Legal Alert: Employers Must Comply With The Illinois Biometric Information Privacy Act

1/15/2009

With increasing frequency, employers are using "biometric information" of their employees as a means of identification for an array of work-related transactions, such as background screening, computer login, timekeeping, and facility access. In October 2008, the Illinois legislature enacted the Biometric Information Privacy Act (the "Act"), 740 ILCS 14/1 *et seq*., to regulate the collection, use, safeguarding, and storage of biometric information by private entities and to address public concerns regarding use of biometric information. "Private entities" under the Act include "individual[s], partnership[s], corporation[s], limited liability company[ies], association[s], or other group, however organized." As noted below, the definition contemplates private entities who collect biometric information for employment purposes.

Biometric information includes retina or iris scans, fingerprints, voiceprints, or scans of hand or facial geometry. The list of what is *not* biometric information protected under the Act is fairly extensive and includes such things as handwriting and signatures, biological "samples" (such as blood or tissues), or physical descriptions such as eye color, hair color, height, or weight. The Act also excludes from coverage such things as x-rays, MRIs, mammograms, and other image or film of a person's anatomy.

The requirements of the Act apply to a private entity that possesses biometric information, regardless of the purpose or intended use. Any private entity in possession of biometric information must develop a written policy, which must be made available to the public. The policy must establish and describe a retention schedule and guidelines for permanently destroying biometric information. The Act provides that biometric information collected by a private entity must be destroyed when the initial purpose for collecting the information has been satisfied, or within three years of the individual's last interaction with the entity – an employee's resignation, for example – whichever occurs first.

Before a private entity may obtain biometric information, it must first inform the individual (or a legally authorized representative) that his or her biometric information is to be collected; indicate the purpose for collecting the biometric information and the length of time for which it is to be collected, stored, and used; and receive a written release from the individual. The term "written release" is defined in the Act, and specifically includes "in the context of employment, a release executed by an employee as a condition of employment." Once collected, biometric information may not be sold, leased, or traded; and may not be disclosed or disseminated unless the individual who is the subject of the biometric information consents; the disclosure

completes a financial transaction requested or authorized by the individual; the disclosure is required by federal or state law; or the disclosure is required pursuant to a valid warrant or subpoena.

An entity that possesses biometric information must store, transmit, and protect the information from disclosure using a standard of care that is reasonable within the private entity's industry, and a method that is the same as or more protective than the manner in which the entity stores, transmits, and protects other confidential and sensitive information that is used to uniquely identify an individual, such as account numbers, PIN numbers, drivers license numbers, or social security numbers.

Entities that violate the Act may be subject to a lawsuit in Illinois state court or a supplemental claim in federal court by an individual whose biometric information was collected, stored, transmitted, disclosed, or otherwise handled in a manner inconsistent with the Act's requirements. A successful claimant can recover $1000 or actual damages (whichever is greater) for negligent violations and $5000 or actual damages (again, whichever is greater) in the case of intentional or reckless violations. In all cases, a prevailing plaintiff may recover attorneys' fees and costs as well as any other relief, including an injunction, that the court deems appropriate.

Illinois employers who currently use employee biometric information, or who are considering implementing procedures that require collecting and using biometric information, should review their policies and practices and ensure that they have an appropriate written policy in place, and that the policy is made available to the public. Furthermore, any practices that require the use of biometric information should include obtaining a proper written release.

If you have questions regarding the Illinois Biometric Information Privacy Act, you may contact Becky Kalas in our Chicago office at (312) 960-6115, bkalas@fordharrison.com, or the Ford & Harrison attorney with whom you usually work.