Comprehensive State Privacy Laws: Compliance Considerations for New York Businesses

By Anna Mercado Clark and Lavanya Sathyamurthy

Phillips Lytle LLP

State Privacy Laws Continue to Evolve with Varying Requirements Across Jurisdictions

New York State businesses may be subject to a growing number of comprehensive state privacy laws, many of which have recently taken effect. There are key distinctions and common obligations among these laws, in addition to recent enforcement actions and strategies for compliance that businesses should apply to their operations.

Anna Mercado Clark
Partner

Lavanya Sathyamurthy
Attorney

Comprehensive State Privacy Laws from Various States May Apply to New York Businesses

Applicability is typically a multi-step inquiry that involves an analysis of one or more certain threshold criteria, such as minimum annual revenue and the number of state residents whose personal data a business controls or processes. These factors are neither uniform across states nor exhaustive.

State Privacy Laws May Impose Similar, but Not Identical, Obligations on Businesses

Businesses subject to comprehensive state privacy laws may have to comply with similar obligations, but the specific requirements may vary by state. These obligations may include, but are not limited to:

- Recognition of consumer (state residents') rights (e.g., CA, CO, VA): Consumers may request confirmation as to whether a business is processing their personal data and request access to such data, subject to certain limitations (e.g., verification requirements, trade secret protection, etc.). However, these requirements may differ by state, including applicable exemptions.
- Opt-in (e.g., CT, OR) / Opt-out (e.g., UT, IA): Sensitive personal data, such as precise geolocation, racial or ethnic origin, religious beliefs and health information, may only be processed with the consumer's consent, with some states requiring an opt-in and others allowing an opt-out for certain uses.
- Privacy policies (e.g., CO, CT, MN): Businesses may have to provide notice to consumers on how they collect, use and share personal data.

Potential Penalties for Failure to Comply

Failure to comply with comprehensive state privacy laws may result in reputational damage, enforcement actions by regulators or state Attorneys General, lawsuits and/or fines.

For instance, on October 30, 2025, the California Attorney General secured a $530,000 settlement with Sling TV for alleged violations of the California Consumer Privacy Act (CCPA) related to inadequate opt-out mechanisms. Sling TV directed users to cookie-preference tools that did not effectuate a full opt-out and required unnecessary multi-step webform submissions for logged-in users.

On January 13, 2025, the Texas Attorney General filed its first enforcement action against Allstate and its subsidiary, Arity, for, among other things, violation of the Texas Data Privacy and Security Act (TDPSA) for allegedly paying third-party developers to embed software that enabled the collection (and eventual sale) of geolocation data through mobile applications (such as Life360) from consumers without proper notice or consent.

Across the country, states have brought enforcement actions based on businesses' inadequate privacy notices, burdensome mechanisms for exercising consumer rights and unlawful collection of minors' data.

Businesses should regularly review their data privacy compliance procedures. Given the complexity and variability of state privacy laws, legal counsel can assist in assessing applicability and developing compliance strategies.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, Partner and Chief Information Security Officer at Phillips Lytle, is also Co-Leader of the firm's Technology Industry Team. She can be reached at aclark@phillipslytle.com or (716) 847-8400 ext. 6466.

Lavanya Sathyamurthy, attorney and member of Phillips Lytle's Corporate and Business Law Practice, can be reached at lsathyamurthy@phillipslytle.com or (212) 508-0494.