CALIFORNIA PRIVACY RIGHTS AND ENFORCEMENT ACT OF 2020: WHAT YOU NEED TO KNOW

What has happened?

Alastair Mactaggart, Founder and Chair of the Californians for Consumer Privacy announced, on 25 September 2019, that he filed an initiative on the November 2020 ballot for the California Privacy Enforcement Act of 2020.

In particular, Mactaggart highlighted that his proposal would create new rights on the use and sale of sensitive personal information concerning, among other things, health and financial information, racial or ethnic origin, and precise geolocation.

Furthermore, Mactaggart highlighted how his proposal would enhance protection for violations of children's privacy by tripling fines under the California Consumer Privacy Act of 2018 ('CCPA') and establish a new authority, the California Privacy Protection Agency ('the Agency'), to enforce the law and provide guidance to industry and consumers.

Changes in scope

The definition of 'business' would be changed to mean an organisation that is:

1. For profit;
2. that collects consumers' personal information, or on the behalf of which such information is collected;
3. that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information;
4. that does business in the State of California, and that satisfies one or more of the following thresholds:
    a. as of 1 January of the calendar year, **had** annual gross revenues in excess of twenty-five million dollars ($25,000,000) **in the preceding calendar year**;
    b. alone or in combination, annually buys **or** sells the personal information of **100,000** or more consumers **or** households;
    c. derives 50 percent or more of its annual revenues from selling consumers' personal information.

The definition also covers joint ventures or partnerships 'composed of businesses in

which each business has at least a 40% interest.'

Moreover, the obligations have been expanded to cover not just businesses that collect personal information, but also those that **control the collection of information.**

Similar to the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), businesses should only collect consumers' personal information for 'specific, explicit, and legitimate purposes, and should not further collect, use, or disclose consumers' personal information for reasons incompatible with those purposes.'

The addition of 'sensitive personal information'

A new category of 'sensitive personal information' is proposed with additional obligations on businesses and additional rights for consumers. In particular, businesses must inform consumers of:

- the categories of sensitive personal information to be collected;
- the specific purposes for which the categories of sensitive personal information are collected or used;
- whether such information is sold; and
- the length of time the business intends to retain each category,

at or before the point of collection.

Consumers would have the right, at any time, to opt-out of the sale their personal information, **as well as** the right to opt-out of use or disclosure of their **sensitive personal information** for **advertising and marketing purposes**.

Businesses that are required to comply with the opt-out request must provide a clear and conspicuous link on their internet homepage **and in addition**, an easily accessible link that allows consumers to opt-out of the use or disclosure of the consumer's sensitive personal information for advertising and marketing.

If consumers exercise their right to opt-out of the use or disclosure of their sensitive personal information for advertising and marketing, businesses **must wait for at least 12 months** before requesting that the consumer authorise such use and disclosure.

New third party requirements

A business that sells that personal information to a third party or that discloses it to a service provider or contractor **will be required to enter into an agreement** that:

a. specifies that the personal information is sold or disclosed only for limited and specified purposes;

b. obligates the third party, service provider, or contractor to provide at least the same level of privacy protection;

c. grants the business rights to take reasonable and appropriate steps to help to ensure that the third party, service provider, or contractor effectively uses the personal information transferred in a manner consistent with the business's obligations;

d. requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required;

e. grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

Regarding the **right to deletion,** when a business receives a verifiable consumer request to delete personal information, service providers or contractors **must cooperate** with the business in responding and of the direction of the business, delete personal information about the consumer, **but shall not be required** to comply with a deletion request submitted by the consumer directly to the extent that it has collected, used, processed, or retained the consumer's personal information in its role.

A business, or a service provider or contractor, **will not be required to comply** with a consumer's request to delete the consumer's personal information if it is necessary for the business, service provider, or contractor to maintain the consumer's personal information in order to **detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions, and to help prosecute those responsible for such actions.**

Requests and disclosures

Requests for information are **no longer** limited to cover the 12-month period preceding the business's receipt of the request, and businesses would be required to disclose unless doing so would involve a disproportionate amount of information or would be unduly burdensome. Such requests or disclosures, however, would only apply to personal information collected after the effective date of the Act.

Profiling

Consumer would have the **right to request** whether the business is **profiling** for eligibility for financial/lending, housing, insurance, education admission, employment, or health care, including meaningful information about the logic involved in using consumers' personal information for profiling.

Children

A business **would be prevented from collecting or selling** the personal information of consumers if it has actual knowledge that the individual is less than 16 years, unless the child, in the case of at least 13 years and less than 16 years, or the child's parent or guardian, in the case of children who are less than 13 years, has consented.

Exemptions

Several exemptions from the obligations under the Act are also proposed, including where businesses are required to:

- comply with requests from government agencies for personal information for child welfare, foster care, adoption, parental support, etc.; and
- cooperate with government agencies if business has good faith belief that consumer is at risk of serious physical injury or heath and the situation requires a disclosure of personal information.

