Past, Present and Future: What's Happening with Illinois' and Other Biometric Privacy Laws

Article By
Dmitry Shifrin
Mary Buckley Tobin
Polsinelli PC
Intelligence

- Communications, Media & Internet
- Corporate & Business Organizations
- Election Law / Legislative News

- California
- New York
- Texas
- Washington

Friday, May 28, 2021

Introduction

Despite its passage in 2008, class action litigation alleging violations of the Illinois Biometric Information Privacy Act (BIPA) has increased significantly in recent years and settlement figures can be quite high. In February 2021, for example, a federal court approved the $650 million proposed settlement of a BIPA class action against Facebook.

BIPA requires private entities that obtain biometric information or identifiers to first inform the subject in writing that their information is being collected and stored, inform the subject of the specific purpose and term for collection and storage, and secure a written release from the subject. BIPA also prohibits the disclosure of biometric information without the subject's consent, unless an exception is met.
Private entities also cannot sell, lease, trade, or profit from a person's biometric information. Further, BIPA requires a private entity in possession of biometric identifiers and information to develop a publicly available written policy establishing a retention schedule and providing guidelines for the permanent destruction of the information.

Any person aggrieved by a BIPA violation may file suit to recover statutory damages of $1,000 for each negligent violation or $5,000 for each intentional or reckless violation, plus reasonable attorneys’ fees and costs. To establish standing, actual harm is not required and mere procedural violations are sufficient.

**Status of Current BIPA Cases in Illinois**

Despite the increase in litigation, there is limited controlling precedent in state court to rely upon, with federal court litigation bringing its unique considerations for parties. For example, BIPA does not provide for a statute of limitations, which is an important issue litigated across lower courts without prevailing input from appellate courts (yet). As of this writing, there also are two pending appellate court cases that will address key issues for businesses and employers facing BIPA lawsuits.

The Illinois Supreme Court is set to decide whether the exclusive remedies under the Illinois Workers’ Compensation Act bar claims for statutory damages under BIPA where an employee alleges that an employer violated the employee’s statutory privacy rights under BIPA. In *McDonald v. Symphony Bronzeville Park, LLC*, No. 1-19-2398 – highly anticipated case because the decision will impact hundreds of BIPA cases – the Defendant-former employer seeks to bar the Plaintiff-employee’s claims for injuries incurred when scanning her fingerprints to clock into and out of work. As of April 30, 2021, Defendant-Appellant filed its opening brief, and Plaintiff’s response is forthcoming. A ruling in favor of Defendant will have resounding effects on current and future BIPA cases in the employment setting, which typically involve the alleged collection of biometric information for timekeeping purposes and access to computer systems.

Pending before the Seventh Circuit is a challenge to the Northern District of Illinois’ decision that two independent and actionable BIPA violations occurred and accrued each time the Plaintiff used Defendant’s finger-scan system without appropriate notice and consent (i.e., to access both work computers as well as weekly paystubs). In *Cothron v. White Castle System, Inc.*, No. 20-3202, the Defendant and Amicus Curiae argue that potentially crippling damages may ensue if each employee is entitled to one or more awards of statutory damages each time an employee uses biometric technology. If the lower court’s reasoning stands, conservative estimates of damages for the plaintiff alone are estimated to exceed $3 million and the class to easily exceed $1 billion.

In response to the torrent of BIPA litigation, the Illinois House of Representatives is considering House Bill 559 which is intended to stem the impact of BIPA claims on businesses of all sizes in the state. Illinois House Bill 559 seeks to make several changes to BIPA: (1) narrowing the definition of biometric information by exempting “information derived from biometric information that cannot be used to recreate the...”
original biometric identifier [e.g., a numerical identifier converted from a finger scan]”; (2) employees must provide employers with written notice and an opportunity to cure a BIPA violation 30 days before being able to file a lawsuit; (3) a one year statute of limitations to file a BIPA suit; (4) eliminating statutory penalties of $1,000 or $5,000 “for each violation” and limiting recovery to actual damages and attorneys’ fees; (5) excluding suits filed by employees subject to a collective bargaining agreement; and (6) permitting electronic consent instead of requiring a “written release.”

Current and Proposed Biometric Privacy Laws in Other States

Several states have followed Illinois in passing legislation regulating the use and disclosure of biometric information; however, Illinois currently is the only state whose statute includes a private right of action. Laws governing biometric information range from comprehensive laws governing biometric information that are similar to BIPA, to data privacy laws which include biometric information within the definition of “personal data,” to breach response laws including biometric information under “covered personal information.”

Currently, only two other states have a comprehensive law governing biometric information: Texas and Washington. Tex. Bus. & Com. Code §503.001 provides that a person may not capture a biometric identifier without prior consent, may not sell biometric data without consent or unless allowed by law, must use reasonable care in storing it, and shall destroy the biometric identifier within a reasonable time. Similarly, Wash. Rev. Code Ann. §19.375.020, prohibits any company or individual from entering biometric data “in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose.” While both laws have similar requirements to BIPA, neither include a private right of action and both authorize their respective state attorney general to enforce the laws.

Other states have introduced proposed comprehensive legislation that has failed to pass, with Maryland and New York as the latest to consider implementing a comprehensive biometric information privacy law. New York Assembly Bill 27 would require written consent for collecting biometric information and prohibit the sale of that information. Maryland House Bill 218 would impose similar restrictions. Both laws would feature a private right of action, distinguishing them from the Washington and Texas statutes.

The California Consumer Privacy Act includes biometric data within the definition of personal data. The law intends to provide consumer rights related to the control of their personal information, which extends to biometric data defined as “physiological, biological or behavioral characteristics, including ... DNA[,] that can be used ... to establish individual identity,” including “imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.” Cal. Civ. Code § 1798.140(b).
New York and Arkansas both have breach response statutes covering biometrics. Specifically, in New York, the 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act includes “biometric information” within the definition of “private information.” The law requires notification to individuals upon discovery of unauthorized access to their private information. And Arkansas’ breach response law, Arkansas Code §4-110-103(7), now includes “fingerprints; faceprint; a retinal or iris scan; hand geometry; voiceprint analysis; deoxyribonucleic acid (DNA); or any other unique biological characteristics” as biometric data within the definition of covered personal information. Arkansas’ law also requires notice to individuals upon discovery of a breach of personal information.

Congressional Interest in Biometric Privacy Laws

Federal lawmakers have also shown an interest in legislating biometric information. The National Biometric Information Privacy Act of 2020 was introduced in August 2020 and would require covered entities to obtain consent prior to capturing biometrics, and also impose retention, disclosures, and destruction requirements. The proposed federal law, which is currently still under review in the U.S. Senate, would also include a private right of action.

While the future of a federal law governing biometric information remains to be seen, it is clear that the regulatory landscape governing biometrics is constantly evolving and entities handling biometric information must be vigilant as to their obligations under current and future laws, particularly as enforcement increases and private litigation shows no sign of abating where permitted.

© Polsinelli PC, Polsinelli LLP in California

National Law Review, Volume XI, Number 148