Get Your Acts Together, Act VI: The Biometric Information Privacy Act

It has been a decade since the Illinois legislature passed The Biometric Information Privacy Act, or "BIPA", as it is known to nobody but a handful of employment attorneys. BIPA sets forth standards of conduct for private entities in connection with the collection and possession of biometric identifiers and biometric information.

I know what you're thinking. *Emily, I may be a successful business owner, but I am no Dr. Strangelove! How does this apply to me?*

Glad you asked. As it turns, out, a "biometric identifier" includes: a retina or iris scan, **fingerprint**, voiceprint, or hand-or face-geometry scan. *That's right, I said fingerprint.*And since many, many clients use fingerprint scans for employees to enter their place of work and patrons to enter their facilities, BIPA applies to more than meets the scanned-with-your-consent eye.

Paperwork Protocols

The Act requires private entities to develop **written policies**, made available to the public, establishing a retention schedule and guidelines for the destruction of biometric identifiers.

Private entities who collect or purchase biometric identifiers are required to first (1) inform subjects that the information is being collected or stored; (2) inform subjects of the purpose and length of term for which the information is being collected and stored; and (3) **receive from subjects written consent** to collect the information. Private entities are prohibited from selling the information and from disclosing the information without consent or other authorization.

Retention Requirements

The Act also requires "using the reasonable standard of care within the private entity's industry" to store and protect the information.

BIPA violations may cost employers as much as *$5,000 per violation.* The good news? If you haven't been in compliance, don't panic. Section 20 of the Act provides a cause of action to any "person aggrieved by a violation of this Act." But what does "aggrieved" mean in the context of BIPA? Last December, the Illinois Appellate Court (2nd District) shed light on the Act's limits in its review of a case where a mother purchased a season pass for her son for the Great America theme park* and defendants fingerprinted him without properly obtaining written consent or disclosing their plan for the collection, storage, use, or destruction of his biometric identifiers or information.

The Court threw out the case, finding that the Plaintiff was not aggrieved. While acknowledging that BIPA does not define "aggrieved," the Court held that "[a]lleging only technical violations of the notice and consent provisions of the statute, as plaintiff did here, does not equate to alleging an adverse effect or harm." The Court went on to dismiss any notions that BIPA is a strict liability statute (those where liability considerations begin and end at a violation, no matter the efforts made to prevent it, nor the harm done). In a nice soundbite for defense attorneys, the Court opined that reading BIPA as "a strict liability statute permitting a private cause of action for a mere technical violation ... requires that the word 'aggrieved' be read out of the statute. We avoid a construction of a statute that results in words being superfluous."

The Takeaway? If you use or are planning to use fingerprint scans or other biometric identifiers, take care to ensure your notice provisions and storage protocols are in compliance. Otherwise, you could face fines as quickly as you can scan your retina, as they say.

* Lucky kid!

Source: 740 ILCS 14/15 (2008)