Strategic Perspectives

California Privacy Rights Act Nudges State Closer to the GDPR

By *Jena Valdetero,* Shareholder, *Greenberg Traurig, LLC*

This is the first in a series of three Strategic Perspectives that will appear monthly through November in the Cybersecurity Policy Report to help subscribers prepare for the impending applicability of new state laws in 2023, as well as highlight increasing regulatory and enforcement activity at the state and federal levels. This article, from Jena Valdetero, Co-Chair of the U.S. Data, Privacy and Cybersecurity practice at Greenberg Traurig, LLP, focuses on the significant substantive changes made by the California Privacy Rights Act (CPRA), which takes effect on January 1, 2023.

After Europe blazed the trail by passing the sweeping General Data Protection Regulation ("GDPR") in 2016, California followed closely in the footsteps of European efforts by passing the most comprehensive data privacy law in the United States, the California Consumer Privacy Act (the "CCPA"). Effective January 1, 2020, the CCPA provided a number of obligations for businesses and rights for consumers. Although similar in many respects, the GDPR and CCPA are not identical. With the passage of the California Privacy Rights Act of 2020 (the CPRA), California is seeking to close some of the gaps between the CCPA and the GDPR.

Unlike the GDPR, which applies to all businesses processing personal information, the CCPA does not apply to all California businesses. Instead, businesses must meet one of the following minimum thresholds:

- Have annual gross revenue in excess of $25 million;
- Buy, receive for the business's commercial purpose, sell, or share for commercial purpose, the personal information of at least 50,000 California residents, households, or devices; or
- Derive 50 percent or more of its annual revenue from selling consumers' personal information.

When the CPRA takes effect in January 2023, the minimum number of Californians for which the collection of personal information triggers application of the CPRA increases from 50,000 to 100,000. In addition, a company must buy, sell, or share that quantity of consumer information to trigger the statute (as opposed to simply receive the information for a business purpose).

The CPRA was enacted by the voters of California via a ballot referendum on November 3, 2020, although most of its substantive provisions do not become operative until January 1, 2023, and enforcement will not begin until July 1, 2023.

The CPRA made a number of amendments to the CCPA, which are outlined below. The biggest substantive change, however, is the sunsetting of the exemptions from most requirements of the CCPA for data collected about employees and data collected in the context of B2B relationships. This change mirrors the GDPR, which applies to all personal information regardless of the context in which it is collected.

Data Subject Rights

The CCPA grants California consumers the right to access personal information held about them and request deletion of such information, although those deletion rights are subject to multiple exceptions. Consumers also must be informed if their personal information is sold and have the right to opt out of the sale.

The CPRA grants the following additional rights:

- The right to fix errors or correct inaccurate personal information;
- The right to opt out of information sharing with third parties for behavioral advertising across websites,
- The right to object to certain uses of an individual's "sensitive" personal information; and
- The right to object to certain forms of automated decision making and profiling (note, however, that the right to opt out of automated decision making will only go into effect if, and when, the California Privacy Protection Agency finalizes regulations relating to such right).

A New Category: Sensitive Information

Although the CCPA included multiple examples of data considered to be personal information, the CPRA introduces "sensitive personal information," identified to include each of the following types of information:

- Biometric information
- California Identification Card number
- Contents of consumer's email
- Contents of consumer's mail
- Contents of consumer's SMS texts
- Credit or debit card number (with required security code or password)
- Driver's license number
- Ethnic origin
- Financial account number (which permits access to the account)
- Genetic data
- Health information
- Passport number
- Philosophical beliefs
- Precise geolocation
- Racial origin
- Religious beliefs
- Sex life or sexual orientation
- Social Security Number
- Trade union membership

The CPRA permits businesses to use sensitive personal information for the following purposes without offering consumers a right to opt out:

1. Performing services reasonably expected by the consumer;
2. Providing goods reasonably expected by the consumer;
3. Ensuring the security and integrity of the consumer's information;
4. Other short-term and transient uses (e.g., serving one-time advertisements);
5. Performing services on behalf of a business; and
6. Product or service improvement.

Beginning on January 1, 2023, if a business chooses to use sensitive personal information for something other than one of the purposes described above, the business is required to provide a notice to consumers that, among other things, informs them that they have a right to opt out of the additional use. The business also will be required to include a link on its homepage titled "Limit the Use of My Sensitive Personal Information."

Restrictions on Sharing Personal Information

While the CCPA requires companies who sell personal information to give notice and the right to opt out, the CPRA introduced the term "sharing" and similar restrictions. However, the term "sharing" has caused confusion because it refers to a very narrow set of transfers.

Personal information will be "shared" for the purposes of the CCPA only when it is provided to a third party for the specific purpose of "cross-context behavioral advertising." The term "cross-context behavioral advertising" includes only the "targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts." In general, this refers to adtech providers utilizing third party cookies to track users across websites for targeted marketing.

