ROPES & GRAY

ALERT ▪ Data Practice

August 26, 2019

New York Updates Privacy Laws

New York has recently enacted two laws expanding its breach notification and security safeguards requirements, and it may be poised to pass a third bill, aimed at increasing the privacy rights of New York residents. On July 25, 2019, New York Governor Andrew M. Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act (“SHIELD”) and Identity Theft Protection and Mitigation Services Act. Together, these bills expand the type of personal information covered by New York’s data breach reporting law, require business to implement specific data security safeguards, and demand that any business regulated as a credit reporting agency (“CRA”) provide identity theft prevention and mitigation services to affected consumers for five years – a new high water mark for such requirements.

These bills may be only the start of New York’s efforts to strengthen the protections over state residents’ personal data. New York is also considering a new privacy law that, if enacted, would be more stringent than California’s Consumer Protection Act (“CCPA”) and introduce the concept of a “data fiduciary” to the U.S. privacy lexicon.

As more states follow California’s lead and debate new privacy laws aimed at protecting residents’ personal data, companies should consider how these new laws, if enacted, might affect their business practices and the value of the personal data they collect. Below we discuss some of the key features of New York’s recently enacted and pending legislation and the potential implications on companies.

Recently Enacted: SHIELD Act

New York’s original data breach notification law required any person or business conducting business in New York to notify state residents when their “private information” was acquired without valid authorization. *See* N.Y. Gen. Bus. L. § 899-aa(2). The SHIELD Act, which takes effect on March 21, 2020, broadens the scope of New York’s data breach notification law in several ways. The notification requirements now apply to any person and business that handles New York residents’ information *regardless of whether that person or business conducts business in New York*.

Perhaps most significantly, the SHIELD Act requires any person or business handling New York residents’ private information to implement and maintain “reasonable” administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of private information. Several states have similar laws that require reasonable controls, but the New York SHIELD Act now mandates that a covered company:

- designate one or more employees to coordinate the security program;
- identify reasonably foreseeable internal and external risks;
- assess the sufficiency of safeguards in place to control the identified risks;
- train and manage employees in the security program practices and procedures;
- select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract;
- adjust the security program in light of business changes or new circumstances;
- assess risks in network and software design;
- assess risks in information processing, transmission and storage;
- detect, prevent and respond to attacks or system failures;
- regularly test and monitor the effectiveness of key controls, systems and procedures;
- assess risks of information storage and disposal;

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.

- detect, prevent and respond to intrusions;
- protect against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- dispose of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

Failure to establish reasonable safeguards would mean potential action against the company by New York regulators.

In addition, the SHIELD Act broadens the scope of incidents that require notification in the following ways:

- Expanded definition of "private information"
  The SHIELD Act expands "private information" in line with the laws of several other states to include (i) biometric information, (ii) financial account numbers that can be used alone to access an account, and (iii) usernames or email address in combination with a password or security question and answer.

- Notification for incidents involving unauthorized access
  Under the original law, notification was required only if there was "unauthorized acquisition" of private information. The SHIELD Act requires notification even where there was "unauthorized access" but no acquisition of private information, such as where there are "indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person."

As do the laws of most other states, the SHIELD Act provides for exceptions to its notification and reasonable security requirements, including for those businesses already regulated by and in adherence with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). Companies covered by HIPAA or GLBA, however, are still required to provide notice to the New York Attorney General, Department of State, and the Division of State Police in the event of a data breach.

Recently Enacted: Identity Theft Protection and Mitigation Services Act

The second bill signed by the governor also affects the notice that some businesses must provide to their customers. Under the Identity Theft Protection and Mitigation Services Act, whenever a business that is regulated as a CRA suffers a breach involving Social Security numbers, it must provide five years of identity theft prevention and mitigation services to anyone affected. This is the longest monitoring requirement that any state imposes. States such as Connecticut and Delaware require a business that experiences a breach involving social security numbers to provide one to two years of identity theft prevention or credit monitoring, and Massachusetts requires 18 months of monitoring be provided in similar situations. Massachusetts also has a heightened requirement for CRAs—requiring them to provide 42 months (3.5 years) of monitoring after a breach. New York's bill surpasses even that, and could push the standard amount of monitoring businesses provide. The bill, which also provides consumers with the right to freeze their credit at no cost, goes into effect on September 23, 2019.

