November 18, 2020

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.com
An ALM Publication

Businesses Should Prepare for a New Phase of Privacy Regulation and Enforcement in the United States

The continuing shift in privacy law embodied by the California Privacy Rights Act is set to make a significant impact on businesses' compliance efforts and operational risk, as well as individuals' expectations, says Gibson, Dunn & Crutcher's Cassandra Gaedt-Sheckter, Alexander H. Southwell and Ryan Bergsieker.

By Cassandra Gaedt-Sheckter, Alexander H. Southwell and Ryan Bergsieker

Californians have ushered in a law protecting individuals' privacy unlike any other in the United States, and businesses are well-advised to evaluate its impact and prepare to comply. Proposition 24, which passed last week, establishes the California Privacy Rights Act (CPRA), which will take effect Jan. 1, 2023. If this seems like déjà vu, it is because just two years ago, the California legislature passed an unprecedented privacy law, the California Consumer Privacy Act (CCPA), which the CPRA amends. The continuing shift in privacy law embodied by the CPRA is set to make a significant impact on businesses' compliance efforts and operational risk, as well as individuals' expectations.

Take Steps Internally To Prepare for New Rights and Requirements

Businesses should take comfort that the Jan. 1, 2023 effective date, and delayed enforcement start (July 1, 2023), means there is time to come into compliance. However, the law imposes various changes that will require businesses to address new considerations—even factoring in the efforts many already have made to comply with the CCPA—including:

- Determining what "sensitive information" is maintained. Businesses must now differentiate between general "personal information" and "sensitive information," the latter of which requires additional compliance measures, including relating to disclosing the collection and use of such information, and a new right for consumers to limit the business's use of the information.

(Courtesy photo)

Gibson, Dunn & Crutcher's Cassandra Gaedt-Sheckter, Alexander H. Southwell and Ryan Bergsieker

- Reconsidering whether the business "sells" information, and providing an opt out. CPRA explicitly expands the CCPA's definition of "sale" to include sharing of personal information even without exchange of money, and "cross-context behavioral advertising." As a result, businesses that fell outside of the CCPA definition of "sale," may fall within the CPRA definition. Further analysis will require digging into the business's advertising activities (e.g., business practices in ad tech, advertising-related contracts, whether uses of personal information provided by the business to third parties are limited to the business's purposes, and uses of cookies and pixels), and whether additional efforts to minimize data sharing or cross-contextual use is necessary. In light of CCPA, certain tech companies have afforded options for limiting such data uses, and other advances are likely to result from the CPRA.
- Laying the groundwork for employees/contractors and individuals whose personal information is gathered in B2B transactions. Although various exemptions have governed the handling of this data under the CCPA, under the CPRA businesses will need to consider their own California workforce and California business contacts as consumers. Particularly in light of COVID-19, businesses are collecting sensitive information from employees with more frequency than ever before. Mapping out the information collected, how it is used, and where it is going will be particularly important to comply with requests, including rights to access, delete, or limit the use of data.
- Evaluating data minimization and data retention practices. The CPRA is the first U.S. law to

memorialize rights to data minimization (only using information as necessary) and limited data retention. Whereas data retention policies and minimizing collection of information were previously best practices in the United States, failure to address these will now be an actionable violation.

- Updating disclosures—again. Businesses will need to update their privacy policies, web links, and other disclosures to cover CPRA and individuals' additional rights, including relating to the sharing opt-out and limited use option, discussed above. Once again, however, businesses have another two years (Jan. 1, 2023) before these disclosures are required.
- Reviewing third party relationships where personal information is shared. Businesses should again consider amendments to agreements with third parties, including to ensure that new obligations and distinctions are covered, such as the obligation that service providers must assist businesses with executing individual rights.

Businesses will need to remain nimble in their efforts to come into compliance, as the law will undoubtedly morph in light of implementing regulations that may not be finalized until approximately 18 months from now. In addition, the act adds 15 areas of regulation that the California Attorney General (and then a new agency, as discussed below) will need to promulgate, ranging from which entities are required to do an annual cybersecurity audit, to identifying for what purposes service providers may use personal information outside of the written contract with the business, to defining "precise geolocation."

Watch Development and Staffing of New Agency To Assess Enforcement Risk

Significantly, the CPRA establishes a new agency to take over governance of the CPRA from the California Attorney General, the California Privacy Protection Agency. The Agency's leadership will be appointed by Feb. 1, 2021—just a few months from now—and it is set to monitor, administratively enforce, implement, regulate, and otherwise govern the CPRA.

CPRA does not materially expand an individual's right to bring suit—which is still limited to certain data breaches—but a new, dedicated agency is intended to make enforcement more active. The California Attorney General's Office has stated in the past that it does not have sufficient resources to enforce the CCPA, and the CPRA sought to remedy this by including a $10 million annual budget in the law (after fiscal year 2020-2021) for the Agency from the General Fund of the state in order to staff more than even the FTC. If civil penalties are on par with those in FTC Section 5 enforcement matters, they may range in the millions of dollars, particularly as the fines under the CPRA can range from $2,500 to $7,500 per person per incident.

Watch Other States and the Federal Government

Consistent with various other areas of law, we expect these bold moves in California to foreshadow what will come across the country, potentially through establishment of a patchwork of state laws (similar to data breach notification laws, which differ by state). Indeed, following CCPA, a multitude of state and federal laws were introduced, and while most did not succeed, this round may be different—a new administration, another year into CCPA, an even stronger CPRA, and the unique introduction through a ballot initiative in California might very well spur new legislative and initiative-driven laws in the near future. Because of this, businesses and practitioners should pay attention to the requirements of CPRA, including in anticipation of copy-cat laws across the country.

Keep Business Leaders Apprised and Involved

Finally, businesses should make CPRA and its implications a topic of conversation, not just in legal departments, but also with management and C-suites, whether they are in California, another state, or abroad. Because the law affects entities "doing business" in California, it will not be a regional issue, and privacy will continue to be a business issue, rather than a solely legal issue. That is, whether relating to budgeting for compliance purposes, satisfying consumer expectations, ensuring positive public relations and communications, forecasting the effect of potentially operation-altering requirements (including relating to advertising), or risk disclosure purposes for publicly-traded companies, this topic will likely need to be at the forefront of many businesses' considerations in planning for the future.

Cassandra Gaedt-Sheckter *is a senior associate in Gibson, Dunn & Crutcher's Palo Alto office. Her practice focuses on data privacy and cybersecurity litigation and counseling, technology-related class actions, and trade secret disputes.*

Alexander H. Southwell *is a partner in Gibson Dunn's New York office. He is a co-chair of the firm's privacy, cybersecurity and consumer protection practice group.*

Ryan Bergsieker *is a partner in Gibson Dunn's Denver office. His practice is focused on government investigations, complex civil litigation, and cybersecurity/data privacy counseling.*