New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 265—NO. 38

MONDAY, MARCH 1, 2021

Empire State of Privacy: Recent Developments in New York's Privacy and Cybersecurity Laws

BY ELIZABETH McGINN, AMANDA LAWRENCE, SASHA LEONHARDT AND MAGDA GATHANI

New York over the past few years has steadily raised the bar on privacy and cybersecurity standards for commercial enterprises, and, along with the European Union and California, is increasingly seen as a pacesetter in this fast-developing area of law. Proposed legislation before its General Assembly and Senate this year promises new obligations, while the New York Department of Financial Services has implemented its own cybersecurity regulations and continues to provide guidance to the financial institutions under its jurisdiction.

This article outlines new rules that companies of all stripes will need to follow in the coming years in New York. In addition, we discuss some of the privacy bills that may become law in 2021. Finally, we describe steps that companies can take now to respond to—and prepare for—these changes.

Current New York Laws And Regulations

New York's Information Security Breach and Notification Act requires companies to notify New York residents whose information is subject to a data breach. For breaches involving more than 500 individuals, the company must inform the state attorney general; breaches involving 5,000 or more individuals require notifying consumer reporting agencies, as well. In 2019, the General Assembly passed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which expanded the data elements covered by the Breach Notification Act to include account number, biometric information, or a username and password that would allow access to an online account.

However, there are limitations to the Breach Notification Act's reach. If

SHUTTERSTOCK

encrypted data is subject to a breach, a company does not need to provide notifications so long as the encryption key was not compromised. In addition, a company need not provide notice to consumers under the Breach Notification Act if it instead provides notice under the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), or another New

ELIZABETH MCGINN *and* AMANDA LAWRENCE *and are partners,* SASHA LEONHARDT *is counsel, and* MAGDA GATHANI *is an associate at Buckley LLP.*

York data security rule or regulation.

In addition to expanding the Breach Notification Act, the SHIELD Act also requires companies to "develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity" of private information. Companies can meet this requirement by implementing data security programs that contain administrative safeguards (designating employees to coordinate the program, identifying risks, assessing these safeguards, training employees, selecting service providers, and adjusting the program); technical safeguards (assessing network and risks, identifying system failures, and testing key controls), and physical safeguards (evaluating risks, detecting intrusions, and protecting information). As with the Breach Notification Act, companies that comply with the data security requirements under other laws are exempt from the SHIELD Act.

Specific Requirements For Financial Institutions Operating in New York

NYDFS Cybersecurity Regulations. NYDFS's Cybersecurity Regulations apply to financial entities under its jurisdiction, including many banks, insurance companies, licensed lenders, credit unions, trust companies, savings and loans associations, money transmitters, and virtual currency businesses. The regulations require these institutions to implement risk assessments, create audit trails, develop incident-response plans, and impose limitations on data access and data retention. They must also provide training for cyber staff, designate a chief information security officer, protect and encrypt consumer data in transit and at rest, and oversee third-party organizations' compliance with the regulations. Institutions must also notify NYDFS within 72 hours of identifying an attempted material breach of the financial institution's systems.

NYDFS filed its first enforcement action last year against a title insurance company, and it is expected that it will continue to enforce the cybersecurity regulations vigorously.

Other NYDFS Requirements and Guidance. In light of the COVID-19 pandemic, NYDFS issued a letter in March 2020 requiring businesses under its authority to submit plans to address the potential increased cyberattacks and fraud arising from the pandemic, as well as outlining measures to limit potential disruptions that are appropriate for their business profiles. In a separate letter the same day, NYDFS specifically highlighted pandemic-related risks to virtual currency businesses, including custody risk for virtual currency and the need to ensure that cryptocurrency is secure offline and available online to consumers while employees are working remotely.

In April 2020, NYDFS identified new areas of cybersecurity risk heightened by the pandemic, including secure connections, use of employees' personal devices, remote working communications, phishing and fraud, and third-party vendors. NYDFS stated that financial institutions should assess these risks and address them appropriately.

On the Horizon

New York Privacy Act. The New York legislature is considering the New York Privacy Act (NYPA), which would significantly expand privacy rights of New York residents. This legislation would prohibit businesses from using, processing, or transferring a consumer's personal data to a third party unless the consumer provides express and documented consent. Further, businesses would be required to act as data fiduciaries, acting in the consumer's best interest "without regard for the interests of the entity." Businesses would also be required to place special safeguards around data sharing and allow consumers to obtain the names of all entities with whom their information is shared. Similar to the California Consumer Privacy Act and the European Union's General Data Protection Regulation, the proposed NYPA establishes a set of consumer rights, including the right to be forgotten, the right to rectification, and the right to data portability, and, like the CCPA, would not apply to data collected under the Gramm-Leach-Bliley Act.

Senate Bill 567. Separately, the New York Senate is also considering enacting Senate Bill 567, which is also similar to the CCPA. Under both SB 567 and the CCPA, a consumer can request that a business disclose the personal information it collects about the consumer, the business purposes for collecting or

selling the information, and the categories of third parties with which it shares the information. SB 567 further parallels the CCPA by allowing consumers to opt out of the sale of their personal information, though it would not allow consumers to delete their information as the CCPA does. Additionally, while the CCPA limits the private right of action to data breaches of unencrypted information, SB 567 allows consumers to file suit for any violation of the law.

Biometric Privacy Act. Finally, New York is also considering enacting Assembly Bill 27, the Biometric Privacy Act (BPA). The proposed BPA is a mirror-image of Illinois' first-in-the-nation Biometric Information Privacy Act (BIPA), and follows other biometric privacy laws enacted in Arkansas, Texas, and Washington. Under BIPA and the proposed BPA, a covered private entity must: (1) create a publicly available privacy policy describing when it deletes biometric information; (2) provide disclosure and obtain a written release before obtaining biometric information; (3) not disclose biometric information without first obtaining written consent, in order to complete a financial transaction requested by the consumer, or as required by subpoena/warrant; and (4) exercise a "reasonable standard of care" in storing biometric information. Like the BIPA, the proposed BPA would allow for a private right of action, including statutory damages of up to $5,000 per incident. Financial institutions can expect some relief, however, as neither the BIPA nor the BPA applies to entities subject to the GLBA.

What Business Can Do Now

Given the new obligations imposed by New York's data protection laws and regulations, and the possible future expansions of these requirements, businesses serving New York consumers should review their plans for compliance with these laws. Companies may want to:

- Determine which New York (and federal) laws and regulations apply to them
- Assess their risk, including the challenges posed by the COVID-19 pandemic and remote work
- Evaluate their administrative, technical, and physical safeguards to ensure that they meet requirements that apply to their line of business
- Train employees to follow security programs, detect data breaches, and reduce foreseeable risks to business systems
- Develop a comprehensive plan for notifying consumers and government entities in the event of a data breach
- Perform data breach tabletop exercises, including containment steps to minimize data exposed in the event of a breach
- For financial institutions, consider how the collection and storage of financial data can create increased cybersecurity risk for you and your customers
- For virtual currency businesses, consider how possessing consumers' private encryption keys could make a company a target for malicious actors, and plan how to respond
- Stay abreast of legislative and regulatory developments related to data security

Given the new obligations imposed by New York's data protection laws and regulations, and the possible future expansions of these requirements, businesses serving New York consumers **should review their plans for compliance** with these laws.

Conclusion

New York is already a leader in privacy and data security, and proposed legislation seems likely to keep New York at the forefront of these areas. With several new privacy bills before the General Assembly and Senate, businesses can anticipate further demands on their privacy and data security operations in the years to come.