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

NY Data Security Law Will Dramatically Expand AG's Reach

By **Harlan Levy and Sam Kleiner** (February 25, 2020, 2:48 PM EST)

Harlan Levy

Sam Kleiner

On March 20, a new law goes live in New York state requiring any company holding electronic records containing the private data of New Yorkers to put in place a series of data security measures.

The Stop Hacks and Improve Electronic Data Security, or SHIELD, Act is sweeping in its reach, requiring that companies comply with these standards for protecting New Yorkers' private information regardless of whether they do any business in New York. The law is a dramatic expansion of the power of the New York Attorney General's Office in the realm of data security.

Under the old law, the New York attorney general was limited to bringing a case in the event of a data breach, but now a company violating these data security standards could be subject to an enforcement action absent any breach. Based on the New York attorney general's proven track record of vigorously enforcing data security laws, it is likely that the New York attorney general will aggressively investigate potential violations of these requirements.

The SHIELD Act represents a major shift in how New York law approaches data security. New York first passed a data breach law in 2005, and it has not been updated until now. The 2005 law, General Business Law Section 899-aa, only set requirements for companies in the event of a data breach and had no requirement that companies protect private information on an ongoing basis.

The SHIELD Act provides a set of detailed requirements on how companies holding New Yorkers' private information must protect that data with an array of data security protections.

These requirements carry penalties that could be very significant for companies. If the New York attorney general finds that a company has failed to maintain those standards, the office can seek injunctive relief to enjoin such violations and issue fines of up to $5000 for each violation under General Business Law Section 350-d.

Enforcement authority is also provided in Section 899-aa to the New York attorney general under Article 63 of the General Business Law, one of the New York attorney general's most powerful tools.

Under the new law, the New York attorney general does not have to wait for a data breach to start an investigation. The New York attorney general's Bureau of Internet and Technology is responsible for enforcing these laws and states on its website that it “accepts tips and complaints directly from the public.”[1]

A data breach or a news story calling into question a company’s data security or a whistleblower within a company or a disgruntled former employee making a report to the New York attorney general could set off an investigation.

New York has a powerful 2020 counterpart in California. Much ink has been spilled about California’s recently enacted California Consumer Privacy Act, and companies have devoted substantial resources to compliance with the new law. The CCPA became operative on Jan. 1, and the California attorney general will be allowed to bring actions as of July 1.

The core of the CCPA is allowing California residents to find out how companies have used and stored their data and providing mechanisms for consumers to demand its deletion. The CCPA also allows California residents to bring private suits where companies have failed to utilize reasonable security measures,[2] and an earlier California state law required companies to have reasonable security procedures and practices for private information.[3]

Neither California law defines what data security is reasonable. A report by the California Attorney General’s Office relating to the earlier California law refers companies for guidance on the meaning of reasonable security to an external report by the Center for Internet Security’s controls program. By contrast, the SHIELD Act takes steps toward defining reasonable data security, providing companies with some direct guidance in the statute itself on the sets of measures companies must take.

The reasonable security requirement in the SHIELD Act expansively applies to “any person or business that owns or licenses computerized data which includes private information of a resident of New York.” The New York attorney general played a role in sponsoring this bill and the law specifically empowers the New York attorney general to pursue actions against companies that fail to reasonably protect the personal information of New Yorkers absent these businesses even conducting business in the state.

Indeed, the SHIELD Act amended the 2005 law on data breaches to remove the requirement that a business must conduct business in New York state to be subject to the law.

Further, the SHIELD Act applies to any person or business that holds the private information of a New York resident, regardless of the size of the company, with partial exemptions for companies already complying with the data security provisions established under other laws.

A small business (one with fewer than 50 employees, less than $3 million in gross annual revenue in each of the last three fiscal years or less than $5 million in year-end total assets) must still maintain reasonable data security measures, adjusted for the size of its business and other relevant factors.

Companies subject to the SHIELD Act will have to ensure that they meet the requirements for three categories of safeguards: reasonable administrative safeguards, reasonable technical safeguards and reasonable physical safeguards. These requirements are akin to technical guidance — the law contains descriptions of how companies should take steps to ensure they are complying with these requirements.

The law requires not only that the company set up these systems but that they then maintain them by

regularly testing and monitoring “the effectiveness of key controls, systems and procedures,” as well as training and managing “employees in the security program practices and procedures.”

Further, the law applies not only to how companies maintain their data but also to the disposal of data. Businesses must establish systems for disposing “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.” This is an obligation companies will have to approach carefully because it has to be balanced with any potential legal obligations to preserve data, such as a litigation hold.

Based on the New York attorney general's track record, it is likely that the New York attorney general will seek to aggressively enforce the new data security requirements. As the bill was making its way to becoming a law, Attorney General Letitia James described the 2005 law as outdated[4] and said that companies will be held accountable under the SHIELD Act.[5]

The New York attorney general’s press release on passage specifically noted that the law imposes consumer data protection obligations.[6] The New York attorney general has regularly brought cases against companies that it believes violated the data breach requirements of the 2005 law — pursuing cases in 2019 against Dunkin’ Brands Group Inc. (the franchisor of Dunkin Donuts) and Bombas LLC (an online sock company) — but now the New York attorney general can bring cases even where there has not been a data breach.

With no federal law establishing companies’ obligations to protect data and to respond to a data breach, state attorneys general are leading the way on these issues. Though the Federal Trade Commission has some limited authority in the privacy arena, that authority is framed in acting against unfair and deceptive practices and the agency “is woefully understaffed in privacy.”[7]

With Americans deeply concerned about their data privacy, it is unsurprising that the state attorneys general — with the New York attorney general as a leader — have focused on building out data security laws and then enforcing them.

The SHIELD Act also expanded the scope of a company’s requirements in the event of a breach. These amendments to the existing law were effective immediately when the governor signed the law in July 2019. The law expanded the definition of “private information” to include “a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account” as well as biometric information.

The law even expanded the definition of a “breach.” Where the old law specified a breach was an unauthorized acquisition of information, the SHIELD Act provides that unauthorized access also constitutes a breach. And in removing the requirement that the business conducts business in New York state, the data breach requirements now apply to any company that holds the private information of New Yorkers.

As of March 20, a new data security law becomes effective, and the New York attorney general will be empowered to enforce the new requirements. The New York law provides a measure of guidance defining reasonable security and has potential application to corporations regardless of whether they do business in the state. New York has had a data breach law on the books for 15 years, but now a new era of data security enforcement begins in earnest.

Harlan Levy is a partner at Boies Schiller Flexner LLP and former chief deputy attorney general of New York.

Sam Kleiner is an associate at the firm.

[1] https://ag.ny.gov/bureau/internet-bureau.

[2] Cal. Civ. Code § 1798.150.

[3] Cal. Civ. Code Section 1798.81.5(b).

[4] https://ag.ny.gov/press-release/2019/attorney-general-james-applauds-passage-shield-act.

[5] https://ag.ny.gov/press-release/2019/attorney-general-james-statement-shield-act.

[6] https://ag.ny.gov/press-release/2019/attorney-general-james-statement-shield-act.

[7] https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html.