Freeborn

Your Future Is Our Purpose

Collecting Fingerprints or Other Biometric Information without Consent Could Be Costly

by Andrew L. Goldstein

A FREEBORN & PETERS LLP CLIENT ALERT

If you are an employer or other entity that is using the biometric information of your employees, customers or others, such as fingerprint or retina scans, for purposes such as timekeeping, computer login, or customer identification, you could be the target of a class action lawsuit based on Illinois' Biometric Identification Privacy Act ("BIPA") unless you have appropriate signed releases and a policy in place governing the storage, retention, and destruction of the biometric information.

What Is BIPA?

Adopted by Illinois in 2008, the BIPA regulates the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and biometric information by private entities. "Biometric identifiers" are defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." Biometric identifiers do not include: writing samples, written signatures, photographs, human biological samples used for scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. "Biometric information" means any information – regardless of how it is captured, converted, stored, or shared – based on an individual's biometric identifier used to identify an individual.

The BIPA provides that no entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's biometric identifier or biometric information unless it first:

1. Informs the subject in writing that the information is being stored;
2. Informs the subject about "the specific purpose and length" of the use; and,
3. Receives express written authorization to use the information. For employers, the release can be conditioned on continued employment.

The BIPA also requires entities storing biometric identifiers or biometric information to have a written policy establishing a retention schedule and guidelines for permanently destroying the identifiers and information when the initial purpose for collecting or obtaining them has been satisfied or within three years of the individual's last interaction with the entity, whichever occurs first.

Additionally, entities in possession of biometric identifiers or biometric information must store, transmit, and protect them from disclosure using a reasonable standard of care based on the entity's industry using the same or more protective manner as used by the entity to store, transmit, and protect other confidential and sensitive information. Further, no entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from the identifier or information.

Which States Have Regulated Biometric Privacy?
Illinois' BIPA was the first statute regulating the use of biometric information. Texas has a similar statute regulating biometric privacy, and other states – namely, Alaska, Connecticut, Montana, New Hampshire, and Washington – are considering similar legislation. Illinois' BIPA, however, is the only statute allowing private citizens to bring suits for violations of the act. Under the BIPA, an individual can recover $1,000 for each unintentional violation and $5,000 for each intentional or reckless violation, or actual damages, whichever are greater. Attorneys' fees are also recoverable.

While Illinois' BIPA has been in effect since 2008, not many cases were brought based on the act until recently when it garnered attention from plaintiff's class action attorneys. In the past couple of years, class action cases have been filed against grocery store Mariano's related to employee timeclocks, against education/daycare provider Crème de la Crème related to authorizations to pick up children, and against tech company behemoths such as Facebook, Google, Snapchat, and Shutterfly regarding facial recognition technologies.

The first reported settlement under a BIPA case was reached at the end of 2016 when L.A. Tan agreed to a $1.5 million payment. This class action alleged that L.A. Tan used fingerprint scans to identify its customers in a membership database without obtaining their consent.

How Have Courts Ruled on the BIPA?
Courts have reached opposite results as to whether a plaintiff must show damages in order to have standing to bring a claim under Illinois' BIPA.

McCullough v. Smarte Carte, Inc. was a class action suit filed in Illinois federal court alleging that Smarte Carte violated Illinois' BIPA by collecting fingerprints of consumers for rental electronic lockers, luggage carts, and the like without consent. Smarte Carte argued that the plaintiffs lacked standing to bring the claims based on a mere procedural violation of the BIPA without the plaintiffs suffering any actual damages. The court agreed and dismissed the case asking, "How can there be an injury from the lack of advance consent to retain the fingerprint data beyond the rental period if there is no allegation that the information was disclosed or at risk of disclosure?"

In January 2017, a New York federal court reached a similar holding in ***Vigil v. Take-Two Interactive Software, Inc.***, a class action suit under Illinois' BIPA, which alleged that videogame distributor Take-Two did not get consent from players of a video game that allowed players to create avatars from a scan of their face. In dismissing the case, the New York court held that the plaintiff only alleged a bare procedural violation of the Illinois act without demonstrating any harm.

An Illinois state court reached a different result, however, in ***Sekura v Krishna Schaumberg Tan, Inc.*** Like the L.A. Tan case, the defendant operated a tanning salon and collected fingerprints of members for identification purposes. As opposed to the courts in the ***Take-Two*** and ***Smarte Carte*** cases, the Illinois state court held in February 2017 that actual damages need not be shown and refused to dismiss the case, which is still pending.

Complying with BIPA
As the use of biometric identifiers expands, more and more states are likely to enact statutes similar to Illinois' BIPA regulating the use of biometric information. It is clear that, if you collect fingerprints or other biometric information from your employees, customers, or others, you need to comply with Illinois' BIPA and other similar laws by obtaining appropriate consents and by creating and adhering to policies regarding the storage, retention, and destruction of such information.

If you require assistance in creating an appropriate consent form and/or a policy compliant with biometric privacy laws, contact Andrew L. Goldstein, at agoldstein@freeborn.com.

Andrew L. Goldstein
Partner

Chicago Office
(312) 360-6438

agoldstein@freeborn.com

Andy focuses his practice in the area of Intellectual Property and Information Technology. He has extensive experience in the areas of intellectual property law, including trademark, trade dress and copyright law; technology, internet, website, cloud computing, technology, outsourcing and computer law in general; advertising, marketing, and promotion law; and entertainment law, including video production, theater and dance-related matters.