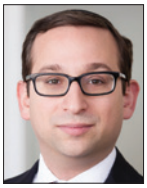
New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 262—NO. 66
WEDNESDAY, OCTOBER 2, 2019

Outside Counsel

Preparing for New Requirements Under the N.Y. SHIELD Act



By **Mark Krotoski**

And **Martin Hirschprung**

On July 25, 2019, New York Governor Andrew Cuomo signed the Stop Hacks and Improve Electronic Data Security Act, or SHIELD Act (the Act) into law, which provides significant changes to New York's Information Security Breach and Notification Act.

The Act establishes three major changes: (1) expands the data elements that may trigger data breach notification to include biometric information, user names or e-mail addresses, and account, credit or debit card number; (2) broadens the definition of a breach to include unauthorized "access" (in addition to unauthorized "acquisition") and (3) creates a new reasonable security requirement for companies to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of" private information of New York residents. The first two changes take effect on Oct. 23, 2019; the third change becomes effective on March 21, 2020.

These amendments reflect a recent trend to enact stricter data breach laws. For companies responding to data breach incidents, the amendments further add to the current patchwork of differing state standards.

Presently, 54 U.S. jurisdictions (50 states and the District of Columbia, Guam, Puerto Rico and the Virgin Islands) require notification of data security breaches involving "personal information" or "private information" (PI). Collectively, the differing standards create cumbersome, costly and complex requirements. Uniform national standards would simplify the process and avoid conflicts in the laws in a more efficient and cost-effective manner.

Analysis of Changes

PI Expanded Scope. Most data breach notification laws have a core definition of "PI" (in New York, "private information") which may trigger data breach notification requirements. The core data elements typically include an individual's name in combination with an unencrypted (a) Social Security number, (b) driver's license or state identification card number, or (c) account or credit or debit card number along with a security code, access code or password that would permit access to the financial account. See, e.g., Cal. Civ. Code §1798.82(h)(1)(A), (B), (C).

Uniform national standards would simplify the process and avoid conflicts in the laws in a more efficient and cost-effective manner.

The states continue to expand the definition of PI that may trigger data breach notification requirements. For example, some include

MARK KROTOSKI *is a litigation partner in the privacy and cybersecurity, and antitrust practice groups of Morgan, Lewis & Bockius. He served as the National Coordinator of the Computer Hacking and Intellectual Property Program in the Criminal Division of the U.S. Department of Justice.* MARTIN HIRSCHPRUNG *is an associate at the firm.*

medical and health insurance information, eight include passport information, North Dakota includes the maiden name of the individual's mother, and at least three include military identification number.

The Act broadens the definition of PI in three significant respects. Now, PI will include, in combination with a personal identifier: (1) biometric information and (2) an account, credit or debit card number, if the number could be used to access an individual's financial account without any additional identifying information, such as a security code or password. Additionally, even without a personal identifier, PI includes: "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."

Why the Addition of Biometrics Is Important. Biometric information represents a new frontier of data collection. Thus, the protection of this information, and the laws surrounding it, is crucial.

Seventeen states include biometric information as PI. Under the Act, "biometric information" is defined as "data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity." While some common examples are provided, other unspecified forms may apply.

The definition varies among the states. For example, Arizona's definition only covers information that relates to online account access; New Mexico adds facial characteristics and hand geometry; and some states, including Colorado, Maryland, and Louisiana, do not define "biometric data".

Currently, three states have laws focused on protecting the privacy and use of biometric data. Two statutes (the Washington Biometric Privacy Act and the Texas Biometric Identifier Statute) do *not* provide consumers with a private right of action, while the Illinois Biometric Information Privacy Act does. In January 2019, the Illinois Supreme Court held that individuals can file suit under the Illinois Act for a mere violation of the law's requirements, even if the individuals do not suffer any actual harm. See Rosenbach v. Six Flags Entertainment, 2019 IL 123186 (Jan. 25, 2019).

The legal landscape is changing on biometric information. Firstly, biometric information is subject to heightened protections under the European General Data Protection Regulation and the California Consumer Privacy Act (effective January 2020). Secondly, a number of bills relating to biometric data collection have recently been introduced at both the state (see, e.g., Mass. Bill S.120 and similar proposals in New York, Delaware, Michigan, among others) and federal level (see S. 847, Commercial Facial Recognition Privacy Act of 2019). Finally, there is a proliferation of wearable digital devices and "Internet of Things" devices as biometric access is designed into consumer-facing products and workplace processes. The Act represents another effort to have biometric information covered under data breach notification laws.

User Names and Passwords. The Act adds "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" to the definition of "PI" an additional data element for which companies to assess. This change does not limit the online account referenced therein only to accounts that contain sensitive personal or financial information.

At least twelve states have expanded the PI definition to include user names and passwords. California was the first to include usernames and email addresses in January 2014, followed by Florida in July 2014 and Wyoming in July 2015. See generally LawFlash, Three States Join Others to Expand Personal Information Definition to Include Usernames or Email Addresses (Jan. 3, 2017) (Illinois, Nebraska, and Nevada join trend). There are variances in the other states, creating more inconsistencies.

