An Update on Recent and Emerging Privacy Laws: When the Client's Reach Is Nationwid

It is critical for attorneys advising businesses that reach consumers both inside and outside of New Jersey to be aware of these new requirements to provide appropriate advice to their clients.

November 18, 2022 at 10:00 AM

Privacy

By Nancy Del Pizzo and Deborah Isaacson | November 18, 2022 at 10:00 AM

The increasing threat of cyber-attacks and data breaches is spotlighting the need for practitioners to keep up to date on the changing landscape of privacy law. Doing so, however, is challenging. Unfortunately, there is no comprehensive consumer privacy law at the federal level yet, leaving it to individual states to enact laws to protect the privacy rights of their residents. More states are beginning to do so, and new state privacy litigation is coming into effect next year, which will impose new requirements on businesses and offer expanded rights for consumers. It is therefore critical for attorneys advising businesses that reach consumers both inside and outside of New Jersey to be aware of these new requirements to provide appropriate advice to their clients.

Currently, California has what is considered comprehensive consumer privacy legislation to protect its resident consumers. That legislation governs what businesses that meet certain requirements can and cannot do with customers' personal identifiable information (PII).[1] PII is any type of data or information that can be used to identify someone, such as their name, social security number, email address or phone number. See U.S. Department of Labor Guidance on the Protection of Personal Identifiable Information. Virginia, Colorado, Utah, and most recently, Connecticut, have followed California's lead by enacting their own comprehensive privacy legislation, and their laws become effective next year. New Jersey has yet to enact its own comprehensive privacy law, but the New Jersey State General Assembly in January of this year introduced the Disclosure and Accountability Transparency Act, which is working its way through the legislative process.

This article will discuss and compare the comprehensive privacy acts that have been signed into law in this country in five states, as well as the provisions in New Jersey's proposed privacy law. The comparison will provide guidance as to how New Jersey's proposed privacy law might look, given that the five states often borrowed from their predecessors in crafting their laws. It also will be helpful for attorneys who offer guidance to clients that do business throughout the United States for, by way of example, ensuring website terms of use and privacy policies comply where required.

California Leads the Way

The California Consumer Privacy Act of 2018 (CCPA) is the first of its kind in the country to secure new privacy rights for its state's consumers. See Cal. Civ. Code §1798.100 et seq. The CCPA provides California consumers with the right to know about the personal information a business collects about them and how it is used and shared; the right, with some exceptions, to delete personal information collected from them; the right to opt out of the sale of their personal information and the right to non-discrimination for exercising their rights under the CCPA. The CCPA applies to for-profit businesses doing business in California that 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.

In November 2020, the California Privacy Rights Act (CPRA) was passed via ballot initiative. See CA Prop. 24, 2020 Cal. Legis. Serv. Prop. 24 (PROPOSITION 24) The CPRA amended and expanded the CCPA, clarifying existing provisions of the CCPA and providing additional privacy protections for consumers. The majority of the CPRA's provisions will go into effect on Jan. 1, 2023, with a look-back to January 2022.

Virginia Follows Suit

On March 2, 2021, Virginia became the second state to enact a comprehensive data privacy law through the Virginia Consumer Data Protection Act (VCPDA). See Va. Code Ann. §59.1-571 et seq. Like the CCPA, the VCDPA, which does not come into effect until Jan. 1, 2023, applies to companies that do business in Virginia, even if they are not headquartered or incorporated there. If a business conducts business in Virginia or markets its goods and services to Virginia residents and either (1) controls or processes the personal data of at least 100,000 Virginia residents; or (2) controls or processes the personal data of at least 25,000 Virginia residents and derives more than 50% of its gross revenue from the sale of personal data, it is subject to the VCDPA. Unlike the CCPA, there is no business revenue threshold imposing obligations under the law. The number of residents' data that must be collected or processed before the VCDPA applies to a business is double that of the CCPA.

The VCDPA provides consumers with the right to know, access and confirm personal data; the right to request that their personal data be deleted by businesses; the right to correct inaccuracies in personal data; the right to obtain a copy of their personal data; 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; and the right to not be discriminated against for exercising any of the foregoing rights. A consumer is defined as a Virginia resident acting only in an individual or household context, omitting a person acting in a commercial or employment context from its definition. This differs from the CPRA, which includes employee data.

In addition, the VCDPA requires that companies only hold onto the pieces of data they need for a specific purpose and for only as long as is necessary to achieve that purpose. Companies are also required to implement and maintain reasonable data security practices to protect the confidentiality, integrity and accessibility of personal data.

Colorado Enacts Its Own Comprehensive Privacy Legislation

On July 8, 2021, Colorado became the third state to provide its residents with protection for their personal data. The Colorado Privacy Act (CPA) provides Colorado's Attorney General with the authority to adopt rules governing privacy and requires that by July 1, 2023, the Attorney General specifically adopt rules that detail the specifications for one or more universal mechanisms that communicate a consumer's affirmative, unambiguous and freely given choice to opt out of the processing of personal data for the purposes of its sale or targeted advertising. See Colo. Rev. Stat. §6-1-1301 et seq.

On Oct. 10, 2022, the Colorado Secretary of State published the CPA's draft rules for public comment. The CPA applies to legal entities conducting business or producing commercial products or services intentionally targeted to Colorado residents that either: (1) control or process personal data of at least 100,000 consumers per calendar year; or (2) derive revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers. The CPA does not apply to certain specified entities, including state and local governments and state institutions of higher education; and personal data governed by listed state and federal laws, listed activities and employment records. Similar to the VCPDA, the CPA does not include any revenue thresholds to subject a business to the law.

