Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Prepare For NY Data Privacy Law To Catch Up To Calif.

By **Mylan Denerstein, Alexander Southwell, Amanda Aycock**
(January 29, 2021, 6:19 PM EST)


Mylan Denerstein


Alexander Southwell


Amanda Aycock

Gov. Andrew Cuomo's recently released 2022 budget includes a proposal for a comprehensive data privacy bill,[1] and with Democratic supermajorities in both houses of the state Legislature for the first time in history, it is likely that New York may soon have a comprehensive data privacy law that rivals the California Consumer Protection Act and the newly enacted California Privacy Rights and Enforcement Act.

This focus on data protection is not new in New York — the state recently enacted the Stop Hacks and Improve Electronic Data Security, or SHIELD, Act, an update to the state data breach notification law, and the New York Department of Financial Services, or NYDFS, has increased pressure on companies regarding data security.

The continuing shift in data privacy and data security law is set to have a significant impact on businesses' compliance efforts and operational risk, as well as on the expectations of consumers. Below we discuss what businesses can do to prepare.

Understand Existing New York Data Security Laws

Any comprehensive data privacy bill that New York passes will coexist with the data security laws already in effect. The SHIELD Act, which went into effect in March 2020, imposes cybersecurity requirements on companies that collect or maintain private information of New York residents, and the NYDFS Cybersecurity Regulation, Part 500, which went into effect in March 2017, imposes them on financial service companies that do business in New York.

The SHIELD Act

The SHIELD Act amended New York's data breach notification law to broaden the definitions of "private information" and "data breach," which now includes "unauthorized access," and not just "acquisition," and to impose new data security requirements.[2] The act grants the attorney general the power to pursue civil penalties for violations, but it does not create a

private right of action.

The information protected by the SHIELD Act is narrower than what is protected under the CCPA and CPRA and includes "any information concerning a natural person which ... can be used to identify such natural person" in combination with any of the following sensitive data elements: (1) Social Security number or driver's license number; (2) biometric information; (3) account, credit and debit card numbers, under certain circumstances; and (4) usernames and/or email addresses and their corresponding passwords or security questions and answers.[3]

But the SHIELD Act's reach is broader than CCPA or Part 500: If a business collects or maintains the private information of a single New York resident, New York would likely take the view that the business is subject to the act, even if the business is based and has operations outside of New York.[4]

While the SHIELD Act imposes new requirements on businesses, it is more flexible than Part 500. Rather than mandate specific safeguards, it requires the implementation and maintenance of reasonable administrative, physical and technical data safeguards and provides examples.[5]

The suggested safeguards have some overlap with Part 500's more rigid requirements, including, for example, designating an employee to oversee the data security program. The act specifies that if an entity is compliant with Part 500, or certain federal statutes, like the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act, then it is deemed compliant with the SHIELD Act as well.[6]

NYDFS Cybersecurity Rule Part 500

Part 500 only applies to companies that are subject to the NYDFS' authority, including state-licensed banking and financial institutions and insurance companies, together with their affiliated companies and subsidiaries.[7]

Part 500 requires covered entities to implement and maintain robust cybersecurity programs, which include designating a chief information officer and implementing, among other things: various specified written policies, periodic risk assessments, continuous monitoring or periodic penetration testing, biannual vulnerability assessments and annual certifications of compliance by the board of directors or a senior officer.[8]

Enforcement

New York is ramping up its enforcement of these provisions. The attorney general has not yet publicly announced any actions brought pursuant to the SHIELD Act, but a few settlements in the last year have included requirements for businesses that mirror the SHIELD Act's specified examples of what is reasonable for a data security program.

NYDFS Superintendent Linda Lacewell brought her first action based on Part 500 last year: In July 2020, she announced charges against First American Title Insurance Co. based on an alleged vulnerability in the company's information systems that resulted in the purported exposure of millions of consumers' sensitive personal information.[9]

Developments in the State To Watch

Increased Public Scrutiny

Businesses that have New York residents as customers should keep an eye on what is going on in New York, and not just legislatively. Even in the absence of clear legal authority or jurisdiction, the NYDFS has endeavored to pressure companies into adopting practices that would render them compliant with Part 500.

A prime example of this is the NYDFS' October 2020 report on Twitter Inc. After the Twitter accounts of high-profile individuals like former President Barack Obama and Kim Kardashian were hacked by bitcoin scammers in July 2020, Cuomo directed the NYDFS to investigate the cyberattack.

Despite Twitter's cooperation, the NYDFS issued a scathing report calling for broad cybersecurity regulation of social media companies "to curb the potential weaponization of major social media companies."[10]

In contrast, NYDFS Superintendent Linda Lacewell praised NYDFS-compliant cryptocurrency companies for their response to the Twitter hack: "The[ir] swift and effective response … illustrates how effective regulation can foster innovation and growth, while also protecting consumers."[11] The message is clear — if companies do not live up to the data protection standards set forth in Part 500, the NYDFS will use the bully pulpit in order to encourage companies to do so, even in the absence of clear jurisdiction.

