NEW ZEALAND
FOREIGN AFFAIRS & TRADE
Manatū Aorere

United States: California's New Digital Privacy Legislation

Market Report

5 January 2021

Prepared by the New Zealand Consulate-General in Los Angeles

Summary

- California voters recently passed the California Privacy Rights Act of 2020 - a California State ballot measure that aims to strengthen and enhance the state's digital privacy standards. The law, which will be operational in 2023, amends the current California Consumer Privacy Act of 2018 and adopts a number of European 'General Data Protection Regulation' (GDPR) principles. Many advocates of the new legislation are now optimistic that California will be able to achieve a level of data protection that would meet the EU's adequacy requirements.
- Any company that transacts business in California (no matter where they are physically located) and meets one of the following criteria will be subject to the law: annual revenue of US$25 million; buys, sells or shares the personal information of at least 100,000 Californian consumers a year; or makes more than half of its revenue from selling or sharing personal information.
- The law also creates a California data protection agency to be established in 2021 – the first of its kind in the US. The agency will have a dedicated funding stream and represents a significant increase in California's ability to enforce data protection rules.

Regional updates

1 This report provides an outline of changes to digital privacy law in California following the passing of the California Privacy Rights Act (CPRA), a California ballot measure in the November 2020 election. The New Zealand Consulate-General in Los Angeles spoke with California based digital privacy experts and academics as well as advocates of the privacy legislation.

2 The CPRA was the subject of a ballot measure voted on by Californians in the 2020 US General Election. The measure received 56 percent of the vote and subsequently passed. The CPRA will expand and strengthen California's current standards and will create a near-permanent baseline for California privacy law. This is because the CPRA is worded in such a way that any legislative amendments made to the law must be consistent with further enhancing consumer protections (and cannot derogate from existing protections).

3 Supporters of the measure stated that the objective of the CPRA was to ensure that California could achieve a level of data protection that would meet the EU's GDPR adequacy requirements. Advocates also note that the GDPR allows territories, not just countries, to be considered for adequacy. The hope is that the California framework will meet the EU's requirements and lead the way for the US.

4 The CPRA will have a wide application and include businesses that generate revenue from buying or selling personal information. Companies that do business in California and meet any of the following will be subject to the privacy law, no matter where the company is physically located:

- Generate more than US$25 million in annual revenue in the preceding year;
- Buys, sells or shares the personal information of at least 100,000 Californian consumers a year (up from 50,000 under the CCPA); or
- Makes more than 50% of its revenue from selling or sharing personal information.

5 The CPRA adopts certain GDPR principles, bringing it closer in line to GDPR than the current standards. The CPRA includes rules on:

- Data minimisation and retention: A business's collection, use, retention and sharing of personal information must be minimized to what is reasonably necessary to complete an interaction or transaction.
- Purpose limitation: Businesses must not collect or use personal information for a new purpose that is incompatible with previously disclosed purposes without first providing consumer notice.
- Storage limitation: Businesses must disclose, at the time of collection, their retention periods for each category of personal information. Businesses are further prohibited from retaining personal information for longer than is "reasonably necessary" for each disclosed purpose.

6 The CPRA introduces a new category of personal information called "sensitive personal information" and gives consumers the right to restrict businesses' use of that information. Sensitive personal information is defined to include health data, sexual orientation, race, origin, geolocation, financial data, genetic data, biometric data, and government identity information such as social security number and driver's licence. Businesses will be required to give consumers the option (through a link on their website) to limit the use of sensitive personal information to only that which is necessary to perform the service or provide the goods requested.

7 The CPRA will increase consumer protection by adding the following "rights":

- The right to correct data. Consumers may request correction of personal information that is inaccurate.
- The right to limit the use and disclosure of sensitive personal information.
- The right to opt-out of companies tracking precise geolocation.
- The right to opt-out of automated decision-making technology and consumer profiling.

8 In addition, the CPRA updates data protections for minors. The law will prohibit businesses from selling or sharing the personal information of children under the age of 16, unless consent is granted by consumer (when aged 13-16) or parent (for those under the age of 13). It also increases the financial penalties for mishandling the data of minors with fines of $7,500 per violation (three times higher than current law).

9 The CPRA also aims to clarify the scope and coverage of concepts and terms contained in the state's current privacy legislation such as the role of digital advertising and whether the "sale" of data applies to companies sharing personal information to a third party for "cross-context behavioural advertising". Cross-context behavioural advertising is targeted advertising that is sent to consumers based on their activities across several websites, applications, or services from different businesses. The CPRA directly regulates digital advertising by making it clear that consumers will have the right to opt-out of not only the sale, but also the sharing of personal information with third parties for cross-context behavioural advertising. The CPRA requires that if a third party organisation is sold or shared personal information, it must also comply with the CPRA and that this compliance is contractually bound.

10 The CPRA is also designed to increase the ability of the state to enforce privacy standards. The CPRA will create a new independent enforcement agency, the California Privacy Protection Agency. The new agency will be the first of its kind in the US, will take over enforcement of California's current data privacy law and have authority for issuing new regulations. The California Privacy Protection Agency will have a dedicated funding stream of US$10 million from the state. With this funding, the agency can hire around 50 full-time employees dedicated to making rules, pursuing investigations, and handing down enforcement actions. This indicates a significant ramping up in enforcement ability in California.

11 Now that the ballot measure has passed, the timeline for implementation begins with most provisions of the law not operational until 1 January 2023, giving businesses two years to come into compliance. The first step however, will be establishing the independent enforcement agency, which will be governed by an independent five member board. The agency will begin to be resourced in 2021 and will oversee compliance with the privacy legislation that will remain in place during the transition period.

12 It is likely that the passing of the CPRA will influence the privacy discussions of other US states as well as the discussions occurring at a US federal level.

More reports

View full list of market reports from MFAT at https://www.mfat.govt.nz/en/trade/mfat-market-reports

If you would like to request a topic for reporting please email exports@mfat.net

To contact the Export Helpdesk

Email exports@mfat.net

Call 0800 824 605

Visit Tradebarriers.govt.nz

Disclaimer