Expansion of the Definition of "Exempt Publicly Available Information"

The CPRA broadened the category of "publicly available information" to include the following:

- Information that is lawfully made available from federal, state, or local government records;
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or
- Information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

Private Right of Action

Although the CCPA does not permit Californians to sue for violations of privacy provisions, it does permit residents whose sensitive personal information is exposed in a data breach to bring such an action. Actual damages are not required; affected residents can sue and recover between $100-750 per violation.

The CPRA added an additional data type which, if exposed in a breach, would permit a resident to sue under the CPRA: the consumer's email address in combination with a password or security question and answer that would permit access to the email account.

Service Provider Agreements

In order for businesses to share personal information with third parties who are performing services on their behalf, businesses must enter into written agreements that prohibit service providers from, among other things:

1. Selling or sharing personal information;
2. Retaining, using, or disclosing personal information "outside of the direct business relationship between the service provider and the business;" and
3. Combining (subject to some exceptions) the personal information that the service

provider receives from one business with information that it receives from another business.

The CPRA also adds two separate categories of contractors: "contractors" and "independent contractors." It has redefined the concept of "contractor" used in the CCPA to be an "independent contractor," and it has created a new definition for "contractor" that substantially resembles the definition of "service provider." The only significant difference between a contractor and a service provider appears to be that contractors provide a "certification" in which they state they understand their contractual limitations and will comply with them. As a functional matter, it is not clear whether providing such a certification would have any different legal status, or effect, as compared with a standard contractual representation, warranty, guarantee, or agreement.

Accountability and Data Retention

The CPRA will create two additional categories of core requirements: (1) the ability to process and retain data, which will require a business to, among other things, have a record retention policy and minimize data collected, and (2) business accountability and governance, in which some companies will be required to conduct security risk audits and privacy risk assessments (note that this provision will only become effective if, and when, the California Privacy Protection Agency issues regulations addressed to this topic).

Similar to the GDPR, which prohibits companies from retaining personal data when they no longer have a legal basis to process it, the CPRA requires that businesses "not retain personal information or sensitive personal information . . . for longer than is reasonably necessary for that disclosed purpose for which it was collected." The CPRA also states that a "business' collection [and] use" of a consumer's personal information "shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed."

In addition, the CPRA will require that businesses inform consumers at the point at which information is collected of "[t]he length of time the business intends to retain each category of personal information" that it collects. If it is not possible for a business to provide consumers with a specific retention period, the business is instructed to disclose "the criteria used to determine that period. . ."

Data Security

The CPRA amended the CCPA to require that the California government issue regulations requiring businesses whose processing of consumers' personal information "presents a significant risk to consumers' privacy or security" to perform a "cybersecurity audit on an annual basis." The factors to be considered when determining whether processing poses a significant risk to the security of personal information include the size and complexity of the business and the nature and scope of the processing activities. Thus, it is possible that the regulations will not require all businesses to undergo a security audit.

Enforcement

Currently, the CCPA is enforced by the California Attorney General. The CPRA created a new agency, the California Privacy Protection Agency ("CPPA"), which will enforce violations of the CCPA as amended by the CPRA. The CPRA also removes the 30-day cure period businesses have under the CCPA to cure a violation before being fined.

Takeaways

Companies concerned about compliance should consider the following:

- **Revise Privacy Notices** – Privacy notices will need to be updated to advise consumers about their new rights and disclose the period of time each category of personal information will be retained.

- **Conduct a Data Inventory** – In order to ensure compliance with a number of new requirements, including entering into service provider agreements and ensuring data is deleted when it is no longer needed for processing, companies may find it most efficient to inventory all types of personal information collected. A data inventory will also help companies identify if they are processing sensitive information and ensure it is doing so for a permissible purpose.

- **Implement a Data Retention Policy** – Perhaps the biggest lift will be creating a data retention schedule and ensuring compliance, considering the treasure trove of data most companies hold. A data retention policy will ensure compliance with the CPRA and also minimize risks in the event of a data security incident.

- **Update Service Provider Agreements** – Contracts should be reviewed with any third party to whom an organization entrusts personal information to ensure compliance with the restrictions set forth in the CPRA around a service provider's use of personal information.

- **Evaluate Cookie Banners** – The new requirements around requiring consumers to opt out of the sharing of their personal information for behavioral advertising purposes should spur companies to review their cookie preferences and banners to ensure compliance.

- **Review Data Security Measures** – In light of the data breach private right of action and the increase in data security incidents in the last two years, companies should conduct a review of their security measures and shore up any risks by implementing multi-factor authentication, increasing audit trails and logging, and upgrading antivirus and endpoint detection tools.

Despite the CPRA containing numerous new requirements, the CPPA has proposed dozens of pages of regulations that would impose numerous requirements on businesses, particularly those who might be selling or sharing data. Because those regulations are not final, businesses should expect to make updates to their privacy notices and procedures after the regulations are implemented.