New York Passes Laws That Impose New Data Security and Notification Obligations

On July 25, 2019, New York passed two bills to amend and expand existing data security laws that demand attention from companies located in the United States and abroad.[1] Although these laws do not give consumers' access to or control over their own data,[2] the laws do broaden potential liability for companies handling data of New York residents. The new laws represent a reaction to the 2017 Equifax data breach, a months-long exposure that compromised the data of 147 million people and sparked a national debate on the necessity of regulating data storage and manipulation.[3]

The two laws nominally expand data protections by (i) imposing a duty on companies to adopt reasonable data security measures and modest penalties for failing to comply, (ii) broadening the definition of "breach" to include unauthorized access and viewing of data, (iii) increasing penalty limits for failure to inform individuals about breaches of their data, and (iv) granting extraterritorial effect to these obligations.

Companies holding data of New York residents must ensure their data operations are in compliance, but should note that these new laws are more forgiving than those in peer jurisdictions. The laws offer only modest changes to data protections, grant no private right of action, and do not create any additional right, such as the right to delete or limit the use of data, that would impact a company's everyday data operations.

Modest Advances in Data Security Protections

The first law, called the Stop Hacks and Improve Electronic Data Security Act (or the "SHIELD Act"), enacts a new section, New York General Business Law § 899-bb, which requires companies possessing data of New York residents to implement a data security program with a number of features, including:

- Designating one or more employees to coordinate the program.
- Training employees in the security program's practices and procedures.

---

[1] Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019 N.Y. Laws 117; Act of July 25, 2019, 2019 N.Y. Laws 115 (the "Identity Theft Prevention and Mitigation Services Act").

[2] Data protected under the SHIELD Act includes social security and other identification numbers, banking account numbers, biometric information, and online account details such as usernames and passwords. The Identity Theft Prevention and Mitigation Services Act protects only social security information. SHIELD Act §§ 3, 4; Identity Theft Prevention and Mitigation Services Act § 1.

[3] More information on the Equifax data breach can be found at the official Equifax response website, https://www.equifaxsecurity2017.com/frequently-asked-questions/.

- Selecting service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract.
- Adopting reasonable technical and physical safeguards for the processing, transmission, storage, and disposal of data.[4]

Companies that fail to implement reasonable security measures can be fined up to $5,000 for each violation.[5]

The SHIELD Act also supplements the preexisting law under New York General Business Law § 899-aa, which concerns a company's obligation to notify victims of a data breach, by:

- Expanding the definition of a data breach to include an event of *access* in addition to *acquisition*. Under the new law, the mere unauthorized viewing of protected data, without more, qualifies as a breach.
- Broadening the scope of protected information to include three additional categories: (i) banking and credit card information; (ii) biometric data such as fingerprints and retina scans; and (iii) online account details such as usernames and passwords.
- Increasing the penalty for failure to notify affected persons of the breach from ten dollars per individual to twenty dollars, with the maximum total penalty per breach event rising from $150,000 to $250,000.[6]

Both the SHIELD Act's security program and notice requirements purport to have extraterritorial effect—i.e., they apply to entities outside of New York.[7] In other words, where an entity previously had to conduct business within New York to be subject to its data security regulations, any entity that possesses the data of a New York resident now falls within the ambit of the SHIELD Act.

The second law, known as the Identity Theft Prevention and Mitigation Services Act, is a direct response to the Equifax scandal and requires consumer credit reporting agencies to provide consumers impacted by a data breach with identity theft prevention and mitigation services for up to five years.[8]

In light of these new laws, companies must review their data operations to determine whether they possess data about New York residents. If so, they may be required under New York law to update their security measures, and if they fail to notify affected New York residents in the event of a breach, they may be subject to liability.

---

[4] SHIELD Act § 4.
[5] *Id.*
[6] SHIELD Act § 3.
[7] *Id.* §§ 3, 4.
[8] Identity Theft Prevention and Mitigation Services Act § 1.

