DORSEY
DORSEY+WHITNEY LLP

New York Expands Data Privacy Protections

August 7, 2019 – The TMCA
by Robert E. Cattanach, Nick Akerman, and Sam Bolstad

New York continued its active legislative session last week, this time by expanding its data breach notification law. The SHIELD Act (Stop Hacks and Improve Electronic Data Security), signed by Governor Andrew Cuomo on July 25, 2019, notably expands the definition of a data breach and the scope of what constitutes personal information. But the law could have gone farther; the state did not enact a private right of action, as has California, and which several other states are considering. New York's action does, however, contain several other very significant provisions in the context of data breaches involving New York residents.

Here are the major elements of the SHIELD Act:

- **Expanded Definition of What Constitutes a Data Breach:** New York expanded its definition of a data breach (a "breach of the security of the system") to include instances when an attacker merely views ("accesses") personal information, even if the attacker does not download, steal, or otherwise acquire that information, commonly labeled as 'exfiltration.' Under the expanded definition, any unauthorized "access" requires the company to provide notice of the data breach.
- **Expanded Definition of Personal Information:** New York also expanded its definition of personal information ("private information," in the Act's terms), to include two new categories: (1) biometric information, such as a fingerprint or "voice print"; and (2) an email address or user name, in combination with the corresponding password or a security question and answer. The law also requires a company to provide notice when an attacker accesses information protected under HIPAA, just as

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

if that information were “private information” under New York’s definition.

- **Global Reach:** The law applies to every company holding the personal information of a New York consumer, regardless of where the company is based. As with GDPR and soon to be California’s Consumer Privacy Act, the enforceability of this extraterritorial reach remains open to question.
- **Increased Damages:** The new law increases the maximum penalty for failure to provide notice from $150,000 to $250,000, and authorizes a statutory penalty for the greater of $5,000 or $20 per instance of failed notification. The law also authorizes courts to award actual damages to consumers.
- **Enforcement:** The law will be enforced by the Attorney General’s Office, and takes effect in 90 days, *i.e.*, late October.
- **Ramp Up to Improved Cybersecurity Programs:** The law also requires companies to improve their cybersecurity programs by March 2020. The law specifies a number “administrative, technical and physical safeguards” that each company must implement by that date, and requires each company to appoint an employee to manage the cybersecurity program. The law makes an exception for a “small business,” defined as a company with either: (1) fewer than fifty employees; (2) less than $3 million in gross annual revenue for the last three years; or (3) less than $5 million in year-end total assets. Small business are still required to maintain “reasonable” safeguards.

Increased Requirements for Consumer Credit Reporting Agencies: That same day, Governor Cuomo also signed a bill that addresses consumer credit reporting agencies, a direct response to the Equifax breach of 2017. The new law requires consumer credit reporting agencies to provide identity theft prevention and mitigation services to consumers who are affected by a security breach at a credit reporting agency. The agency must provide those protections to an affected consumer for five years, and cannot charge the consumer fees during security freezes on credit reports.

What’s Next

In the absence of any overarching federal breach notification or consumer privacy law, states are expected to continue to adopt initiatives that require companies to protect consumers’ personal information. Whether it be an expanded definition of personal information, greater statutory damages, or allowing private rights of action, individual states can be expected to keep pace with, or in some instances outpace, developments in other states. The challenges of this emerging ‘patchwork quilt’ of regulations may be significant, but compliance always starts with robust information governance policies and procedures.