For example, we previously noted that in most jurisdictions, a username or email address combined with the password or security question and answer provides an independent basis to meet the PI

definition—even if no first or last name (or other personally identifiable information) is disclosed. However, the Nevada, Rhode Island, and Wyoming definitions require at least a last name and first initial to also be disclosed.

Access Versus Acquisition. Current New York law focuses on the "acquisition" of data: "Breach of the security of the system" shall mean "*unauthorized acquisition or acquisition without valid authorization* ..." (Emphasis added.)

The Act broadens the definition of security breach to include access of PI. Factors indicating access include whether "the information was viewed, communicated with, used, or altered without valid authorization or by an unauthorized person."

Some states use the "access" standard. Under this standard, a more extensive forensic analysis may be required when companies learn about a possible breach. It remains to be seen whether other states using the "acquisition" standard will also add the access standard.

New Reasonable Security Requirement. The Act requires covered entities to develop, implement, and maintain "reasonable safeguards" to protect the security, confidentiality, and integrity of private information. The safeguards may include designating employees to coordinate the security program; conducting risk assessments and employee training on security practices and procedures; selecting vendors capable of maintaining appropriate safeguards and implementing contractual obligations for those vendors; and disposal of private information within a reasonable time. At least 25 states have laws that address comparable data security practices.

Notably, the Act does not provide for a private right of action, which is the case for the Colorado, Delaware, Illinois, Louisiana, Maryland, Minnesota, Oregon, Rhode Island and Vermont statutes. New York and the remaining states leave enforcement of the reasonable security requirement to the state attorney general or other responsible state official.

> Compliance under the patchwork of state laws is more costly, cumbersome and complex and may ultimately have the unintended consequence of diverting limited resources to compliance without enhancing cybersecurity.

Laws such as the Health Insurance Portability and Accountability Act, the New York Department of Financial Services Cyber-Security Regulations, and the Gramm-Leach Bliley Act already cover many New York companies. The Act takes these laws into account and exempts businesses that are already regulated by and comply with notice requirements under those laws from certain further notification and security requirements. (The Act also provides an exemption from notification where inadvertent disclosure occurs at the hands of persons authorized to access PI and disclosure will not likely result in misuse or harm. This determination must be documented and where more than 500 New York residents are affected a copy of the documented analysis must be provided to the New York Attorney General within 10 days of the determination.)

Notification Period. As another trend, many states are imposing specific time periods for data breach notification to individuals or state attorneys general. For example, some impose a 30-day notification period; some a 45-day notification period; and others a 60-day notification deadline.

The Act maintains existing law in New York in that it does not impose a particular notification period. Under New York law, notification is required to "be made in the most expedient time possible and without unreasonable delay…".

Other Changes. The Act increases the penalties for "knowingly or recklessly" violating the statute, allowing a court to "impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification" up to $250,000, increasing the maximum penalty of $150,000 provided under current law.

The Act also extends the statute of limitations for enforcement actions. Under existing New York law, an enforcement action must be brought within two years from "the date of the act complained of

or the date of discovery of such act." Under the Act, the period would be extended to three years from either (1) the date on which the attorney general became aware of the violation, or (2) the date of notice sent to the attorney general but not later than six years following the discovery of the breach by the company (unless the company took steps to hide the breach).

Additionally, while New York's existing data breach notification requirement only covers any person and business that conducts business in New York state, the Act requires that any person or business that holds New York residents' PI must comply with the Act.

Conflicting Patchwork Standards

As noted, 54 U.S. jurisdictions have their own data breach notification statutes. While each statute is ostensibly passed to strengthen notification laws in a particular state, without uniform standards companies must comply with conflicting standards among various states. We have discussed some notable variations. Additionally, many of these laws diverge on requiring a risk-of-harm analysis, permitting a private right of action, an encryption safe harbor and who must be notified.

The time has come for the enactment of a uniform federal standard for data breach notification. See, e.g., M. Krotoski, et al., "The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze," BNA's Privacy & Security Law Report, 15 PVLR 271 (Feb. 8, 2016). This would make the notification process more certain, efficient and effective.

We believe that a uniform state data breach notification standard as well as the government cooperating with the private sector in developing cyber-security laws, are necessary to protect individuals' information. Compliance under the patchwork of state laws is more costly, cumbersome and complex and may ultimately have the unintended consequence of diverting limited resources to compliance without enhancing cybersecurity.

Next Steps

Any "person or business that owns or licenses the private information of a New York resident" should consider:

The effective date for the new data breach requirements is Oct. 23, 2019.

- Assess what "PI" may be collected including biometric or account log-in information of any New York resident.
- Assess what other jurisdictions may apply including the PI of other state residents.
- Consider the new "access" standard for any unauthorized access of PI.
- Review and, if necessary, revise data protection and breach notification policies and procedures.
- Review your incident response plans including to ensure that the attorney client privilege and work product doctrines apply where appropriate.
- Ensure you are prepared to respond to a potential data breach incident and regularly test your incident response plan.

The effective date for the reasonable security requirement is March 21, 2020.

- Ensure you have a data security program with reasonable safeguards (including administrative, technical and physical safeguards) for computerized data PI of New York residents.
- Tailor the reasonable safeguards to the business including type of information that is collected and risks that may apply.