ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
OCTOBER 19, 2022

Navigating different obligations of next year's state privacy statutes

■ Anna Mercado Clark and Michael Staszkiw

BUSINESSES HAVE a limited amount of time remaining to prepare for various comprehensive privacy laws that will take effect next year. Five states have comprehensive privacy laws that will take effect: California (update to existing law), Virginia, Colorado, Connecticut and Utah. These laws may apply even to organizations that are located in New York State.


Clark


Staszkiw

Generally, these laws grant consumers certain rights over their own personal information and impose requirements on how businesses collect, handle, process and share such information. Although these laws have similarities, they do have key differences. Compliance with these laws can be confusing and overwhelming, especially given state regulators' potential enforcement.

PRIVACY LAWS OUTSIDE OF NEW YORK STATE MAY APPLY TO NEW YORK STATE BUSINESSES

The California Consumer Privacy Act ("CCPA"), in effect since January 1, 2020, will be amended by a new law, the California Privacy Rights Act ("CPRA") as of January 1, 2023. The CCPA, as amended, applies to companies — as well as entities that control or are controlled by the business and share common branding — that do business in California (a complex question under California law), collect personal information of California residents, and meet one of three thresholds: (1) has annual gross revenues in excess of $25 million; (2) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more California residents, households or devices; or (3) derives 50% or more of its annual revenues from selling consumers' personal information.

Meanwhile, the Colorado, Connecticut, Virginia and Utah laws apply not only to persons or companies that conduct business in their respective state, but also to those that produce products or services directed to those states' residents provided that thresholds similar to CCPA are met. Businesses should be aware that the thresholds do not exactly mirror CCPA's thresholds.

For example, the Virginia law applies to businesses that conduct business in Virginia or produce products or services that are targeted to residents of Virginia and (1) control or process personal data of at least 100,000 consumers during a calendar year; or (2) control or process personal data of at least 25,000 Virginia residents and derive over 50% of gross revenue from the sale of personal data.

Service providers and organizations that work with covered entities under these laws may be subject to certain obligations as well. It is important for businesses to evaluate what laws apply based on their physical location, their business activity's geographic footprint, and information they store about residents of certain states. Doing so will help a business understand which privacy statutes — and which obligations — may apply.

DIFFERING BUSINESS OBLIGATIONS

Although they cover similar topics, these laws have significant differences. For instance, California, Colorado, Connecticut, Virginia and Utah all require businesses to disclose what data the business collects, how it processes such data, and the purposes for collecting and processing such data. Each law also prescribes certain specifications that businesses must disclose to consumers to allow them to exercise consumer rights, such as a data subject access request, or a request

ROCHESTER BUSINESS JOURNAL

that the business delete the data subject's personal information.

However, not every law imposes the same specifications. For example, Virginia, Colorado and Connecticut require subject businesses to not only create a process for how a consumer may appeal a denial of a data subject access request, but they also require subject businesses to conspicuously list how a consumer may submit their appeal. California and Utah, however, do not mandate that businesses establish and implement such a process.

Data impact risk assessments may also be required. Generally, a data risk assessment allows a business to identify and evaluate the risks associated with processing personal information. Virginia, Colorado and Connecticut require subject businesses to conduct data protection risk assessments, whereas Utah and California do not.

For example, Virginia's law requires subject businesses to conduct and document a data protection assessment regarding the business's processing of personal information for targeted advertising, the sale of consumers' personal data, the processing of personal data for profiling purposes, the processing of sensitive data (such as genetic or biometric information), and any other processing activities that would "present a heightened risk of harm to consumers." Va. Code Ann. § 59.1-580 (A)(5). The Colorado and Connecticut statutes impose substantially similar obligations on subject businesses requiring them to "identify and weigh the benefits that may flow . . . from the processing [of the data] . . . against the potential risks to the rights of the consumer associated with the processing." See Colo. Rev. Stat. § 6-1-1309 (3); see also 2022 Conn. Pub. Acts § 8 (b).

Other differences between these statutes may include: (1) required contractual provisions with service providers; (2) requiring a consumer (or their parent or legal guardian) to opt in to the processing of their data if they are younger than a certain age (generally 13 or 16 years of age depending on the state); (3) requirements on how to respond to consumer privacy requests; and (4) specifications on whether and how to provide consumers with an opportunity to opt out of the processing of their personal information.

ENFORCEMENT PENALTIES

Failure to comply with these laws can result in considerable fines and sanctions and, in California, private causes of action in limited scenarios. For example, noncompliance with the California law can result in a $2,500 fine per violation (or $7,500 per violation for intentional violations), while failing to comply with the Virginia law can result in a fine of $7,500 per violation. Generally, enforcement of these statutes is left to each state's respective attorney general, with the exception of California, which has established the California Privacy Protection Agency that will be charged with enforcement starting January 1, 2023.

Businesses should dedicate appropriate resources to developing and updating their data protection policies, practices and procedures. The consequences of failing to do so have begun to impact some businesses already.

Sephora, for example, recently agreed to pay a civil penalty of $1.2 million to the attorney general to resolve allegations that the company violated CCPA. As part of the settlement, Sephora must clarify its online privacy disclosures and revise its privacy policy. Pursuant to CCPA, the $1.2 million civil penalty will be deposited into the Consumer Privacy Fund, which was established to "offset any costs incurred by the state courts and the Attorney General in connection" with enforcing CCPA. See Cal. Civ. Code § 1798.160.

WHAT CAN BUSINESSES DO?

To prepare for these privacy statutes taking effect, businesses may want to consider:

- The applicability of these laws.
- The obligations these laws specifically impose.
- Determining a strategy for compliance, which may include updating data inventory, consumer data access requests response procedures, privacy and other policies, and vendor contracts.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at aclark@phillipslytle.com or (716) 847-8400 ext. 6466.

Michael R. Staszkiw, CIPP/US, is an attorney at Phillips Lytle LLP and member of the firm's Data Security & Privacy Practice Team. He can be reached at mstaszkiw@phillipslytle.com or (585) 238-2044.