Under the CPA, consumers, which is defined as Colorado residents acting in an individual or household context, have the right to opt out of a controller's processing of their personal data; access, correct, or delete the data; or obtain a portable copy of the data from a controller. A controller is defined under the CPA as a person who determines the purposes and means of processing personal data. The CPA also specifies how controllers must fulfill duties regarding consumers' assertions of their rights, transparency, and avoiding unlawful discrimination and requires controllers to conduct a data protection assessment for each of their processing activities involving personal data that present a heightened risk of harm to consumers, such as processing for selling personal data, profiling, processing of sensitive data or for targeting advertising. See https://leg.colorado.gov/bills/sb21-190.

Utah Joins California, Virginia and Colorado

On March 24, 2022, the Utah Consumer Privacy Act (UCPA) was signed into law, and it goes into effect Dec. 31, 2023. See Utah Code Ann. §13-61-101 et seq. The UCPA draws heavily from the VCDPA, but its substance takes a more business-friendly approach to consumer privacy. Like the VCDPA, the UCPA applies to any controller or processor who conducts business in Utah or produces a product or service targeted to consumers who are Utah residents; has annual revenue of $25 million or more; and satisfies one or more of the following thresholds: (1) controls or processes personal data of 100,000 or more consumers during a calendar year; or (2) derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

Under the UCPA, a consumer is defined as an individual who is a Utah resident acting in an individual or household context. Consumers are provided with four main rights: (1) the right to confirm whether a controller is processing their personal data and to access their personal data; (2) the right to delete the personal data that they provided to the controller; (3) the right to obtain a copy of

the personal data that they previously provided to the controller; and (4) the right to opt out of the processing of their personal data for the purposes of targeted advertising or the sale of personal data.

Connecticut Makes Five

Connecticut became the fifth state to enact comprehensive privacy legislation when the Connecticut Data Privacy Act (CTDPA) was signed into law on May 10, 2022. See Substitute Senate Bill No. 6 Public Act No. 22-15 An Act Concerning Personal Data Privacy and Online Monitoring. The law, which will go into effect July 1, 2023, applies to entities that conduct business in Connecticut or produce products or services targeted to Connecticut residents and that during the preceding calendar year either (1) controlled or processed the personal data of at least 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing payment transactions; or (2) derived over 25% of their gross revenue from the sale of personal data and controlled or processed the personal data of 25,000 or more consumers. The CTDPA, unlike the CCPA, does not have an annual revenue threshold to trigger obligations to businesses under the law.

The CTDPA grants consumers the rights to: (1) confirm whether a controller is processing their personal data and access such personal data, unless such actions would reveal a trade secret; (2) correct inaccuracies in their personal data; (3) delete personal data provided by or about them; (4) obtain a portable copy of their personal data to the extent technically; and (5) opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data or profiling in connection with automated decisions that produce legal or similarly significant effects concerning them. A consumer is defined as a Connecticut resident and explicitly excludes individuals acting in a commercial or employment context, just like Virginia, Colorado and Utah's laws.

Will New Jersey Be Next?

The assembly bill for the New Jersey Disclosure and Accountability Transparency Act (NJ DaTA) was introduced in the New Jersey State General Assembly on Jan. 11, 2022. See New Jersey Legislature Bill A505. The bill would establish requirements for the processing and disclosure of personally identifiable information and establish the Office of Data Protection and Responsible Use in the New Jersey Division of Consumer Affairs. Like the laws in California, Virginia, Colorado, Utah and Connecticut, the bill would provide the rights of access, correction, deletion and data portability for residents of New Jersey. The bill would also require a consumer's affirmative consent to the controller's processing of personal information for a specific purpose; require the controller to provide concise and transparent information to consumers regarding the processing of personal information; establish rules concerning the securing of a consumer's personal data; and set forth procedures to be followed in the event of a data breach.

The NJ DaTA has been referred to the Assembly Science, Innovation and Technology Committee.

It is incumbent on New Jersey practitioners who provide legal counsel to companies on privacy issues (such as lawyers who prepare website or mobile application terms of use and privacy policies for companies who have nationwide clients) to be aware of the ever-changing privacy landscape. That is, until or unless federal legislation enters the fray.

Endnote:

[1]The importance of protecting PII from security threats is not only for the obvious reasons of preventing identity theft, but also for the fines that could be imposed upon business violating these new privacy laws. For example, violations of the California Consumer Privacy Act are subject to enforcement by California's Attorney General's office. If, after receiving notice, a business fails to cure its violation(s) within 30 days, civil penalties of $2,500 for each violation or $7,500 for each intentional violation can be imposed on the business. As businesses collect personal information from large numbers of consumers on a regular basis, the fines could be significant, particularly so if the violations are intentional. The law also creates a private right of action for consumers that are affected by a data breach resulting in unauthorized access, theft, or disclosure of the individual's PPI if the breach is attributable to a business' failure to put reasonable security practices and procedures in place.

Nancy Del Pizzo *is a partner at Rivkin Radler in its Hackensack, N.J., office. Her practice focuses on intellectual property; commercial litigation; and privacy, data and cyber law. She is co-chair of the Internet and Privacy Subcommittee of the American Bar Association's IP Section of Litigation.* Deborah Isaacson *is counsel in the firm's New York City office. Her practice focuses on professional liability; employment; and privacy, data and cyber law.*