summary of some of the changes implemented by the CPRA.

Scope

As mentioned previously, the revised law modifies the definition of a covered business by increasing the threshold of the number of California residents from whom a business collects, sells or buys personal information from 50,000 to 100,000 consumers or households.[4] It also expands the scope of businesses subject to the CCPA by imposing obligations on businesses that "share"[5] personal information, rather than just those businesses that sell personal information, and requires businesses that engage in either activity to place a "Do Not Sell or Share My Personal Information" link on their websites.[6]

Employee and B2B Information

One of the notable changes established by the CPRA includes the expiration of the CCPA's exemption for employee personal information and business-to-business ("B2B") personal information, which means that these categories of personal information (and the employees or B2B individuals involved) are now protected under the CCPA. Below are brief summaries of the changes:

- Employee Personal Information: California employers (that are "covered businesses" and which collect personal information in the employment context) must provide notice to all "employees" prior to or at the time of collection,[7] and respond to requests from such employees who exercise rights associated with their personal information. All covered businesses should also recognize that the term "employee" broadly encompasses any natural person, or all California employees, applicants, independent contractors, members of boards of directors, emergency contacts, and beneficiaries, and that these individuals will generally have the same rights and protections under the CCPA as any other consumer.
- B2B Personal Information: Businesses should understand that all personal information obtained in the business context via verbal or written communication (concerning due diligence of, the provision of, or the receipt of a product or service) with any individual who is acting as an employee, owner, director, officer, or contractor of a company doing business with a covered business (such as customers, vendors, service providers, etc.), is no longer exempt under the CCPA. As with employee data, covered businesses must provide notice at the point of collection and honor other businesses' (*i.e.*, their employees') rights.

Security Practices and Cybersecurity Audits

The CPRA establishes an explicit duty for businesses retaining and handling personal information collected from individuals to implement reasonable security procedures and practices in maintaining documentation related to requests from individuals, transmitting personal information to individuals when responding to requests to know, detecting unauthorized access to personal information, conducting risk assessments and protecting personal information from unauthorized or illegal access, disclosure, modification, or destruction. Though the CPRA does not include specific technical requirements, the Office of the Attorney General indicated that businesses should look to the list of security controls set forth by the Center for Internet Security's Critical Security Controls (CIS) as the minimum level of security an organization should meet,[8] and the list has since been modified by CIS.[9] Additionally, the CPRA requires businesses to perform annual cybersecurity audits if their

processing of personal information poses a significant risk to individuals' privacy or security. The regulations do not outline the parameters of the audit requirement but suggest that in evaluating whether processing may result in significant security risks to personal information, businesses should consider the size and complexity of their business and the nature and scope of the processing activities.[10]

Purpose Limitation and Data Minimization

The CPRA creates a broad purpose limitation, modeled on the Fair Information Practice Principles implemented under the GDPR,[11] which requires businesses to collect, use, retain, and share personal information only as "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected."[12] The limitation requires businesses to (i) only collect, process, and retain personal information to the minimum necessary that is required for the purpose disclosed by the business and (ii) only retain information for as long as necessary to fulfill the disclosed purpose.

Sensitive Personal Information

The CPRA codifies a new category of personal information referred to as "sensitive personal information," obligates businesses to disclose the categories of sensitive personal information that they collect and establishes a new right wherein individuals may limit the use and disclosure of their sensitive personal information. Sensitive personal information includes any information that reveals:

- an individual's social security, driver's license, state identification card or passport number;
- an individual's account log-in, financial account, debit card or credit card number combined with any required security or access code, password or credentials allowing access to an account;
- an individual's precise geolocation;
- an individual's racial or ethnic origin, religious or philosophical beliefs or union membership;
- the contents of an individual's physical mail, email and text messages, unless the business is the intended recipient of the communication; or
- an individual's genetic data, which may include:
  - biometric information processed for the purpose of identifying an individual;
  - personal information involving an individual's health; or
  - personal information regarding an individual's sex life or sexual orientation.

Businesses should offer individuals this right to limit use and disclosure of their sensitive personal information subject to certain exceptions.[13] Moreover, businesses should include separate disclosures for the categories of sensitive personal information collected, the purpose of collection, and whether such information is sold or shared.[14]

Publicly Available Information

Under the CCPA, "personal information" does not include information that is lawfully made available through public records from federal, state or local governments. This exception (prior to being amended by the CPRA) was narrow and did not include information that individuals voluntarily shared publicly online (e.g., via social media). The CPRA expands on the definition of "publicly available," consequently limiting the scope of information that is subject to the law. The CPRA definition of "personal information" similarly excludes publicly available or truthful information that is lawfully obtained and a matter of public concern, and includes the following:

- information that a business has a reasonable basis to believe is lawfully made available;
- information from widely distributed media; and
- information made available by a person to whom the individual has disclosed the information if the individual has not restricted its use.