Lacewell's focus on data protection is not entirely surprising. Since her confirmation in June 2019, she has made several public statements noting her intention to focus on ensuring privacy, cybersecurity and consumer protection.

She has already created two new divisions to do just that: the Consumer Protection and Financial Enforcement Division, and the Cybersecurity Division — the latter is the first of its kind to be established by any insurance or banking regulator in the country. Companies should therefore expect continued pressure to live up to the NYDFS' data privacy, security and consumer protection standards.

New York Data Accountability and Transparency Act

Cuomo's proposal for a comprehensive data privacy law, which is quite similar to the CCPA and CPRA, is titled the New York Data Accountability and Transparency Act, or NYDATA. If Cuomo and the Legislature come to agreement, it could potentially be finalized as soon as April 1 when the state budget is due.

Over the past few years, Democratic legislators have proposed at least four comprehensive privacy bills, many of which include more stringent provisions than the governor's proposal, for example, a broad private right of action or criminal liability for some violations.[12]

Given the Democrats' veto-proof majority in the state Legislature, it is possible that the final bill might include of some of these heightened protections or broader enforcement mechanisms. Nonetheless, any bill that passes will likely have a delayed effective or enforcement date — NYDATA proposes a two-year grace period — so businesses should take comfort in knowing that they will have some time to come into compliance.

Furthermore, companies can likely leverage the work already done or underway for CCPA or CPRA compliance. Below are some steps businesses can take now to get ready.

Consider whether the business might be subject to a New York privacy law.

The proposed NYDATA applies to "legal entities, including any affiliates, that conduct business in New York state or produce products or services that are intentionally targeted to residents of New York state" and either (1)"control ... or process ... personal information of one hundred thousand [identifiable natural persons who are New York residents] or more" or (2) "derive ... over fifty percent of gross revenue from the sale, control, or processing of personal information."[13]

The former threshold is similar to the CPRA's revised threshold for applicability as it concerns California residents — the CPRA revised the CCPA's comparable 50,000 threshold up to 100,000. The latter threshold is broader than CCPA and CPRA's comparable provision, which just applies if the business derives fifty percent of gross revenue from the sale or sharing of California residents' information — the NYDATA provision looks at gross revenue derived from the sale, control or processing of any personal information.[14]

There is also the possibility that any finalized New York law may reach further: the already-effective SHIELD Act has broad reach, and the privacy bills previously proposed in the Legislature have had a broad scope. For example, state Sen. Kevin Thomas' proposed New York Privacy Act would apply to "legal entities that conduct business in New York State or Produce Products or Services that are intentionally targeted to residents of New York State."[15]

Evaluate the purposes of data collection and data minimization practices.

The proposed NYDATA requires that covered entities "[o]nly collect personal information relevant to the purposes for which they are intended to be used and only to the extent necessary for those purposes."[16] Extending compliance with California laws to New York may be the solution for some companies, since the CPRA memorializes the right to data minimization and will likely come into effect before any New York equivalent.[17]

Determine what personal information is maintained.

Any New York comprehensive privacy law will require the implementation of mechanisms to protect personal information and to respond to requests to access, control, correct, delete and opt out of the sale or sharing of such information.

Under the proposed NYDATA, personal information consists of "data relating to an identified or identifiable natural person."[18] The most notable example categories include: employment information; medical or insurance information; commercial information like records of products purchased; biometric information like fingerprints; internet activity; political information or criminal history; geolocation data; and inferences from any personal information that could create a profile about preferences and characteristics.

The proposed NYDATA definition excludes publicly available data — which includes federal, state and local records and any public information — deidentified data, and employee and job applicant information like emergency contact information or benefits information.[19]

The NYDATA definition of personal information, and its exclusions, closely mirrors the information protected and excluded under the CPRA, with a few notable exceptions: The NYDATA includes political information and information on criminal convictions and arrests but does not include genetic

information.[20] Accordingly, companies working on compliance with the CPRA may be one step ahead but may need to conduct some additional assessment of what New York personal information is maintained.

Prepare to update disclosures and website.

The proposed NYDATA would require, among other things, that businesses disclose the type of data collected, the purposes for such collection, whether any personal information is shared with third-party data processors or controllers, financial incentives, and the rights granted under the NYDATA and how to exercise them including the rights to limit data collection; return, destroy and correct data; and to data protection, portability and nondiscrimination.[21]

Additionally, businesses must incorporate a "do not sell or share my personal information" link on the business' internet homepage.[22] The rights and related disclosures required by the proposed NYDATA are consistent with the core tenets of the CCPA and CPRA, so disclosures and policies compliant with those laws may serve as good models for compliance with the eventual New York law.

