SpencerFane®

Illinois: Land of 12 Million Biometric Privacy Regulators

FEBRUARY 20, 2019| PUBLICATIONS

The Supreme Court of Illinois recently held that every Illinois citizen has a private right of action to enforce violations of the Illinois Biometric Information Privacy Act ("BIPA") without alleging or showing actual harm. Businesses collecting, using and storing the biometric data of Illinois consumers take notice: there are over 12 million regulators with the power to enforce this law against you. But don't worry too much, the state's high court promises that "Compliance should not be difficult."

In *Rosenbach v. Six Flags Entertainment Corporation et al.*, 2019 IL 123186, the court considered whether a person is "aggrieved" under BIPA – and therefore entitled to the statutory damages, attorneys' fees and injunctive relief provided by the statute – if they only allege a violation of the statute but not some additional actual injury or adverse effect (e.g., unauthorized disclosure and misuse of their biometric data to their actual harm). Six Flags Great America has used fingerprinting to register and process season pass holders since at least 2014. Patrons signing up for a season pass are required to allow Six Flags to scan and store their fingerprint. The patron then presents their season pass card and scans their fingerprint to gain access to the theme park as a season pass holder. In 2014, Alexander Rosenbach, a minor, went to the park as part of a school field trip. He signed up for a season pass. Six Flags scanned his fingerprint. His mother sued, on behalf of Alex and a class of all others similarly situated, alleging that Six Flags violated the BIPA by:

1. Collecting Alexander and other consumers' biometric identifiers without giving them written notice that the information was being collected and stored;
2. Not informing class members in writing of the purposes for which the biometric information was being collected and stored, nor for how long they would keep it and use it; and
3. Not obtaining a written release from the consumers (or their legal guardians) before collecting the information.

The appellate court held that the case should be dismissed because plaintiffs alleged only a "technical violation of the Act" and not additional, actual damages. The state high court unanimously and emphatically disagreed, holding that Illinois' "General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." The court also emphasized that "[o]ther than the private right of action authorized in section 20 of the Act, no other enforcement mechanism is available."

So, there it is: Illinois consumers have a statutory right to privacy of their biometric information, and are also each empowered to enforce that statute through a private right of action, for statutory damages, attorneys' fees and possibly injunctive relief.

Any business or organization engaged or interested in collecting, storing and using the biometric identifiers and information of Illinois consumers in order to enhance and improve the goods and services they are offering need to act promptly to confirm compliance with this law. As the Illinois court suggested, this is a relatively simple endeavor as far as compliance goes – as long as you know what you need to do. Organizations should:

1. Assess whether they are, or plan to, collect and use biometric information subject to the law.
2. Adopt and implement appropriate written policies and procedures to govern their collection, retention, use, disclosure and destruction of biometric identifiers and information. These policies should align with industry best practices for information security.
3. Make the policies and procedures available to the public.
4. Prepare written notice compliant with the law, and provide that notice to individuals from whom biometric identifiers and information, and make those policies available to the public.

AUTHORS

- Thomas W. Hayde, CIPP/US

RELATED PRACTICES

- Data Privacy and Cybersecurity

BLOG TOPICS

- Privacy and Cybersecurity Solutions

5. Train all employees – upon hire and at regular intervals – on the implementation of the written policies and procedures.

An organization's biometric privacy policies should be one facet of its overall cyber risk management strategy and program. See Spencer Fane's Cyber Hygiene Checklist here.