ALM | LAW.COM

New York Law Journal

OUTSIDE COUNSEL

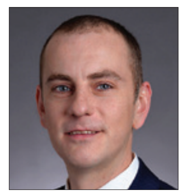
Proposed Statute Offers Sword And Shield To Protect Biometric Info

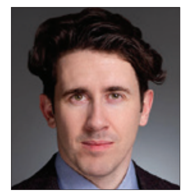
Wednesday, May 31, 2023

As technology has advanced, so too has the use of biometric information to enhance security and authentication processes. But while this biometric technology can provide more robust, advanced security—think face identification to log into your smart phone—it also carries increased risk.

If compromised, the uniquely personal nature of biometric information leaves a wronged party vulnerable to identity theft, hacking, and other nefarious privacy violations. Increasingly, legislatures throughout the U.S. are enacting statutes requiring companies that collect this information to protect it as well.

New York State's Biometric Privacy Act, first introduced in 2021 and reintroduced (as S04457/A01362) in February 2023, would act as both a shield to protect consumers from





By **John M. Leonard**

And **Seán McCabe**

the release of their biometric information, and a sword to enforce their rights should those protections fail.

Following in the footsteps of Illinois' landmark Biometric Information Privacy Act (BIPA), the BPA intends to legislate how private entities collect, retain, disclose, and destroy biometric information and identifiers. Although the bill remains in the early legislative phase, because privacy legislation has been gaining significant traction across the country it seems likely that New York's legislature will see it through to passage. The bill would take effect on the ninetieth day after it passes.

Like BIPA, New York's BPA requires that a private entity—be that an individual or an

JOHN M. LEONARD *is a shareholder in the New York office of Anderson Kill P.C. and co-chair of the firm's biometric liability insurance recovery group.* SEÁN McCABE *is an attorney in Anderson Kill's New York office and a member of the firm's white collar and insurance recovery groups.*

organization—comply with three prerequisites before collecting biometric information or biometric identifiers. First, the private entity must inform the individual in writing that the private entity is collecting or sharing a biometric identifier or information. Biometric identifiers include eye scans, fingerprint or voice prints, and scans of one's hand or facial geometry, while biometric information means any identifying information based on an individual's biometric identifier. Second, the private entity must inform the individual in writing of the specific purpose and length of time for which it is collecting or storing the biometric material. Finally, the private entity must receive a written release executed by the subject. These threshold requirements substantially mirror BIPA.

If compromised, the uniquely personal nature of biometric information leaves a wronged party vulnerable to identity theft, hacking, and other nefarious privacy violations. Increasingly, legislatures throughout the U.S. are enacting statutes requiring companies that collect this information to protect it as well.

But the private entity's responsibilities do not end there. It also must develop and implement a publicly available, written retention policy. The policy must establish a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information when the purpose for collecting has been satisfied or within three years of the individuals last interaction with the private entity, whichever occurs first. The bill also requires that private entities store all information using a reasonable standard of care that is at least as protective as for other confidential and sensitive information.

Also similar to BIPA, the BPA creates a private right of action for any aggrieved person with a right to recovery for each violation. For negligent violations, a party may recover liquid damages of $1,000 or actual damages suffered by the individual, whichever amount is greater. For intentional or reckless violations, liquidated damages are set at $5,000 or actual damages, whichever is greater. The aggrieved party may also recover reasonable attorney's fees and costs.

New York's BPA has not yet passed, so the courts have not yet weighed in. But as the legislature clearly used BIPA as a blueprint, and because BIPA has spawned numerous high-profile cases, Illinois may help predict how New York will enforce its version, should it become law. For instance, Illinois courts have broadly enforced the threshold mandates of BIPA, such that an actual data breach or misappropriation of biometric information need not occur for a claimant to be entitled to damages.

The violation itself creates a viable statutory cause of action. And because BIPA incorporates minimum statutory damages, a claimant also need not prove actual damages to recover. Moreover, Illinois courts construe BIPA such that each improper collection of biometric information constitutes a violation—entitling each claimant to at least the minimum statutory damages. Illinois courts have found entities liable for thousands of violations at a time. And at a minimum of either $1,000 or $5,000 per violation, damages can multiply quickly.

If New York courts follow Illinois' lead, New York entities currently collecting and using biometric information could face significant new statutory liabilities. And, because the New York bill adopts BIPA's statutory damages provision, losses arising out of statutory violations could mount quickly and exponentially.

The threat of these multiplied damages should immediately trigger thoughts of insurance. Ideally, New York courts also will take after Illinois regarding insurance coverage for losses sustained as a result of violations of the BPA. Fortunately for policyholders, Illinois courts also have taken an expansive view of BIPA for coverage purposes. For example, unauthorized release of biometric information to a single unauthorized party has been found to constitute publication under a standard commercial general liability policy.

Additionally, courts also have favorably found coverage under EPLI policies for employers collecting data from their employees. Even directors and officers policies may provide coverage for policyholders facing liability under BIPA or a similar statute. When legal challenges begin to hit the courts after the bill passes, New York courts' analysis of this new biometric privacy law will come into focus.

As with any emerging risk, insurance companies will closely monitor New York's BPA. The insurance industry almost certainly is developing policies to account for the additional exposure that BIPA and its clones engender.

Accordingly, policyholders that collect and use biometric information should proactively assess the entirety of their insurance programs to ensure that a loss does not fall within an area of no coverage. Losses arising from biometric liability may fit within numerous policies—the aforementioned commercial general liability, EPLI, and directors and officers to name just a few. Policyholders cannot afford to not have a shield in this fight.