Articles + Publications | January 24, 2024

The Garden State Joins the Privacy Party

WRITTEN BY

James Koenig | Ronald Raether, Jr. | Kim Phan | Stephen C. Piepgrass | Samuel E. "Gene" Fishel | Robyn W. Lin

On January 16, New Jersey Governor Phil Murphy signed S332 (the act), making New Jersey the first state in 2024 to enact a comprehensive privacy law. Several other states are currently considering similar comprehensive privacy legislation, including New York, Pennsylvania, North Carolina, and Ohio. The New Jersey bill is undoubtedly the opening salvo of further state privacy action to come in 2024.

Applicability

S332 will apply to controllers and processors who conduct business in New Jersey or produce products or services that are targeted to residents of New Jersey, and who (1) "control or process the personal data of at least 100,000 consumers, excluding personal data processed solely for the purpose of completing a payment transaction"; or (2) "control or process the personal data of at least 25,000 consumers and the controller derives revenue or receives a discount on the price of any goods or services, from the sale of personal data."

Exemptions: Like other comprehensive privacy laws, there are exemptions for financial institutions, nonprofits, and state agencies. There are also data level exemptions for protected health information; financial data; personal data collected, processed, sold, or disclosed by a consumer reporting agency; and personal data for persons acting in a commercial or employment context.

Consumer Rights

Like many of the other state comprehensive privacy laws, consumers will have the right to:

1. Confirm whether a controller processes the consumer's personal data;

2. Correct inaccuracies to their personal data;

3. Delete their personal data;

4. Obtain a copy of their personal data; and

5. Opt out of the processing of their personal data for (a) targeted advertising; (b) sale; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects.

Consumers may exercise their rights or authorize an agent to exercise their rights on their behalf. Like California and Colorado, New Jersey will require controllers to allow consumers to exercise their right to opt out of processing through a user-selected universal opt-out mechanism.

Controller Obligations

Under S332, controllers have various obligations, including limiting the collection of personal data to what is adequate, relevant, and reasonably necessary; establishing, implementing, and maintaining administrative, technical, and physical data security practices; and providing a privacy notice.

Data Protection Assessment Requirement

S332 also requires that controllers "not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data … that present a heightened risk of harm to a consumer." This data protection assessment must be made available to the Division of Consumer Affairs in the New Jersey Department of Law and Public Safety upon request. Heightened risk of harm is defined as:

1. Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of: unfair or deceptive treatment of, or unlawful disparate impact on, consumers; financial or physical injury to consumers; a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or other substantial injury to consumers;

2. Selling personal data; and

3. Processing sensitive data.

Enforcement

The act grants the New Jersey Attorney General's (AG) Office "sole and exclusive authority" to enforce violations and expressly forecloses private rights of action. The office has aggressively enforced privacy and data security laws in recent years, particularly pursuant to New Jersey's data breach notification law and consumer protection act. Under this new law, the office is armed with more robust tools, and thus organizations should anticipate even greater privacy enforcement activity out of New Jersey.

AGs typically seek both injunctive relief and monetary penalties in privacy enforcement actions. Yet unlike most other recently enacted state comprehensive privacy laws, the New Jersey statute does not prescribe a monetary penalty within its text. Rather, it states that a violation of the act shall be treated as an "unlawful practice" under the New Jersey Consumer Fraud Act (CFA). Consequently, this means an offending business will be liable under CFA's monetary penalty provisions, in addition to injunctive measures. An "unlawful practice" in violation of the CFA garners a maximum $10,000 penalty for a first offense and a maximum $20,000 penalty for subsequent offenses. For comparison, the state comprehensive privacy laws of California, Texas, and Virginia contain a

$7,500 penalty cap for each violation, while Connecticut has a $5,000 cap per violation. Colorado has a $2,000 cap per affected consumer with a $500,000 maximum penalty per violation.

Like the California Consumer Privacy Act, the New Jersey statute grants rulemaking authority to a specified state agency, in this case the Division of Consumer Affairs within the New Jersey Department of Law and Public Safety. The 13 state comprehensive privacy laws enacted thus far vary widely on granting such authority. For example, while the California Privacy Protection Agency and the Colorado Secretary of State were empowered with rulemaking authority under their respective statutes, the Virginia, Iowa, and Utah laws grant no additional rulemaking authority. And some state statutes grant only limited authority to certain state agencies. The Colorado statute, for example, grants limited authority to the Colorado AG's Office to approve a list of universal opt-out mechanisms for consumers that companies can employ to satisfy opt-out requirements in the statute, which they did just last month. Applicable businesses must now be cognizant of future promulgations from New Jersey that shift parameters or create new mandates under the law. The rulemaking authority conferred by the act is permissive, rather than mandatory, and does not establish a deadline for the issuance of any new regulations.

The New Jersey statute takes effect on January 16, 2025. However, the statute allows for an 18-month grace period after it takes effect, during which the Division of Consumer Affairs must give an offending organization a 30-day cure period prior to the AG's office bringing an enforcement action. This right to cure will sunset after this grace period.

Our Take

While many of the rights and obligations are similar to other state laws, S332 highlights two trends in privacy laws: (1) requiring businesses to respond to universal opt-out mechanisms and (2) requiring businesses to conduct data impact assessments. Businesses looking to stay ahead and on top of the patchwork of state comprehensive privacy laws should also:

1. **Review and Update Privacy Policy.** Evaluate your current privacy policy and make necessary adjustments to ensure compliance with S332, and consider updating your policy if you have not done so already, with an integrated approach with other requirements and obligations under other state and global laws.

2. **Update Template and Conduct Comprehensive Data Protection Impact Assessments.** Incorporate New Jersey requirements into your data protection impact assessment template (DPIA) and conduct assessments on an integrated approach in compliance with other state and global laws.

3. **Inventory Adtech Usage and Honor Global Privacy Controls.** Carry out an audit of all cookies and other adtech tracking technologies currently used on your digital platforms. Also, consider implementation of universal opt-out mechanisms, such as the Global Privacy Controls, for compliance under the New Jersey law, as well as California and Colorado.

4. **Update Data Maps.** Revamping your data mapping activities, including understanding the types of data collected, how this data is used, and where it is being disclosed will assist with determining the scope and applicability of S332. This activity can be integrated into your compliance efforts related to other U.S. state comprehensive privacy laws or for your records of processing activities (ROPA) under EU and other laws.

5. **Make a Plan**. Be on the lookout for the yet-to-be promulgated and soon-to-be effective regulations and plan accordingly to meet the obligations that will arise under them. Consider taking an integrated approach to comply with S332 (and the other laws) prior to its effective date in 2025.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- Regulatory Investigations, Strategy + Enforcement