COVINGTON

New California Ballot Initiative Seeks to Redo CCPA

September 27, 2019

Data Privacy and Cybersecurity

Real estate developer Alastair Mactaggart is making news with the announcement of another privacy ballot initiative, the California Privacy Rights and Enforcement Act ("CPREA"). He intends to include his new initiative on the November 2020 ballot.

Before the California Consumer Privacy Act ("CCPA") even takes effect and the California Attorney General's draft regulations are published, CPREA seeks to amend the current CCPA statute in several material respects, including to establish a new California Privacy Protection Agency to adopt rules, enforce the CCPA, and appoint a "Chief Privacy Auditor" whose duty would be to proactively "conduct audits of businesses to ensure compliance" (regardless of whether any consumer complaints have been filed or violations alleged).

Other key highlights include the following:

- CPREA expressly addresses whether use of certain advertising technologies constitutes a "sale" of personal information for which consumers have the right to opt out.
  - The initiative would amend the definition of "sale" to include disclosures of personal information—even if not for monetary or other valuable consideration—if the disclosure is "otherwise for a commercial purpose, including but not limited to cross-context behavioral advertising." "Cross-context behavioral advertising" is defined as the "targeting of advertising to a consumer based on a profile of the consumer including predictions derived from the consumer's personal information, where such profile is related to the consumer's activity over time and across multiple businesses or across multiple, distinctly-branded websites, application, or services."
  - The ballot initiative also would amend the definition of "business purposes" in a way that could make it challenging to argue that partners engaged in "cross-context behavioral advertising" are "service providers."
  - The Findings and Declarations section of the ballot initiative is drafted in a manner that implies that the current CCPA already gives consumers the right to opt out of their information being used for cross-context behavioral marketing, although the proposed revisions highlight that the current CCPA is ambiguous in this regard and that there are counter-arguments.
- The ballot initiative would impose direct liability on various parties other than the "business" who has collected the personal information from consumers, and this liability would arise for new kinds of prohibited conduct. Among the relevant provisions, the initiative would provide that any person authorized to collect personal information by a

business would be required to comply with the business's instructions in response to a consumer's opt-out request. As directed by the business, such persons would be directly prohibited from selling the personal information and from retaining, using, and disclosing the personal information except for certain purposes. The business that has the relationship with the consumer would not be liable for the other person's non-compliance so long as it does not have actual knowledge, or reason to believe, that the person intends to commit the violation. This language seems designed to shift responsibility for complying with consumer opt-outs to third parties in the advertising technology ecosystem.

- CPREA would create heightened protections for certain categories of "sensitive personal information." Among them, sensitive personal information could not be sold without the affirmative authorization of the consumer. Further, consumers would have the right to opt out of use or disclosure of their sensitive personal information "for advertising and marketing." (Even disclosure of sensitive personal information to a service provider would be prohibited upon receipt of a consumer opt out.) "Advertising and marketing" is defined broadly to include communications intended to induce a consumer to buy, rent, lease, join, use, subscribe to, apply for, provide, or exchange products, goods, property, information, services, or employment. The ballot initiative contemplates a link similar to the Do Not Sell Button to enable consumers to exercise this choice, although it contemplates a single combined link could be provided in some circumstances.
    - "Sensitive personal information" would be defined to mean "a consumer's social security, driver's license, state identification card, or passport number; 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; a consumer's precise geolocation; personal information revealing a consumer's racial or ethnic origin, religion, or union membership; the contents of a consumer's private communications, unless the business is the intended recipient of the communication; a consumer's biometric information; data concerning a consumer's health; data concerning a consumer's sexual orientation; or other data collected and analyzed for the purpose of identifying such information."
- For consumers who opt out of the sale of their personal information or opt out of the use or disclosure of personal information for advertising and marketing, the ballot initiative would require businesses to wait for at least 12 months before requesting authorization to sell, or use and disclose, the consumer's personal information.
- Information about consumers under 16 years of age also would be subject to heightened protections. Businesses would not be permitted to collect (defined broadly to include, for example, "access") personal information of consumers less than 16 without affirmative consent if the business has actual knowledge that the consumer is less than 16. Currently, the CCPA requires affirmative consent to "sell" personal information about such minors—but not an obligation to obtain prior consent to access or otherwise collect the information.
- The ballot initiative would make several changes relevant to data subject requests:
    - Household data would not be subject to a number of obligations under the ballot initiative, including § 1798.105 (deletion rights) and § 1798.110 (right to access "specific pieces of personal information"), as well as the new data correction rights that would become § 1798.105.5 (correction rights).

