Calif. Privacy Law Resembles, Transcends EU Data Regulation

By **Natasha Kohne, Michelle Reed and Rachel Kurzweil** (November 13, 2020)

Natasha Kohne

Michelle Reed

Rachel Kurzweil

The newly passed Proposition 24, the California Privacy Rights Act represents the second time in two years that California has instituted a comprehensive privacy statute that fundamentally changes data privacy practices for most enterprises doing business in California.

While the CPRA builds on many of the provisions of the 2018 California Consumer Privacy Act, the differences between the two statutes are significant. Several of the new CPRA provisions are based on European Union General Data Protection Regulation principles with an eye toward obtaining an adequacy decision from the European Commission.

While balancing transparency, choice and flexibility for technological development, the CPRA also contains unique elements that set it apart from any privacy statute in the world.

Why another California privacy statute so soon?

The ink was barely dry on the CCPA, which went into effect earlier this year, before California's new CPRA made its way to the November 2020 ballot.

Reportedly disheartened by the number of statutory amendments proposed by special interests after the CCPA was enacted and the potential that such amendments could eviscerate the statute's key privacy protections, the founder of the CCPA, Alastair Mactaggart and his consumer advocacy group, Californians for Consumer Privacy, launched the CPRA to limit the possibility of any further amendments that, in their view, would significantly decrease obligations on businesses and restrict the privacy rights of Californians.

The CPRA imposes a distinct limitation not present in the CCPA, as the CPRA only permits amendments that "enhance privacy and are consistent with and further the purposes and intent of the Act."[1] This provision arguably allows the legislature to amend the CPRA with a simple majority only when the amendment benefits consumers, effectively creating a "one-way ratchet," as Mactaggart has described the provision.

Could European Commission Deem California an Adequate Jurisdiction?

The CPRA's enhanced privacy protections were clearly meant to position California as an adequate jurisdiction to which companies in EU Member States can transfer data pursuant to GDPR Article 45.

Earlier this year, the Court of Justice of the European Union in the Schrems II decision struck down the EU-U.S. Privacy Shield that facilitated data transfers from the EU to the U.S. and also put into question the effectiveness of Standard Contractual Clauses, a popular data transfer mechanism.[2]

Thus, a decision by the European Commission that California provides an adequate level of data protection for cross-border transfers from the EU would be welcomed and unprecedented for any state in the U.S. Such a decision could also spur other states to adopt privacy legislation similar to the CPRA.

However, whether the European Commission would be prepared to take such a bold step is unclear, particularly because the EU Court of Justice raised concerns in Schrems II regarding the reach of certain U.S. federal laws — Section 702 of the Foreign Intelligence Surveillance Act, Executive Order 12333 and Presidential Policy Directive 28. As those laws apply to companies in California, the European Commission might find it tricky to grant the state adequacy and still comply with the reasoning in Schrems II.

Nevertheless, the CPRA introduces several new provisions grounded in GDPR principles that could help California obtain an adequacy decision:

1. Right to Correction

While the CCPA provides consumers with a right to know what personal information a business collects and a right to delete personal information within certain parameters, the CPRA includes an additional right for Californians to correct inaccurate personal information. This concept is like the GDPR's right to rectification, which permits data subjects to rectify inaccurate personal data and to have incomplete personal data completed in some cases.[3]

2. Purpose Limitation, Data Minimization and Data Retention

Key privacy principles present in the GDPR include purpose limitation, data minimization and storage limitations.[4] Like the GDPR, the CPRA only permits businesses to collect personal information for "specific, explicit, and legitimate disclosed purposes" and "only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used, and shared."[5]

Additionally, the CPRA incorporates data retention limitations and, like the GDPR, requires that businesses disclose to consumers "the length of time the business intends to retain each category of personal information or if that is not possible the criteria used to determine such period."[6]

3. Protection of Onward Data Transfers

The CPRA's requirements regarding onward transfers of personal information also replicate GDPR principles. The CPRA specifies that businesses selling, sharing or disclosing consumers' personal information must enter into agreements with third parties, service providers or contractors that, among other things, require these entities to comply with applicable obligations, provide adequate privacy protection under the CPRA, and permit the business to confirm the third party's compliance.[7]

The CPRA further mandates that contractors and service providers notify the business when they use a subcontractor and that the subcontractor observe the same CPRA requirements as the contractor or service provider.[8]

GDPR Article 28 similarly specifies contract requirements for controllers and processors, including that the processor be governed by a binding agreement with the controller, that controllers only use processors "providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the

requirements" of the GDPR and that the use of subprocessors conform to certain conditions.

4. Independent Regulatory Agency

Another CPRA concept critical to the GDPR principles and likely an important aspect of issuing an adequacy decision is the creation of the California Privacy Protection Agency, the first dedicated privacy agency of its kind in the U.S.

Pursuant to GDPR Article 51, each member state must establish a supervisory authority to oversee the application of the GDPR in that member state. Notably, Recital 120 mandates that "[e]ach supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget."