In addition, a consumer request for specific pieces of personal information to delete information, or to correct inaccurate personal information pursuant would not extend to personal information about the consumer that belongs to another natural person.

New enforcement and supervisory authority provisions

Civil penalties have proposed to be changed to administrative fines of not more than $2,500 for each violation, or $7,500 for each intentional violation or violations involving the personal information of minor consumers.

Fines shall be used to offset costs for the AG and the Agency, and a specific 'Consumer Privacy Fund' would be set up to provide a budget for the Californian Privacy Protection Agency funded from enforcement actions.

In addition, the Agency would be empowered to undertake investigations and issue cease and desist orders. If two or more persons are responsible for any violation or violations, they shall be jointly and severally liable.

The Agency would be formed of five members with the power, jurisdiction, and authority to implement and enforce the California Consumer Privacy Act. The Chair and one member would be appointed by the Governor, whilst the AG, Senate President Pro Tem, and the Speaker of the Assembly would each appoint one member.

A set of requirements and restrictions would be imposed on members including in relation to:

- qualifications and expertise in privacy and technology;
- confidentiality;
- independence;
- preclusion from employment for a period of one year after leaving office for a business subject to enforcement action within tenure or five years before appointment; and
- length of appointment, limited to no longer than 8 consecutive years.

On or after 1 July 2021 or within six months of taking authority, the Agency shall adopt, amend, and rescind regulations to further goals of the CCPA including regulations specifying record keeping requirements.

The Agency is also tasked with several additional functions, including:

- protecting the fundamental privacy rights of natural persons;
- promoting public awareness;
- providing guidance to companies and individuals;
- providing the legislature with technical assistance and advice; and
- establishing a mechanism for businesses not required to follow the CCPA, can certify that they are.

What's next?

The Attorney General will initiate a public review process following and comments will be accepted through to 25 October 2019.

HOW ONETRUST HELPS

With OneTrust, your organisation can take a holistic approach to CCPA compliance by leveraging a comprehensive suite of tools, each offering CCPA-specific functionality. By leveraging internal governance tools as well as consumer-facing tools, your organisation can pinpoint where personal data resides and how it is used; streamline your ability to act when consumers exercise their rights to information and deletion;

and manage opt outs relating to the sale of personal information. The OneTrust platform directly addresses CCPA requirements and sets organisations on the right trajectory for supporting a global privacy program.

CCPA Research & Readiness

OneTrust DataGuidance™

Use OneTrust DataGuidance™ to access a centralised resource aggregator that includes the full CCPA text, as well as summaries, comprehensive guides, and regulatory guidance. OneTrust DataGuidance™ is continually updated by the OneTrust global research team and includes latest amendments, news, and guidance.

Global Readiness & Accountability Tool

With the OneTrust Readiness & Accountability tool, leverage a research-backed CCPA readiness questionnaire, which helps assess your organisation's CCPA gaps and offers remediation recommendations to minimise risks.

CCPA "Do Not Sell" & "Consumer Rights"

Consumer Rights Management

The CCPA stipulates a 45-day response timeline for consumer data requests. With OneTrust, intake consumer rights requests and leverage CCPA-specific response workflows to help your organisation respond to requests appropriately, and with built-in exception handling, reduce unnecessary work.

Cookie Consent & Website Scanning

OneTrust offers default cookie banners that reflect CCPA-specific messaging. Using geolocation, OneTrust can display different cookie banners with different consent models depending on the website visitor's location.

CCPA Privacy Governance

Data Inventory & Mapping

CCPA-specific data elements built into OneTrust help your organisation track key attributes when mapping data for CCPA compliance. Additionally, leverage bulk importing capabilities to attach CCPA-specific data elements to existing data.

Assessment Automation

OneTrust Assessment Automation offers updated, CCPA-specific PIAs to adhere to

data minimization and purpose limitation considerations outlined under the CCPA. With Assessment Automation, take advantage of automated CCPA-specific risk flagging and research-backed remediation recommendations.

Vendor Risk Management

Leverage OneTrust Vendor Risk Management to communicate with third-party vendors to meet consumer requests for data access and deletion. Additionally, generate visuals to map vendors and data flows state by state and around the world.

Incident & Breach Response

OneTrust Incident & Breach Response enables your organisation to analyse incidents with a built-in, California Data Breach Notification assessment template. With customisable workflows, streamline response and quickly remedy a violation within the CCPA's 30-day cure period.

CCPA Consumer Engagement

Consent & Preference Management

OneTrust Universal Consent & Preference Management solution helps businesses maintain records of consent. Via OneTrust, offer a preference management centre and embed a link to enable consumers to opt out of the sale of their personal information and take more control over their settings