On the Horizon: The New York Privacy Act's Data Fiduciary

In addition to heightening data security and breach requirements through the passage of these two laws, New York is also considering a new privacy law, named the New York Privacy Act ("NYPA") (S.5642), which would further expand the privacy rights of state residents. Introduced on May 9, 2019, by Senator Kevin Thomas, the NYPA, if passed, has the potential to impose stricter requirements on companies than the California Consumer Privacy Act ("CCPA") and provide legal innovations that would change the current framework of U.S. privacy law.

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.

The most surprising and novel part of the current draft NYPA is its proposal of “data fiduciary” obligations that “supersede any duty owed to owners or shareholders” of an entity. Any entity that collects, sells, or licenses personal information of consumers would be required to “exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to security the personal data of a consumer against a privacy risk.” The law defines “privacy risk” to encompass potential financial harm, physical harm, psychological harm and any other consequence that affects an individual’s “private life.” The NYPA also requires entities to act in the best interests of consumers “in a manner expected by a reasonable consumer under the circumstances.” This means, in part, that entities may not use data in any way that causes a consumer financial or physical harm, or would be “unexpected and highly offensive to a reasonable consumer.” In addition, entities must “reasonably secure” personal data from unauthorized access and “promptly inform” consumers about any breach of the fiduciary duty.

An equally significant feature of the NYPA is that it provides for a private right of action. The law may be enforced by the attorney general or “*any person who has been injured*” from a violation of the law. Violators may be subject to injunctions or liable for damages and civil penalties. Damages are to be calculated based on the number of affected individuals, the severity of the violation, and the size and revenues of the covered entity.

The NYPA would affect most companies that do business in New York or with New York residents, regardless of their location, size, or revenue. The law applies broadly to (i) any legal entity that conducts business in New York ***or*** (ii) produces products or services that target New York residents. By way of comparison, the CCPA’s application is limited to for-profit entities that either have a gross revenue greater than $25 million; annually buy, sell, or share the personal information of more than 50,000 consumers, households or devices; or derive 50 percent or more of their annual revenue from selling consumers’ personal information. The NYPA does provide certain exceptions, such as for state and local governments, personal data regulated by HIPAA or the GLBA, and data maintained for employment purposes.

The NYPA would also prohibit covered companies from using, processing or transferring personal data to third parties “unless the consumer provides express and documented consent.” Similar to the CCPA, the NYPA broadly defines “personal data” beyond traditional identifiers, e.g., name, address, social security number, to include, among other things, financial information, medical information, biometric data, internet activity information and geolocation data, as well as inferences drawn from information that could be used to create a profile about an individual’s preferences.

The NYPA establishes a broad set of rights for consumers similar to the EU’s GDPR and California’s CCPA, including the right to access personal data and certain information about how that data is being handled; the right to request that personal data be deleted, subject to certain exceptions; the right to have inaccurate personal data corrected and incomplete data completed; and the right to data portability. In addition to these rights, the NYPA also prohibits entities from making important decisions based solely on “profiling,” or, rather, using algorithms to evaluate certain personal characteristics such as a person’s economic situation, health or personal preferences.

While the ultimate fate of the NYPA is still unknown, if passed, it may surpass the CCPA in terms of privacy rights conferred onto consumers and the obligations imposed on companies that handle New York residents’ data. The NY legislative session has ended for this year, but the NYPA is expected to return to the legislative calendar in the next session

Ropes & Gray will continue to monitor developments in New York and other states and will publish additional alerts relating to these privacy laws. For more information on these New York laws or to discuss privacy or data security issues generally, please contact a member of our Data Practice group or visit https://www.ropesgray.com/en/practices/data-practice.

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.