Now & Next
Cybersecurity & Privacy Alert

May 15, 2024

State Senate Committee introduces the New York Privacy Act

By Timothy D. Sini, Jenny L. Holmes, and Jared Kaiman[1]

The Act aims to balance consumers' privacy expectations with commercial activity in New York State.

What's the impact?

- The Act applies to legal persons and entities that conduct business in New York or produce products or services targeted to residents of New York.
- Consumer data and sensitive personal data require different levels of protection under the Act.
- Businesses must provide clear mechanisms for consumers to opt-out of certain data use activities.

We've watched state after state follow in California's footsteps and pass comprehensive privacy laws, but New York has remained noticeably quiet. Instead, New York's legal data privacy

[1] Jared Kaiman (Legal Intern–Government Investigations and White Collar Defense Group) assisted with the preparation of this alert.

landscape is unclear and often lacks transparency, making it difficult for both New York businesses and individuals to navigate.

New Yorkers cannot evaluate the risks of sharing their personal data with businesses and compare privacy-related protections across services and at the same time, New York businesses are faced with increasing consumer demands for transparency. With a substantial increase in the amount and categories of personal data being generated, collected, stored, analyzed, and potentially shared, it is increasingly clear that New York's legal landscape needs to evolve to address the uncertainties.

What is the New York Privacy Act?

Senate Bill S365B, also known as The New York Privacy Act (the Act), is currently in Senate Committee and aims to create a level playing field between New Yorkers who provide data through interactions with businesses (consumers) and businesses. The Act applies to legal persons that conduct business in New York or produce products or services targeted to residents of New York and that meet one of the following three thresholds:

- Have annual gross revenue of $25 million dollars or more,
- Controls or processes personal data of 50,000 consumers or more, or
- Derives over 50% of gross revenue from the sale of personal data.

If the thresholds look familiar, they largely track other state laws except for the number of consumers; California, for example, has a threshold of 100,000 consumers or more.

CONSUMER DATA

The Act categorizes businesses that handle consumers' data into three distinct groups: controllers, processors, and third-parties, each of which has its own distinct obligations under the Act. As defined in the Act:

- a ***controller*** is a person or legal entity who determines the purpose and means of processing personal data;
- a ***processor*** is a person or legal entity that processes data on behalf of the controller; and
- a ***third party***, with respect to a particular interaction or occurrence, is a person, public authority, agency, or body other than the consumer, controller or processor, unless they also meet the criteria for a controller.

The Act primarily focuses on controllers, which is the business that consumers are usually in direct contact with.

SENSITIVE DATA

The Act also follows other states' laws in its definitions of personal data. Like California, the Act creates a category of "sensitive data," that requires higher protections, such as health condition or diagnosis; racial or ethnic origin; precise geolocation; or social security, financial account, passport, or driver's license number.

DATA TRANSPARENCY OBLIGATIONS

Since the Act aims to create transparency between consumers and controllers, the obligations of the businesses are both structural and procedural in nature. Like other state privacy laws, the Act seeks to provide New York consumers with rights as it pertains to their personal data. These rights include, but are not limited to, the right to notice, the right to opt-out, the right to access, the right to portable data, the right to correct, and the right to delete. Further, a controller must obtain freely given, specific, informed, and unambiguous opt-in consent from a consumer to process their sensitive data or make changes to the existing processing or processing purpose and provide consumers with clear disclosures that are separate and apart from any contract or privacy policy.

OPT-OUT MECHANISMS

The Act requires that controllers allow consumers to opt out, at any time, of processing personal data for purposes of: (i) targeted advertising; (ii) the sale of personal data; and (iii) profiling in furtherance of decisions with legal or similarly significant effects concerning a consumer. Like the CCPA's concept of "sharing" data, targeted advertising is advertising based upon profiling of a consumer's behavior. The Act's definition of "sale" also tracks the CCPA's broad definition, including both monetary and other valuable consideration. However, the Act adds a new concept —profiling. The Act defines "profiling" to mean any form of automated processing on personal data to evaluate, analyze, or predict personal aspects related to an individual's economic situation, health, personal preference, interests, reliability, behavior, location, or movements. Profiling does not include evaluation, analysis, or predictions based solely upon a person's current search queries or activities on a controller's website or online application. While the Act does not preclude a business from engaging in targeted advertising, selling data, or profiling, it must provide clear mechanisms for consumers to opt-out and cannot ask consumers to opt back in.

ADDITIONAL OBLIGATIONS FOR BUSINESSES

Some other responsibilities of businesses include, but are not limited to, maintaining reasonable data security for personal data; notifying consumers of foreseeable harms arising from the use of their data and obtaining specific consent for that use; and conducting regular assessments to ensure that the data is not being used for unacceptable purposes.

The future of the New York Privacy Act

While many would welcome the Act, is it too late? Two US legislators recently unveiled a bipartisan plan to enact the first comprehensive federal data privacy law, the American Privacy Rights Act (APRA). However, APRA would preempt state law in most instances. So while we wait to see what the New York Senate Committee does with the Act, it could quickly become moot.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Timothy D. Sini
516.832.7655
tsini@nixonpeabody.com

Jenny L. Holmes
585.263.1494
jholmes@nixonpeabody.com