Furthermore, this exception is based on whether a business (as opposed to an individual) "has a reasonable basis to believe [the personal information] is lawfully made available to the general public."[15] Thus, the CPRA broadens the scope of information that is subject to this exception, thereby narrowing the scope of information that is applicable to consumer rights.

Consumer Rights

The CCPA established several consumer rights, including the rights to know the categories of personal information, to request deletions of their personal information, to opt-out of the sale or sharing of their personal information, and the right to non-discrimination for electing to exercise any right. The CPRA codifies additional consumer rights, including:

- the right to correct inaccurate information;
- the right to limit the use of sensitive personal information; and
- the right to opt-out of automated decision-making technology.

The CPRA also provides clarifications to the aforementioned new and the following existing rights:

- Notice of right to limit: Businesses that use or disclose sensitive personal information should, on their websites and privacy policies, provide individuals with a Notice of the Right to Limit the use of their sensitive personal information.[16]
- Right to opt-out of "sharing" and sale of personal information: The definition of "sharing" has been modified to broadly mean the transfer or making available of personal information by a business to a third party for the purpose of cross-context behavioral advertising,[17] whether or not for monetary consideration; moreover, a business's homepage should contain link, titled "Do Not Sell or Share My Personal Information" which leads to this information.
- Right to delete: When an individual requests deletion or removal of personal information, businesses must (i) notify their service providers or contractors to delete such individual's personal information (which was collected pursuant to a written contract with the business) from their records, or if able to do so, delete such information on their behalf; and (ii) notify all third parties to whom the business shared or sold personal information to delete the individual's personal information (unless it proves impossible or involves disproportionate effort).[18]
- Private right of action: The CPRA contains a private right of action that allows individuals to bring a private legal action against a business for certain data breaches.[19]

Businesses should understand that these modifications merely supplement the existing rights of individuals under the CCPA.

Contractual Obligations

The CPRA also requires that businesses place new obligations in their contracts with service providers and contractors. These contracts must, among other things: (A) mandate that service providers or contractors cooperate with and assist businesses in responding to and completing requests from individuals to correct, delete, or limit the use of their personal information, (B) prohibit service providers or contractors from retaining, using, or disclosing personal information that they collect pursuant to a written contract with the business for any purpose other than those specified in the contract, unless expressly permitted by the CCPA, and (C) grant the business the right to take reasonable and appropriate steps to (i) ensure that the service provider or contractor comply with their obligations regarding consumer personal information, and (ii) stop and remediate any unauthorized uses.[20]

New Privacy Policy Requirements

The revised CCPA provides additional guidelines on which terms businesses should include in their privacy policies, including policies relating to the collection and processing of personal information from employees and business contacts. Some of these items include a comprehensive description of the business's online and offline information practices, and an explanation of

individuals' rights (including how to exercise them and what to expect from the process).

Recommendations

Each covered business should promptly implement procedures to comply with the CPRA's requirements. At a minimum, these should include:

- updating your business's consumer privacy policy to inform consumers of their new rights and how to exercise them (and revisiting it annually);
- reviewing and updating (or if you haven't already done so, creating) your business's employee or personnel privacy policy and data collection and retention procedures to incorporate the CPRA changes;
- providing written notice to and obtaining acknowledgement from consumers, employees, applicants, contractors, and other individuals covered by the CCPA of their rights and your privacy practices, through an updated employee handbook, employee or applicant portal, or online privacy policy, including receiving written or electronic acknowledgements from personnel and prospective personnel in employee offer letter acknowledgements, onboarding materials and during the recruiting/job application process;
- if applicable, providing an icon that links to specific notices that describe individuals' right to (A) opt-out of the sale of their information on your business's website and in your business's privacy policy titled "Do Not Sell My Personal Information," and (B) limit the use of their sensitive personal information, titled "Notice of Right to Limit";[21]
- reviewing, and if applicable, implementing, procedures to track, review, and respond to CCPA requests from individuals, and training personnel responsible for handling such requests, in accordance with the CCPA's minimum requirements, including implementing appropriate data storage tracking, data inventory and data mapping for each category of personal information collected which will enable the ability to meet those requests;
- reviewing all vendor contracts, including for internal vendors (such as payroll, HR, external recruiters and CRM providers) to ensure protection of your consumer, employee and/or business contact data;
- reviewing and assessing whether your business's internal data security policies, and data retention policies and practices are sufficient to meet the CPRA's purpose limitation and security requirements by ensuring that you are only collecting information for a business purpose,[22] conducting internal audits, and implementing security enhancements or technology upgrades as necssary; and
- lastly, but most importantly, ensuring that your actual practices for collecting, using, securing and retaining all personal information and related data are accurately reflected by and in line with your stated privacy policies and data security practices.

