The New Year Brings New Data Privacy Obligations via the California Privacy Rights Act and Virginia Consumer Data Privacy Act

On Jan. 1, 2023, both the California Privacy Rights Act (CPRA) and Virginia Consumer Data Privacy Act (VCDPA) come into effect, introducing new and updated data privacy and security obligations to covered entities. As these acts will apply to private entities located outside of California and Virginia, respectively, organizations across the country should begin assessing their data use policies and making any updates necessary to avoid regulatory attention and hefty fines. Please note that the summaries below are not intended to be comprehensive.

The California Privacy Rights Act

The CPRA, also known as Proposition 24, will significantly modify and expand existing rights and obligations under the landmark California Consumer Privacy Act (CCPA). A summary of some of the more impactful changes are laid out below.

- ***Clarification of the CCPA's Existing Applicability.*** Generally, the CCPA governs for-profit entities that do business in California and meet one of the following criteria:
    - Have a gross annual revenue of over $25 million;
    - Buy, receive, or sell the personal information of 50,000 or more California residents, households or devices; or
    - Derive 50% or more of their annual revenue from selling California residents' personal information.

  The CPRA modifies these criteria by: (1) clarifying that the revenue threshold should be calculated from January 1 of the preceding year; (2) increasing the threshold of California residents from 50,000 to 100,000; and (3) clarifying that the 50% revenue threshold also includes sharing of consumer's personal information for cross-context behavioral advertising.

  The CCPA also applies to entities that control or are controlled by a business that meets the requirements listed above, provided that this additional entity shares common branding with the covered business. In addition to common branding, the CPRA will now require these entities to receive personal information from the covered business for purposes of cross-context behavioral advertising. In contrast to the CPRA's threshold-based definition above, the act does not reference a for-profit requirement here, suggesting that the controlling or controlled entities classification may extend to non-profit organizations. Thus, a covered business may bring an otherwise exempt entity under the purview of the CPRA.

The CPRA defines cross-context behavioral advertising as 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." For example, if a covered entity's subsidiary that is not subject to the CPRA (1) shares a name, service mark or trademark with the covered entity and (2) receives personal information from the covered entity for purposes of generating targeted ads, this subsidiary will also be subject to the CPRA.

- ***Expansion of the CCPA's Applicability.*** The CPRA expands the CCPA's applicability by adding two new classifications of covered entities. The first classification is joint ventures and partnerships where independent businesses have at least a 40% interest. Notably, classification as a joint venture may not excuse a participating business that meets the thresholds above from individual regulation. The newly formed California Privacy Protection Agency could promulgate regulations to clarify this dynamic between joint ventures and individual businesses in the coming months. The second category is a certified business, which includes entities that (1) do business in California and (2) voluntarily certify to the California Privacy Protection Agency that they are in compliance with and agree to be governed by the CCPA and CPRA.
- ***Addition of "Sensitive Information" Category*.** Inspired by the European Union's General Data Protection Regulation (GDPR) definition, the category includes personal information that reveals a consumer's SSN, driver's license number, passport number, account credentials, precise geolocation, racial or ethnic origin, religious beliefs, biometric data, personal information concerning a consumer's health or sex life or sexual orientation, as well as contents of a consumer's mail, email and text messages.
- ***Sunsetting Certain CCPA Provisions and Exceptions*.** The CPRA will eliminate the following CCPA provisions on Jan. 1, 2023:
    - The exception for employee personal information and business-to-business information;
    - Certain broad exceptions available for the CCPA's right to delete; and
    - The 30-day curative period for CCPA violations.
- ***Expansion of Consumer Rights*.**
    - The CPRA expands the "Do Not Sell" opt-out requirement to include the sharing personal information for purposes of cross-context and/or third-party advertising.
    - Similar to the GDPR, the CPRA grants consumers a new right to correct inaccurate information.
    - The CPRA also expands consumer rights by allowing consumers to limit a business's use or disclosure of sensitive personal information.
- ***Expansion of Vendor Classifications and Obligations.*** The CPRA provides clarity regarding the types of third parties that may be subject to the act. "Service provider" is defined as a "person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant

to a written contract." "Contractor," a new class of third-party under the CPRA, is defined as a "person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract." The definition of "third party" operates as a catchall term and includes any entity that is not the covered entity, service provider or contractor.

