Are You Ready For 2023's New Data Privacy Laws?

January 5, 2023

California continues to serve as the primary driver of privacy law in the United States, but other state laws now warrant compliance. The California Privacy Rights Act (CPRA), effective January 1, 2023, amends and extends the existing California Consumer Privacy Act (CCPA). The revised law is still generally referenced as the CCPA.

Other states have followed California's lead. Virginia's Consumer Data Protection Act went into force on New Year's Day. The Colorado Privacy Act and Connecticut's new privacy law will become effective mid-year, on July 1, 2023, and Utah's Consumer Privacy Act goes into effect on December 31, 2023.

New California Obligations

New Sheriff in Town. A new well-funded state agency, the California Privacy Protection Agency (CPPA), is poised to take over CCPA enforcement this year. It is expected to be far more aggressive than the California Attorney General has been in bringing enforcement actions.

An Expansive View of Data "Selling" and "Sharing." In August 2022, the California Attorney General reached a $1.2 million settlement with Sephora, the makeup and skincare retailer, finding that its sharing of consumer data with analytics and social media companies for discounted services or other non-cash compensation is a "sale" under the CCPA, requiring a "Do Not Sell my Personal Information" button on the company's website and other actions. See our Client Alert on that first enforcement action. Under the CCPA, a company should have contractual provisions in place with vendors and service providers limiting the use and disclosure of personal information shared.

Awareness of Data Tracking Mechanisms. The CPPA will likely look ever more closely at how businesses track personal information and what notice they provide and type of consent they obtain. Companies should review their cookie policies and how they manage consent when sharing personal information with third parties for purposes of targeting advertising. In the *Sephora* enforcement action, the California Attorney General suggested that a company's recognition of the Global Privacy Control browser tool would satisfy some of these obligations, but use and acceptance of the GPC is not widespread to date.

Data of Employees and Applicants. The CPRA amendments to the CCPA removed the moratorium on employee and applicant data as of January 1, 2023. These individuals will be able to request the information your company has about them, and to request you to delete, correct or limit use or sharing of their information. We anticipate that many DSAR requests in 2023 will seek such employment-related data.

Personal Information Collected as Part of a B2B Relationship. The business email address of a vendor or customer representative is now "personal information" under the CCPA. Most businesses and their representatives will not be overly concerned with such data, but it is now covered under the California law. Companies must still be extremely mindful of consumer data shared via B2B relationships.

New Privacy Laws in Virginia, Connecticut, Colorado and Utah

Jurisdictional Thresholds Differ. Virginia and Colorado have similar jurisdictional frameworks, but they are not identical. In general, a company that conducts business in a state or produces products or services targeted to its residents will be covered if, during the last calendar year, they also controlled or processed the personal information of a certain number of consumers in the state and/or derived a certain percentage of revenue from the sale of that information. In Connecticut, there is no annual revenue threshold, meaning that a substantial level of revenue will not automatically trigger coverage, nor will a minimal level of revenue exempt a company from coverage. Connecticut's law also exempts personal information used for payment transactions.

No Coverage of Employee Data. In contrast to the CCPA, the Virginia, Connecticut, Colorado and Utah laws are limited to consumers and do not cover employees.

HIPAA and GLBA Exemptions. The California exemptions for the federal Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act are data-specific, and not entity-level exemptions. Thus, the CCPA does not apply to Protected Health Information (PHI) collected by a covered entity or business associate that is governed by the privacy, security, and breach notification rules of HIPAA. Likewise, the CCPA does not apply to nonpublic personal information (NPI) subject to the GLBA's Privacy and Safeguards Rules. In contrast, states like Connecticut and Virginia not only exempt such data, but the entities subject to the HIPAA and GLBA regulatory requirements for data security and privacy.

Colorado's Law Appears to Apply to Non-Profits. Unlike the other states referenced, which specifically exempt non-profits from their privacy laws, Colorado applies its law to entities that conduct business in Colorado or which "produce products or services that are targeted to the residents of the state."

Consideration Needed to Be a "Sale" of Data. In Virginia and Utah, a sale occurs when personal data is exchanged for monetary consideration only. California, Connecticut and Colorado adopt a broader definition that includes an exchange of data for "other valuable consideration."

Universal Contractual Language Needed. All the new state data privacy laws have requirements regarding contracts with parties who may have access to or process personal data on behalf of a business. These mandatory contract provisions restrict the use and sharing of data and require assurances that the vendor will exercise the same level of protection for any personal data.

Potential for Data Privacy Impact Assessments (DPIA). The CPRA empowered the CPPA to issue regulations that might require a business to conduct and submit a risk assessment for certain data processing activities, but the agency has yet to promulgate any. Colorado and Virginia data privacy laws require privacy impact assessments if a business processes personal data that presents a "heightened risk of harm" to consumers.

Prudent Next Steps

Companies should review their privacy policies, cookies, tracking mechanisms and other aspects of their privacy program in light of these new legal obligations. Legal compliance is a complicated and multifaceted process and requires a team effort. To mitigate risk and liability, privacy programs must continuously adapt as new laws come into effect.

If you have any questions about what steps are best for your business or organization to comply with these new laws, please contact Tedrick Housh or Michael Cohen in our Data Privacy and Cybersecurity Compliance group.