New York State to Consider Biometric Privacy Law, Again

Insights
1.21.21

A bipartisan group of New York state lawmakers recently introduced privacy legislation that would impose new obligations on businesses related to biometric identifiers and biometric information. The Biometric Privacy Act ("New York BIPA"), introduced on January 6, would limit how companies can collect or disclose biometric identifiers and biometric information, notice and consent to persons whose data is collected, security measures for the storage of such data, and private rights of action. Employers would not be exempted from these requirements, and businesses would only have 90 days to bring themselves into compliance if the proposed law passes. If the law does take effect, New York would be the fourth state to pass such legislation, joining the ranks of Illinois, Texas, and Washington. While the law still is a long way from passing – in fact, this is the fourth biometric privacy bill introduced by New York lawmakers since 2018, with all prior bills having failed – the risks for employers who are non-compliant with the law would be high. For this reason, we recommend all companies doing business in New York pay attention to this proposal and familiarize yourself with this legislation. Here is what you need to know about this potential New York law.

New York BIPA Would Limit How Private Entities Can Use Biometric Data

Before delving into how the Biometric Privacy Act would work, it's important to first understand what biometric data would be covered by the law. New York BIPA would apply to two types of information: biometric identifiers and biometric information. Biometric identifiers are retina or iris scans, fingerprints, voiceprints, or scans of hands or face geometry. Specifically excluded from this definition are writing samples, written signatures, photographs, demographic data, tattoo descriptions, and physical descriptions, along with certain medical information. Biometric information is information based on biometric identifiers used to identify an individual. For ease of reference, this blog post will refer to biometric identifiers and biometric information collectively as biometric data.

Private entities — including employers — in possession of biometric identifiers or biometric information would be limited in how they can use such biometric data. New York BIPA would flatly forbid businesses from selling, leasing, trading, or otherwise profiting off of biometric identifiers or biometric information.

New York BIPA would also place strict limitations on when and how businesses (including employers) can disclose biometric identifiers or biometric information. Specifically, disclosure

employers) can disclose biometric identifiers or biometric information. Specifically, disclosure would only be authorized under four circumstances:

- A person or their authorized representative consents to the disclosure;
- The disclosure completes a financial transaction requested or authorized by the person or authorized representative whose data is shared;
- Disclosure is required by federal, state, or local law or municipal ordinance; or
- The disclosure is required pursuant to a valid warrant or subpoena issued by a court.

As such, New York BIPA would shift control of biometric data firmly to the person to whom the data belongs. Moreover, even if a person consents to disclosure to a third-party, that third-party would need to obtain consent before passing it on to yet another entity—and that third-party would not be permitted to profit off of that redisclosure.

New York BIPA Imposes Notice and Consent Obligations on Businesses Which Collect Biometric Data

In order to collect biometric identifiers or biometric information, a company would have to comply with three obligations under New York BIPA.

First, a company would need to inform the person whose data is being collected or their authorized representative, in writing, that a biometric identifier or biometric information is being collected or stored. As such, employers will need to consider carefully what biometric data they are collecting and, as will be set forth below, why. Does an employer use fingerprints for employees to clock in and out, or as a multi-factor authentication feature for a company phone? Does an employer use retinal scans for security? Any such uses would give rise to the duty to provide notice.

Second, a company would need to inform the person whose data is being collected or their authorized representative, in writing, of the specific purpose and length of time for which a biometric identifier or biometric information is being collected, stored, and used. Implicit in this notice requirement is the obligation for businesses to destroy biometric data at the end of the period of time set forth in the notice. New York BIPA would require that businesses develop a written policy, which would need to be made available to the public (including, for employers, their employees), establishing a retention schedule and guidelines for permanently destroying biometric data. While the guidelines should require that biometric data is destroyed once the purpose for obtaining the biometric data has been satisfied, the outside limit for keeping such data is three years from an individual's last interaction with the private entity. As such, the notice to consumer will need to be developed in tandem to this written policy.

Third, a company would need to obtain a written release from the person whose data is being collected or their authorized representative. The good news for employers is that this written release can be a condition of employment.

New York BIPA Would Also Impose Security Obligations on Businesses to Protect Biometric Data

New York BIPA would impose two standards for how biometric data would need to be stored, transmitted, and protected. First, a company would need to use the reasonable standard of care within its industry. Second, a company would need to protect such data in a manner in which it stores, transmits, and protects other confidential and sensitive information. In order to comply with New York BIPA, a company would need to comply with **both** of these standards. In practice, what that means is that a company would need to comply with the more protective standard.

New York BIPA would further suggest that the standard of protection for biometric data would be quite high. The proposed law provides examples of confidential and sensitive information as including social security numbers, genetic data, and account numbers. To the extent that employers collecting biometric data are treating it as less sensitive than these examples, they would need to reevaluate how they treat such data and implement corresponding security measures if this law passes.

New York BIPA Would Create Private Right of Action

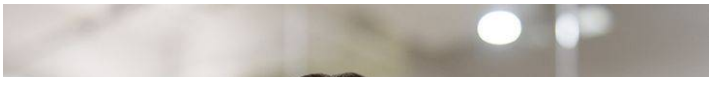
The bad news for businesses is that New York BIPA would create a private right of action in which aggrieved persons could obtain damages, attorneys' fees and costs, and injunctive relief. New York BIPA would recognize two potential types of violations—negligent violations and intentional or reckless violations. For both types of violations, aggrieved persons could obtain liquidated damages or actual damages, whichever is higher. For negligent violations, liquidated damages would be capped at $1,000; for intentional or reckless violations, liquidated damages would be capped at $5,000.

Litigation under a similar BIPA statute in Illinois has demonstrated how high the stakes can be. One federal court held that each unauthorized fingerprint scan by an employer was an individual violation under the Illinois law. The Illinois Supreme Court has held that a violation of the law even without an actual injury is sufficient grounds to bring a lawsuit. We would expect litigants in New York to make similar arguments if New York BIPA becomes law of the land.

Conclusion

Employers in New York should keep an eye on this legislation. While the fact that three prior attempts to pass this legislation may seem a bad omen for hopes of passage, privacy legislation has been gaining steam across in the states in the last couple of years — including in New York. Given this trend, it may only be a matter of when — not if — such legislation ultimately passes.

Related People



Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

Service Focus

Privacy and Cyber