Along with the revamped third-party classification scheme, the CRPA also includes heightened obligations for covered entities that contract with such vendors. First, covered entities must take steps to include the CPRA's use limitations and privacy rules in contracts with vendors to ensure personal information remains protected through the supply chain. Second, contracts must include certain language to allow covered entities to confirm that vendor processing is consistent with CPRA requirements.

Vendors also have heightened obligations under the CPRA and are required to:

- Assist covered entities in maintaining appropriate technical and organizational measures;
- Limit use of personal information at the request of the covered entity; and
- Assist the covered entity in responding to verifiable consumer requests.

While many of the changes introduced by the CPRA are clear, covered entities and consumers alike will likely have to wait until April 2023 for regulations to add detail to some of the more general updates. Private entities should not wait for these regulations before beginning compliance efforts as the elimination of the 30-day curative period means fines arising from violations could be levied immediately. Currently, the CCPA allows the California Attorney General's office to seek civil penalties of $2,500 for each violation or $7,500 for each intentional violation in addition to a private right of action.

The Virginia Consumer Data Privacy Act

The new year will mark Virginia's entry into data privacy regulation with the introduction of the VCDPA, an act remarkably similar to the CCPA in many respects. Much like the CCPA, the VCDPA establishes threshold-based applicability criteria that extends the act's reach far beyond the bounds of the state. The VCDPA applies to entities that conduct business in Virginia or market goods and services to Virginia residents and either (1) control or process the personal data of at least 100,000 Virginia residents; or (2) control or process the personal data of at least 25,000 Virginia residents and derive more than 50% of their gross revenue from the sale of personal information. The following is a brief overview of some of the more significant provisions that entities will need to comply with beginning on Jan. 1, 2023.

- ***Establishment of Consumer Rights*.** Like the GDPR and CCPA, the VCDPA extends familiar data protection rights to Virginia consumers including:
    - The right to know, access and confirm personal data;
    - The right to delete personal data;
    - The right to correct inaccuracies in personal data;
    - The right to data portability;
    - The right to opt out of the processing of personal data for targeted advertising purposes;

- The right to opt out of the sale of personal data;
- The right to opt out of profiling based upon personal data; and
- The right to not be discriminated against for exercising any of the foregoing rights.

- ***Notice and Consent Obligations for Sensitive Data.*** Prior to collecting certain categories of sensitive personal information, such as genetic, biometric or location data, covered entities will be required to obtain consent from Virginia consumers.
- ***Purpose Limitation and Data Minimization.*** The VCDPA aligns with both the GDPR and CCPA by requiring covered entities to collect and retain personal information only for as long as is necessary to fulfill a specific purpose and to comply with record retention laws.
- ***Reasonable Security Practices.*** The VCDPA will require covered entities to establish and maintain "reasonable" data security practices to protect the confidentiality, integrity, and accessibility of personal information. Covered entities will have to wait on regulators and/or the courts to flesh out what constitutes "reasonable" security practices.
- ***Vendor and Third-Party Compliance.*** The VCDPA will require covered entities to include the act's data privacy safeguards in any contracts with vendors who process personal information on behalf of the covered entity.

Unlike the CCPA, the VCDPA does not provide consumers with a private right of action. The Virginia Attorney General has enforcement authority, however, and can levy civil penalties up to $7,500 per violation.

Preparing for Compliance in 2023

With less than a week until both the CPRA and VCDPA come into effect, entities should be evaluating their compliance efforts and working to update internal and public-facing data use policies, and developing procedures to comply with these legal obligations, Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including compliance with state and federal privacy laws.

If you have any questions about the CCPA or VCDPA compliance or would like assistance with creating or updating data use policies, please contact Jessica Copeland, CIPP/US; Amber Lawyer, CIPP/US & CIPP/E; Mario Ayoub; or any attorney in Bond's cybersecurity and data privacy practice.

BOND SCHOENECK & KING ATTORNEYS