In short, assessing compliance with the CCPA and CPRA may be the first step in getting ready to comply with a future New York privacy law. Companies should keep in mind that, once a privacy law is passed, state agencies will also issue rules, regulations and guidance, which may both create additional obligations and provide clarifications.[23]

While the proposed NYDATA does not create a private right of action and instead establishes enforcement and regulatory authority in the secretary of state and Department of State, notably, not the attorney general, any final New York privacy law might include a private right of action given Democratic majorities.[24] Past proposals, such as the NYPA, for example, would have granted New Yorkers the right to sue for injuries suffered as a result of any violation of the law.[25]

While it was not on the governor's agenda, the recently proposed, bipartisan Biometric Privacy Act, which is nearly identical to the Illinois Biometric Information Privacy Act, also includes a private right of action for violations, further suggesting legislative support for such a provision in the context of data privacy.[26] Such a right would be broader than the limited private right of action in the CCPA and CPRA, which only applies in the data breach context.[27]

With the SHIELD Act now in effect, the NYDFS' developed interest in policing privacy and cybersecurity, and comprehensive data privacy legislation looming, New York is setting itself up to follow California as the nation's next important player in consumer data privacy.

Mylan L. Denerstein and Alexander H. Southwell are partners, and Amanda M. Aycock is an associate, at Gibson Dunn & Crutcher LLP.

Gibson Dunn associates Lisa V. Zivkovic and Jennifer Katz contributed to the preparation of this article.

[1] Governor Andrew M. Cuomo, FY 2022 New York State Executive Budget: Public Protection and

General Government Article VII Legislation 144, New York Data Accountability and Transparency Act (2021).

[2] N.Y. Gen. Bus. Law § 899.

[3] Id. §899-AA(1)(a)–(b).

[4] See id. §899-BB4(2)(a)

[5] See id. §899-BB(2)(a)–(c)

[6] See id. §899-BB(1)(a).

[7] N.Y. Comp. Codes R. & Regs. tit. 23, §500.1(c).

[8] Id. § 500.2–17.

[9] Press Release, N.Y. Dep't of Fin. Servs., Department of Financial Services Announces Cybersecurity Charges Against a Leading Title Insurance Provider for Exposing Millions of Documents with Consumers' Personal Information (July 22, 2020), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221.

[10] N.Y. Dep't of Fin. Servs., Twitter Investigation Report (Oct. 14, 2020), https://www.dfs.ny.gov/Twitter_Report.

[11] Id.

[12] See, e.g., Right to Know Act Senate Bill No. 1349/Assembly Bill No. 400 (2021-2022) (declaring privacy a fundamental right); New York Privacy Act, Senate Bill No. 5642/Assembly Bill No. 8526 (2019-2020) (reintroduced in the Assembly in 2021 as No. 680) (creating a private right of action); It's Your Data Act, Senate Bill No. 9073/Assembly Bill No. 7736 (2019-2020) (establishing criminal liability for failure to obtain consent or exercise reasonable care); Senate Bill No. 4411/Assembly Bill No. 6351 (2019-2020) (reintroduced in the Senate in 2021 as No. 567) (creating a private right of action).

[13] NYDATA § 899-CC(1)(c).

[14] Cal. Civ. Code § 1798.140(d) (as amended by California Consumer Privacy Rights and Enforcement Act on November 3, 2020).

[15] Senate Bill No. 5642 § 1101(1) (2019-2020).

[16] NYDATA § 899-CC(3)(b).

[17] Cal. Civ. Code § 1798.100(c).

[18] NYDATA § 899-CC(1)(g).

[19] Id.

[20] Compare id. to Cal. Civ. Code §§ 1798.140(v), 1798.145(m)(1).

[21] NYDATA § 899-CC(3)-(5). Like the California laws, the proposed NYDATA also prohibits discrimination against consumers who exercise these rights, except to the extent it is "reasonably related to the value provided to the business by the consumer's information." Id. § 899-CC(4)(h)(ii); see also Cal. Civ. Code § 1798.125.

[22] NYDATA § 899-CC(5).

[23] NYDATA would create a new data privacy agency, the Consumer Data Privacy Advisory Board, which will be empowered with rulemaking authority (but not enforcement authority, like its CPRA counterpart). Id. §899-CC(7).

[24] Id. § 899-CC(9).

[25] Senate Bill No. 5642 § 1109(3) (2019-2020) (The New York State Assembly reintroduced this bill as Assembly Bill No. 680 on January 6, 2021).

[26] Assembly Bill No. 27 (2021-2022).

[27] Cal. Civ. Code § 1798.150.