    - After the effective date of CPREA, the personal information subject to access requests would not be limited to information collected during the 12-month period preceding receipt of a verifiable consumer request, although the ballot initiative would introduce language limiting the requirement to respond to data outside of the 12-month window where it would “involve a disproportionate amount of information or would be unduly burdensome.”
    - “Specific pieces of information” required to be provided to consumers in response to access requests would not include data generated for certain security, fraud prevention, and similar purposes.

- CPREA also would add new disclosure obligations. Among them, businesses also would need to disclose whether they profile consumers, at least for purposes of determining eligibility for financial services, housing, insurance, or certain other decisions, together with information about the “logic involved” in using personal information for such profiling. Businesses that use personal information for political purposes also would be subject to specific disclosure obligations, including to identify the candidates, committees, or ballot measures for which the personal information will be used.
- There are certain additional principles reflected in the GDPR that would be added to California law through CPREA. Among them:
    - Businesses would be required to take reasonable steps to ensure they do not process inaccurate personal information and to provide consumers the right to correct inaccurate personal information.
    - Businesses would be required to implement reasonable measures to protect personal information from unauthorized or illegal access.
    - CPREA would expressly restrict collection of personal information that is not reasonably necessary to achieve the purposes for which it is collected and introduces a GDPR-like concept of restricting the processing of personal data for purposes that are not “compatible” with the purposes disclosed to the consumer.
    - It also would require businesses to disclose the length of time they intend to retain categories of personal information and prohibit retention of personal information for longer than necessary to achieve those purposes that have been disclosed to consumers.
- CPREA would add to the taxonomy of parties subject to the current CCPA by creating the concept of a “contractor.” The concept of a “contractor” and a “service provider” appear to be very similar, except that a service provider only processes personal information “on behalf of” the business from which it receives personal information. The ballot initiative contemplates that a contractor would be subject to similar contractual restrictions, including prohibitions on sale of personal information, restrictions on retaining, using, or disclosing personal information for any purpose other than to perform the services specified in the contract, and to make a certification to the business.
- Each of the service providers and contractors would be directly subject to CPREA, including obligations to provide assistance to the business with which it has a contractual relationship to respond to consumer requests. The ballot initiative also would require a written contract between businesses and service providers and businesses and contractors to include additional terms that: (1) restrict the purposes for which the personal information may be used; (2) obligate the contractor to provide at least the

same level of privacy protections as required under the CCPA; (3) allow the business to take "reasonable and appropriate steps" to ensure the contractor uses personal information consistent with the CCPA; (4) require notice if the contractor can no longer meet its obligations; and (5) give the business the right to take steps to stop and remediate unauthorized use of personal information. Businesses would be required not just to direct their service providers to delete personal information upon receipt of a verifiable consumer deletion request—but also to direct other third parties to which they have shared or permitted access to the information to delete the information. Each of the service providers and contractors also would have obligations to impose similar restrictions on subcontractors and to notify the applicable business of the use of such subcontractors.

- As drafted, a private right of action is available for certain data breaches that result from unreasonable security practices and only if a business does not cure the "violation" within 30 days' notice by a plaintiff. The ballot initiative would expressly state that implementation and maintenance of reasonable security procedures and practices following a breach would not constitute a "cure" that would serve as a defense to a claim.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice:

Libbie Canter	+1 202 662 5228	ecanter@cov.com
Yaron Dori	+1 202 662 5444	ydori@cov.com
Alex Scott	+1 650 632 4743	ajscott@cov.com
Lindsey Tonsager	+1 415 591 7061	ltonsager@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.