The SHIELD Act comes into effect in late October 2019, with the exception of the security program requirements which will become effective in March 2020.[9] The Identity Theft Prevention and Mitigation Services Act will become effective in late September 2019.[10]

New York's Current Data Protection Framework

Notwithstanding the broadened data security and notice requirements, New York's data protection framework fails to provide New York residents with a means to ensure compliance with these laws and protect their data.[11]

Enforcement of these laws is solely within the purview of the New York Attorney General. Under the SHIELD Act, only the New York Attorney General may bring a civil action to enjoin violations and seek monetary penalties.[12] This serves to cement the misguided stance that consumer data does not belong to consumers. This also has the unfortunate effect of hindering consumer class actions, an emerging and potentially powerful tool in the prosecution of data breaches.

The increased penalty limits for failure to notify and failure to implement reasonable security safeguards are similarly inadequate. The maximum $250,000 fine authorized by the SHIELD Act for failure to notify does not account for the volume and sensitivity of data put at risk in an event of breach. Nor does the maximum $5,000 fine for failure to implement reasonable data security measures adequately incentivize companies to bring their data security practices into compliance. Indeed, even a few hundred thousand dollars appears a pittance in comparison to the hefty fines authorized by other jurisdictions under similar circumstances. For example, the European Union's General Data Protection Regulation authorizes fines of up to €20 million or 4 percent of worldwide annual turnover of the preceding financial year, whichever is higher, for failure to comply with an order of a supervisory authority.[13]

And while the SHIELD Act regulates failure to notify and failure to implement reasonable security measures, the bill establishes no liability for the data breach itself.

---

[9] SHIELD Act § 6.
[10] Identity Theft Prevention and Mitigation Services Act § 2.
[11] A proposed bill called the New York Privacy Act, which was introduced during New York's most recent legislative session but failed to garner enough support, would have given New York residents broad data protection rights, including the right to directly sue companies over data protection violations. S. 5642, 2019-2020 Reg. Sess. (N.Y. 2019).
[12] SHIELD Act §§ 3, 4.
[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1, art. 83(5)(e).

The Identity Theft Prevention and Mitigation Services Act also gives violators an escape hatch: they need not provide identity theft prevention and mitigation services if they "reasonably determine" that consumers were not harmed by a particular data breach.[14]

Perhaps the most troubling omission from the New York laws is any restriction on *data processing*. User data is processed and mined to understand purchasing behavior, to target advertisements, and to dissect with pinpoint accuracy the smallest human interactions. Other jurisdictions such as California, Delaware, and Utah have shifted their focus to limiting the *legitimate* purposes for which data is processed. These laws have forced businesses to explain the ways they use consumer data and give consumers greater control over their data. The most notable recent legislation directed towards these issues is the California Consumer Privacy Act of 2018.[15] That law provides consumers with broader control over their data by, among other things, allowing consumers to opt out of the sale of their data to third parties, granting consumers the right to have their data deleted by businesses that possess it, and requiring businesses to provide equal service and pricing to consumers that exercise their privacy rights.[16] Neither of the New York State laws addresses these issues.

About Curtis

Curtis, Mallet-Prevost, Colt & Mosle LLP is a leading international law firm. Headquartered in New York, Curtis has 16 offices in the United States, Latin America, Europe, the Middle East and Asia. Curtis represents a wide range of clients, including multinational corporations and financial institutions, governments and state-owned companies, money managers, sovereign wealth funds, family-owned businesses, individuals and entrepreneurs.

For more information about Curtis, please visit www.curtis.com.

[14] 2019 N.Y. Laws 115 § 1.
[15] California Consumer Privacy Act of 2018, 2018 Cal. Stat. 55.
[16] *Id.* § 3.

Please feel free to contact any of the persons listed below if you have any questions on this important development:

Jonathan Walsh
Partner
jwalsh@curtis.com
New York: +1 212 696 8817

Edward Combs
Associate
ecombs@curtis.com
New York: +1 212 696 6069

Daniel Banaszynski
Associate
dbanaszynski@curtis.com
New York: +1 212 696 6153

Mustafa Moiz
Associate
mmoiz@curtis.com
New York: +1 212 696 8832