Data Privacy and Cybersecurity

California Consumer Privacy Act Catalyst Alastair Mactaggart Prepares New Ballot Initiative in Response to the California Legislature's Finalized Amendments

By: Kate T. Spelman and Effiong K. Dampha

On September 25, 2019, only 11 days after the California Legislature enacted its final, pre-effective date amendments to the California Consumer Privacy Act of 2018 (CCPA), Californians for Consumer Privacy frontman and founder, Alastair Mactaggart, filed a new privacy initiative set to appear on the November 2020 ballot—the California Privacy Rights and Enforcement Act.

Mactaggart was the initial catalyst behind the California legislature's swift development of the CCPA. Two years ago, Mactaggart spent nearly $3.5 million supporting an internet privacy initiative he sought to place on California's November 2018 ballot. To maintain control over the state's privacy laws, California lawmakers negotiated a deal with Mactaggart: in exchange for removing the initiative from the ballot, state lawmakers agreed to enact consumer privacy legislation, which ultimately became the CCPA.

On September 14, 2019, the Legislature finalized five amendments to the CCPA, which is set to go into effect on January 1, 2020. The Governor has until October 13, 2019 to sign off on the amendments.

According to Mactaggart, the Legislature's finalized version of the CCPA does not go far enough. Through his new initiative, Mactaggart proposes his own amendments to the CCPA, a redline version of which can be found here.

Below are some of the most significant CCPA amendments proposed in Mactaggart's new initiative:

- Adding a GDPR-like "sensitive personal information" classification as a new category of information subject to heightened protections. The category would include not only information typically thought of as sensitive (i.e., social security, driver's license and other identifying numbers and information revealing race, sexual orientation, health or union membership), but also the contents of private communications, biometric data, precise geolocation, and financial or other account numbers or log-ins and any related passwords. Businesses must receive affirmative consent to sell "sensitive personal information," and consumers would have the right to opt-out of the use of sensitive personal information for advertising and marketing purposes.

- Providing for the disclosure of consumer "profiling," defined as the "automated processing of personal information . . . to evaluate or predict aspects concerning that consumer's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." Consumers would have the right to know whether they are being profiled to determine eligibility for financial or lending services, housing, insurance, education admission, employment, or health care services, along with the algorithm used to profile consumers in these areas.

- Requiring that businesses selling personal information to a third party or disclosing such information to a service provider or contractor have contractual provisions in place that obligate the third party, service provider or contractor to protect personal information in accordance with the proposed act, and that grant the businesses the power to "take reasonable and appropriate

steps to help to ensure that the third party, service provider, or contractor effectively uses the personal information . . . ."

- Adding consumers' right to know whether their personal information is being used for "political purposes."

- Establishing a new agency, the California Privacy Protection Agency, to implement and enforce the proposed act. The agency would be responsible for adopting regulations, holding hearings and ordering violators to cease and desist and/or pay an administrative fine of $2,500 for each violation—or $7,500 for each violation involving children—to a specially created fund.

Many of these proposed changes, though seeking to broaden the scope of the CCPA, further complicate the operation of the CCPA. For example, under the proposal, businesses would need to get affirmative consent to sell data within the new category of sensitive personal information, potentially including geolocation data pinpointing a consumer within a half-mile radius, any data from scanning emails (if emails are private communications), and health-related browser and search history. The proposal, however, does not define what that affirmative consent would need to look like. Additionally, businesses that sell personal information to a third party would be required to put in their contract not only a provision requiring that the third party comply with the act, but also a provision allowing the business to oversee how the third party is using the data and even intervene and potentially claw back the data for non-compliance. This suggests that businesses have a continuing obligation to protect client data even once it is out of their hands, that businesses have a right to oversee third party use of data and that third party non-compliance may be a basis for breach of contract.

It remains to be seen whether state lawmakers will again attempt to strike a deal with Mactaggart and his organization, Californians for Consumer Privacy, before the Governor signs the current version of the CCPA into law.

Contact Us

Kate T. Spelman

kspelman@jenner.com | Download V-Card

Effiong K. Dampha

edampha@jenner.com | Download V-Card