PUBLICATION

Navigating U.S. State Privacy Laws: New Jersey Adds New Roads to an Already Complicated Map

January 23, 2024

On January 16, 2024, New Jersey Governor Phil Murphy signed into law the first comprehensive state privacy law of 2024 (SB 332). As states wait for federal privacy legislation to materialize, New Jersey's legislation becomes the 13th comprehensive state privacy law in the U.S. (in addition to certain other sector- or data-specific legislation at the state level). Given the law's applicability thresholds, organizations can expect to fall subject to the New Jersey law more easily than other state privacy laws. The law will take effect January 15, 2025, just one year from the Governor's signature on the bill.

Until now, state privacy legislation outside of the California Consumer Privacy Act (CCPA) has largely followed the model presented in the Virginia Consumer Data Protection Act (the Virginia model). Each state has included its own variations in obligations and scope – causing businesses and industry bodies alike to continually reevaluate their current practices and best practices for, in many instances, unresolved requirements. Although it includes many of the same requirements concerning privacy notices, consumer rights, and data protection assessments as other state laws following the Virginia model, the New Jersey law contains notable differences in several areas that may present challenges to organizations as they continue to adapt their privacy compliance strategies at the state level.

Applicability

The New Jersey law applies to "controllers" that annually control or process the personal data of at least 100,000 New Jersey residents. The New Jersey law likewise applies to controllers that control or process the personal data of at least 25,000 consumers and derive revenue or receive a discount on the price of any goods or services from the sale of personal data. Most other states, besides Colorado, require a percentage of gross revenue to be derived from personal data sales before this threshold applies. New Jersey also does not have a blanket revenue threshold, making it one of the easiest thresholds to cross for organizations doing business in states that have enacted comprehensive privacy legislation.

Exemptions

States following the Virginia model have largely consistent exemptions for certain types of data (e.g. information collected in the employment or B2B context, protected health information (PHI), and de-identified personal data) and certain types of organizations (e.g. non-profits, HIPAA covered entities, and financial institutions who comply with the Gramm-Leach-Bliley Act (GLBA)). The New Jersey law, however, contains narrower exemptions in both categories. For example, while the New Jersey bill exempts GLBA financial institutions, it does not contain exemptions for non-profits or institutions of higher education, nor does it exempt HIPAA covered entities, though it does contain an exemption for PHI. Such covered entities may be required to comply with the New Jersey law at an organizational level even if the PHI they control is excluded from the scope.

Sensitive Data

Like other states following the Virginia model, the New Jersey law requires consent to collect and process "sensitive data." The New Jersey law, however, includes a more extensive definition of "sensitive data" similar to that used in California, including, among other types of data, "financial information, which shall include a consumer's account number, account log-in, financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial

account." The CCPA contains a similar clause in its definition of sensitive personal information; however, the CCPA does not require consent to collect sensitive personal information. Although the New Jersey law excludes data controlled or processed solely for the purpose of completing a payment transaction from the count of New Jersey consumers for the purposes of determining the applicability of the law, this type of data is not generally excluded from the scope of the law once a business crosses that applicability threshold.

Rulemaking

The New Jersey law requires rulemaking by the New Jersey Attorney General's Division of Consumer Affairs in the Department of Law and Public Safety. The law does not include a timeline for this rulemaking, leaving open questions as to the timing and scope of compliance measures to be taken by subject organizations. It is expected that rulemaking measures will also address current questions about the ability to standardize technically universal opt-out mechanisms required by New Jersey with those required under other state laws.

During 2023, seven states passed comprehensive state privacy legislation, among other states that passed consumer health privacy legislation and children's online privacy legislation – making for the most varied and rapidly evolving year to date for privacy legislation. It remains to be seen how many more state lines will be added to the privacy map before legislative action is taken at the federal level. Several of these new laws come into effect in 2024, with more in the years to follow. Organizations should begin or continue building on existing compliance efforts to closely track the evolving and distinct requirements across the U.S. privacy landscape.

For more information or assistance with your privacy efforts, please contact Greta Messer, CIPP/US, or another member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.