PUBLICATION

The New York Privacy Act: A Consumer Privacy Bill to Monitor Closely

Authors: Aldo M. Leiva
July 22, 2019

In the wake of enactment of California's Consumer Privacy Act (CCPA) in 2018, the New York State legislature is now considering its own (and more expansive) consumer privacy law (SB5642), entitled the "New York Privacy Act" (NYPA). The NYPA was introduced in May 2019 by New York State Senator Kevin Thomas, chair of the New York Senate's Committee on Consumer Protection, for consideration by the legislature, in anticipation of the end of the legislative session on June 19, 2019.

If passed and signed into law by New York Governor Andrew Cuomo, the NYPA would apply to legal entities that conduct business in the State of New York, or produce products or services targeted to residents of New York State. The law would, therefore, potentially impact businesses based outside New York State if their marketing efforts are directed at New York residents. Unlike the CCPA, however, which applies only to businesses that generate more than $25 million in annual gross revenue, the NYPA applies to businesses of any size. The current draft of the bill includes several important exemptions. It does not apply to state and local governments, nor does it apply to personal data regulated by the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Gramm-Leach Bliley Act (GLBA), and to data sets maintained for employment records purposes.

The NYPA also broadly defines "personal data" to include not only specific identifiers (such as names, addresses, and social security numbers), but includes financial information, medical information, biometric data, online activity information, geolocation data, or any other information from which inferences could be used to create profiles about an individual's preferences or behavior. Any such information may only be used, processed, or transferred by a business with a consumer's consent, which must be supported by a written statement "or other clear affirmative action" by the consumer.

The bill also imposes the role of "data fiduciary" on any covered business, which is required to exercise the duty of care, loyalty, and confidentiality expected of a fiduciary with regard to securing the personal data against a privacy risk. The term "privacy risk" has a broad definition and includes such adverse consequences as direct or indirect financial loss or economic harm, physical harm, psychological harm (including anxiety, embarrassment, fear and other demonstrable mental trauma), significant inconvenience or expenditure of time, reputational harm, intrusion from unwanted commercial communications, price discrimination, or other effects reasonably foreseeable to the covered legal entity (even if not foreseeable to the consumer), such as alteration of the consumer's experiences, limitation of choices, influence over responses, predetermined outcomes, or other effects on an individual's private life (including family matters, communications within a home, or any similar physical, online, or digital location where an individual has a reasonable expectation of privacy).

In protecting the consumer against any such risk, a covered business would be required to act in the best interests of the consumer, in a manner expected by a reasonable consumer under the circumstances. Notably, this fiduciary duty would expressly supersede any duty owed to owners or shareholders of a covered legal entity. In performing its fiduciary duty to the consumer, a covered business would be required to reasonably secure personal data from unauthorized access and promptly notify any consumer of any breach of the above-described data fiduciary duty, though no specific time period for such notification is provided.

To the extent that the covered business discloses, sells, or shares any personal data with a third party (such as a vendor or third-party data processor), any such third party must enter into a written contract with the covered business that imposes the same duties of care, loyalty, and confidentiality toward the consumer as required of the covered business. In selecting or contracting with any such vendor or third party, the covered business is also required to conduct due diligence of any third-party recipient of personal data, including auditing, on a regular basis, the data security practices of any such recipient.

The NYPA provides consumers with enforceable rights that must be observed and protected by covered businesses. Covered businesses must provide a clear privacy notice to consumers of such rights, and provide an opportunity for consumers to opt in or out of processing of personal data in such a manner that each consumer must select and clearly indicate their consent or denial of consent. Consumer rights include the right to request confirmation as to whether any of the consumer's personal data is being processed, or whether it is being sold to data brokers, as well as the names of any third parties with whom such information is being shared. Such information would need to be provided to the consumer free of charge, up to twice annually, and a reasonable fee may be charged for additional requests within the year.

Consumers would have a right to request correction of inaccurate personal data, place restrictions on processing of personal data, and may also request deletion of personal data in certain circumstances. Any correction, deletion, or restrictions on data processing must be communicated to third-party processors or recipients of such data. Covered businesses must respond to any such consumer request without undue delay, but at minimum within 30 days of receipt of the request, provided that this period may be extended to 60 days upon written notification to the consumer, with reasons for the delay provided to the consumer (such as complexity of the request, or the number of requests). If no action is to be taken in response to the request, the consumer would need to be notified and advised of any possibility of further internal review of the decision not to act on the request.

Violations of the NYPA would be enforced by the New York Attorney General, or, alternatively, by any person who has been injured by any violation of the Act, with reasonable attorney's fees awardable to a prevailing plaintiff. Notably, this fee provision awards fees to a consumer if they were successful in their suit, but a prevailing business would not be entitled to any such fees were it to prevail in its defense of the lawsuit. Where more than one entity is involved in the processing of the personal data, liability will be allocated among the parties based on comparative fault, unless liability is otherwise allocated by contract among the parties.

Violators of the NYPA would be subject to injunctions and civil penalties to be calculated by the courts by considering the number of affected individuals, severity of the violation, and the size and revenues of the covered legal entity. For purposes of such calculation, each individual whose information was unlawfully processed counts as a separate violation, and each provision that was violated counts as a separate violation.

Given the above provisions, which exceed several of the privacy protections afforded by the CCPA, and, if passed, would make the NYPA the most expansive and consumer-oriented privacy law in the country (to date), any company doing business in New York or advertising to New York residents should closely monitor this bill as it is deliberated in the New York State legislature. If passed and signed into law, businesses should consider (1) consulting with legal counsel as to whether their company is a "covered entity" under the NYPA, and therefore subject to its requirements, (2) assess exclusion of data sets under HIPAA/HITECH, GLBA, or as an employment record, (3) review existing data privacy and data security policies and procedures, (4) analyze third-party contracts with data processors or other recipients of personal data, and (5) review insurance coverage status or options.

If you have any questions regarding these issues or any other data privacy or security-breach related issues, please contact the authors of this article or any of the attorneys in Baker Donelson's Data Protection, Privacy and Cybersecurity Group.