Under the CCPA, the attorney general's allocation of funds toward privacy was discretionary and uncertain. In contrast, the CPRA now segregates funds for privacy regulation through the establishment of the Consumer Privacy Fund.[9]

5. Category of Sensitive Personal Information

The CCPA already featured one of the most comprehensive definitions of personal information of any U.S. privacy statute. But the CPRA creates two tiers of consumer data, adding the concept of sensitive personal information, which imposes stricter or additional obligations on businesses that collect, sell or share sensitive personal information, as opposed to just personal information.

This new category aligns the types of data protected by the CPRA with the data protected by the GDPR pursuant to which special categories of personal data deserve heightened protections.[10]

6. Automated Decision Making

GDPR Articles 13 and 14 require controllers to provide data subjects with information about the existence of automated decision making, including profiling and meaningful information about the logic involved and the significance and envisaged consequences of processing personal data for the data subject.

Article 22 further gives individuals the right, in certain circumstances, not to be subject to decisions based solely on automated processing, including profiling, that significantly or legally impact the individual.

Similarly, the CPRA demands that businesses disclose meaningful information to consumers about automated decision-making technology, including profiling information relating to analyzing or predicting aspects of a person's health, economic situation, interest, personal preferences, location, behavior, or interest or performance at work.[11]

7. Risk Assessments

Just as GDPR requires data protection impact assessments, in some cases, the CPRA requires the attorney general to issue regulations to ensure that businesses processing personal information that presents a significant risk to a California resident's privacy or security regularly submit a risk assessment to the CPPA.

The CPRA requires businesses to determine whether the benefits resulting from the

processing outweigh the risks to the consumer. Such a test is arguably borrowed from the GDPR's data protection impact assessment provisions, which require that in certain circumstances companies must carry out a prior risk assessment to evaluate the impact of the intended processing on the protection of personal data, consulting with the supervisory authority where the processing would result in a high risk.[12]

CPRA Elements That Go Beyond the GDPR

The CPRA also includes some unique attributes that set it apart from any privacy statute worldwide, encouraging innovation through explicit provisions while giving consumers more control over privacy choices.

Both the CPRA and GDPR contemplate technological advancement and the need to amend regulations in light of developments. GDPR Article 97 authorizes the European Commission to submit proposals reflecting developments in the information age.

The CPRA, however, is more explicit, mandating that regulations be updated to reflect changes in technology, including with regard to the definitions of deidentified, unique identifier and sensitive personal information as advancements are made.

Going further, the CPRA also identifies specific technological developments it expects to see through fruition. For example, Section 135 provides that consumers can send an opt-out preference signal indicating their intent to opt-out of a business's sale or sharing of their personal information or to limit the use or disclosure of their sensitive personal information.

The attorney general is also directed to adopt regulations defining the requirements and technical specifications for an opt-out preference signal and other opt-out mechanisms. Such provisions appear to be forward looking and suggest that the opt-out preference signal requirements should be updated "from time to time to reflect the means by which consumers interact with businesses."

Notably, comments from the attorney general about a similar provision on global privacy controls in the CCPA regulations stated that such a provision "encourages technology vendors to work with businesses to build global privacy controls that can be customized per website or businesses."

Another unique aspect of the CPRA is giving consumers the option of exchanging their personal information in return for enhanced services. Under CCPA Section 1798.125, businesses may offer consumers financial incentives, such as payments to consumers or a different price, rate, level or quality of goods or services if the incentive reasonably relates to the value provided by the consumers' data.

The CPRA now clarifies that provision, stating that incentives may be offered for the retention of personal information and that the value of the data is determined by the "value provided to the business by the consumer's data."[13]

Though the GDPR does not specifically address incentive programs, offering a different quality of goods or services on the condition that an individual consent to the processing of his or her personal data that is not necessary for the provision of the services might contravene the GDPR's requirement that consent be freely given.

Guidance from the European Data Protection Board contemplates that the GDPR does not preclude all incentives, but places the onus on the business to demonstrate that consent

was freely given and that withdrawal of consent does not result in a service being downgraded. In contrast, the CPRA arguably provides consumers with the choice to consent to the processing of their personal information in exchange for a different price or quality of services.

Conclusion

As businesses grapple with the CPRA and prepare for the majority of the provisions to become operative in 2023, they will likely turn to GDPR resources for guidance, and further similarities between the two statutes may emerge.

Whether California will become the first state to receive an adequacy decision from the European Commission remains to be seen, particularly in light of the concerns presented in Schrems II, but it is undeniable that the CPRA has heralded in a new era of privacy protection in the U.S.

Natasha Kohne and Michelle Reed are partners, and Rachel Kurzweil is an associate, at Akin Gump Strauss Hauer & Feld LLP.

Akin Gump counsel Jenny Arlington and Molly Whitman contributed to this article.

[1] CPRA, 2020 Cal. Legis. Serv. Prop. 24 § 25.

[2] Data Prot. Comm'r v. Facebook Ireland & Maximillian Schrems, Case C-311/18 ECLI:EU:C:2020:559 (July 16, 2020) ("Schrems II").

[3] See GDPR Arts. 5 & 16.

[4] GDPR Art. 5.

[5] CPRA § 3(A).

[6] Id. § 4.

[7] CPRA § 4.

[8] Id. § 14.

[9] See CPRA § 18.

[10] See GDPR Art. 9 & Recital 51.

[11] CPRA § 21.

[12] See GDPR Arts. 35 & 36.

[13] CPRA § 11.