[1] For purposes of this Alert, any references to the "CCPA" include the comprehensive changes enacted by the CPRA.

[2] "Personal Information" is information that identifies, relates to, or could reasonably be linked with a consumer or the consumer's household. *See* Attorney General Rob Bonta's California Consumer Privacy Act (CCPA) Frequently Asked Questions (FAQs), February 15, 2023

[3] "Frequently Asked Questions: What is the California Privacy Protection Agency?" California Privacy Protection Agency website. *See final bullet point to find enforcement date.*

[4] Cal. Civ. Code § 1798.140(d)(1)(B). The CCPA generally refers to persons as a "consumer," which is defined as "a natural person who is a California resident…." *Id.* § 1798.140(g). When referring to applicability in the employee and business context in this Alert, we have at times used "individuals," and references to "consumer" should be read to include employees and business contacts.

[5] "Share," Shared" or "Sharing" is defined under the CPRA as 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-contextual behavioral advertising, whether or not for monetary or other valuable consideration, including when no money is exchanged. Cal. Civ. Code § 1798.140(ah).

[6] Cal. Civ. Code § 1798.135(a).

[7] Final Regulations Text, Article 2 § 7012.

[8] Appendix A, California Data Breach Report (2012-2015), Attorney General California Department of Justice, February 2015.

[9] The 18 CIS Critical Security Controls, Center for Internet Security.

[10] Cal. Civ. Code § 1798.185(a)(15).

[11] The European Union General Data Protection Regulation 2016/679.

[12] Cal. Civ. Code §1798.100(c).

[13] The CPRA notes that a business must offer individuals the right to limit the use and disclosure of their sensitive personal information unless the collection, use or disclosure of such information is reasonably necssary and proportionate: (i) to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services; (ii) to prevent, detect and investigate security incidents that compromise personal information; (iii) to resist malicious, deceptive, fraudulent or illegal actions directed at the business and to prosecute those responsible for those actions; (iv) to ensure the physical safety of natural persons; (v) for short-term and transient use, provided that the personal information is not disclosed to another third party and is not used for targeted advertising outside the consumer's current interaction with the business; (vi) to perform services on behalf of the business; (vii) to verify or maintain the quality or safety of a product, service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business; or (viii) to collect or process sensitive personal information where such collection or processing is not for the purpose of inferring characteristics about a consumer. 27 Final Regulations Text, Section 7027(m).

[14] Cal. Civ. Code § 1798.100(a)(2).

[15] Cal. Civ. Code § 1798.140(v)(2).

[16] Final Regulations Text, Article 3 § 7027(b)(1).

[17] "Cross-context behavioral advertising" is defined as targeted advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across business, distinctly branded websites, applications, or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. Cal. Civ. Code § 1798.140(k).

[18] Final Regulations Text, Article 3 § 7022(b).

[19] Cal. Civ. Code § 1798.150.

[20] Final Regulations Text, Article 4 § 7051.

[21] The CPRA provides an exception to the requirement of having prominent "Do Not Sell or Share My Personal Information" and the "Limit the Use of My Sensitive Information" links. Businesses are not required to include these signals so long as they automatically (through technical specifications set forth in paragraph (20) of subdivision (a) of Section 1798.185), enable the opt-out preference for any individual who visits their website and provided that the business must then refrain from selling such individual's information and also wait at least 12 months before making another request that the individual permit the sale or sharing of personal information or the use and disclosure of the individual's sensitive personal information for additional purposes. Cal. Civ. Code § 1798.135(b)(1) and (4).

[22] A "business purpose" means the use of personal information for the business' operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted in paragraph (11) of subdivision (a) of Section 1798.135. Examples of business purposes include (i) performing services on behalf of the business or (ii) helping ensure security and integrity as reasonably necessary. *See* Cal. Civ. Code § 1798.140(e) for more information.