The Illinois Biometric Information Privacy Act

By Justin O. Kay, Vice-Chair, Class Actions Team
Drinker Biddle & Reath LLP

In the early 2000s, a company called Pay By Touch promised to "Change the Way the World Pays" with a "biometric" authentication and payment system. The system enabled consumers to link various accounts (credit cards, checking accounts, loyalty programs, etc.) to their fingerprints, and then access their accounts or make a payment with the touch of a finger rather than using cash or swiping a card. Investors poured $340 million into the venture, and millions of consumers signed up. By late 2007, however, Pay By Touch and one of its founders—John Rogers—were mired in controversy and litigation (including bankruptcy), and in March 2008, Pay By Touch ceased all operations.

While Pay By Touch's time was short-lived, it did have a profound impact on future endeavors involving biometric information, just not in a way that its founders likely expected. Pay By Touch's rise and fall was the catalyst for first state law governing the collection, use, safeguarding, and storage of biometric information: the Illinois Biometric Privacy Act, 740 ILCS 14/1 et seq. ("BIPA").[1] While BIPA has been on the books since October 2008, it is only recently, as the use of biometric information becomes more commonplace (the fingerprint scanner on the iPhone, for example), that BIPA is once again garnering attention—this time, from the plaintiff's class action bar. Companies looking to use biometric technology in Illinois or during interactions with Illinois residents should be aware of BIPA and ensure that they are complying with its requirements. Companies operating outside of Illinois should pay attention to similar legislative initiatives in other states.

What is BIPA?

BIPA regulates the "collection, use, safeguarding, handling, storage, retention, and destruction of *biometric identifiers* and *information*." 740 ILCS 14/5(g) (emphasis added). BIPA defines a "biometric identifier" to include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," but to exclude things like writing samples, written signatures, photographs, demographic data, physical descriptions, and certain biological materials or tissue samples used for medical or scientific purposes. 740 ILCS 14/10. "Biometric information," in turn, includes "any information, regardless of how it is captured, converted, stored, or shared,

[1] The bill that was to become BIPA was first introduced in the Illinois Senate in February 2008. During hearings on the bill in the Illinois House, Representative Joseph M. Lyons explained, "This legislation is needed because we've seen examples of biometric use in stores. Pay By Touch is the commonly used vendor at Jewel grocery stores and their affiliates. This company marketed themselves as being secure and having a safe place to keep the biometric information it collects. However, it filed for bankruptcy in 2007 and wholly stopped providing verification services in March 2008, leaving the customers who had signed on for this program in Albertsons, Cub Foods, Farm Fresh, Jewel Osco, Shell and Sunflower Market without any information as to how their biometric and financial data will be used." The preamble to BIPA likewise references the fact that, in 2008, "Major national corporations ha[d] selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias," but that "[a]n overwhelming majority of members of the public [were] weary of the use of biometrics" and "deterred from partaking in biometric identifier-facilitated transactions." 740 ILCS 14/5.

based on an individual's biometric identifier used to identify an individual," but excludes "information derived from items or procedures excluded under the definition of biometric identifiers." *Id.*

First, with regard to collection, BIPA prohibits any private entity from collecting, capturing, purchasing, or otherwise obtaining a person's biometric identifiers or information without first informing the person in writing of the collection or storage (including the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used) and obtaining a written release from the person to do so. 740 ILCS 14/15(b).

Second, with regard to dissemination, BIPA prohibits any private entity "in possession" of biometric identifiers or information from (i) selling, leasing, trading, or otherwise profiting from such identifier or information; and (ii) from otherwise disclosing or disseminating such information unless the person consents, the disclosure completes a financial transaction authorized by the person, or the disclosure is required by law or requested via warrant or subpoena. 740 ILCS 14/15(c)-(d).

Third, with regard safeguarding, BIPA requires any private entity in possession of biometric identifiers or information to "store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry," which must be at least "the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." 740 ILCS 14/15(e).

Fourth, with regard to retention and destruction, BIPA requires any private entity in possession of biometric identifiers or information to develop and adhere to "a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a).

Why are Plaintiff's Class Action Attorneys Interested In BIPA?

In recent years, the plaintiff's class action bar has increasingly focused on bringing class actions under statutes that authorize an award of statutory damages—BIPA is such a statute. Under BIPA, any person "aggrieved" by a violation may bring a claim against the "offending party" seeking $1,000 or actual damages (whichever is greater) for each negligent violation; $5,000 or actual damages (whichever is greater) for each intentional or reckless violation; reasonable attorneys' fees, litigation expenses, and costs (including expert witness fees); and "other relief, including an injunction." 740 ILCS 14/20.

The ability to aggregate such claims via a class action has resulted in BIPA claims involving facial recognition technology being filed against Facebook, Snapchat, Shutterfly, and Google related to the use of facial recognition software in conjunction with users' photographs, and against video game manufacturer Take-Two Interactive Software related to the creation of

personal avatars. It has also resulted in BIPA claims involving the use of fingerprinting being filed against LA Tan and Palm Beach Tan related to their membership management programs, against education/daycare provider Crème de la Crème related to verifying the identity of individuals authorized to pick up children, against rental locker provider Smarte Carte related to accessing rental lockers, and against grocery store chain Marianos related to clocking employee hours. The suits have met with mixed results—some have been dismissed at the pleading stage, some have settled (the suit against LA Tan settled on a class-wide basis for $1.5 million), and some remain ongoing.

What Other States Have Similar Laws?

As noted above, BIPA was the first state law of its kind when passed by Illinois in 2008. Texas passed a similar law in 2009 called the Capture or Use Biometric Identifier Act. Early this year, lawmakers in Alaska, Connecticut, Montana, New Hampshire, and Washington each proposed their own laws similar governing the collection, use, and retention of biometric information.

What Are The Key Points for Ensuring Compliance?

The starting point for companies considering using biometric identifiers or information is simple awareness of BIPA. Though simple in concept, it does not appear to have been as simple in practice—until the plaintiff's bar began filing suits, BIPA appears to have received little attention. Once one is aware of the statute, the general requirements for compliance are relatively straightforward: biometric identifiers and information cannot be sold and cannot be kept longer than the shorter of three years or until the original purpose for which they were collected is satisfied, and companies should implement and adhere to robust written policies and procedures for collecting and safeguarding biometric identifiers and information, and obtain written consent from the persons from whom they were obtained in order to use them.