Chicago Daily Law Bulletin®

Volume 163, No. 197 Serving Chicago's legal community for 162 years

Biometric info: What to do and not do

By Gregory Abrams, Terran Chambers and Lindsey Hogan

Gregory Abrams practices labor and employment law with Faegre Baker Daniels LLP. He can be reached at Gregory.abrams@FaegreBD.com. Terran Chambers practices employment law with Faegre Baker Daniels LLP. She can be reached at terran.chambers@faegrebd.com. Lindsey Hogan is an attorney with Faegre Baker Daniels LLP. She can be reached at lindsey.hogan@faegrebd.com.

With the advent of such technologies as facial and voice recognition and fingerprint scanners, employers increasingly are using biometric technology to identify and authenticate employees.

Uses include employee time entry; security purposes, such as allowing access to company premises with keyless doors and restricting computer systems and devices to authorized individuals; and promoting healthy lifestyles through employee wellness programs.

However, employers' use of biometric technology has led to a slew of recent class-action litigation alleging improper collection, use and storage of such information. Here is what employers should know.

Current trends in biometric data regulation

Forty-eight states have laws imposing notification obligations to private entities — including employers — in the event of a security breach involving individuals' personal identifying information, or PII, such as names, addresses and credit card information.

In turn, many states (including Iowa, Michigan, Nebraska, Texas, Wisconsin, Connecticut and New Mexico) have defined PII to include biometric data, such as fingerprints, voice prints, iris or retina patterns and facial characteristics or hand geometry that are used to authenticate an individual's identity when the individual accesses a physical location, device, system or account.

Certain states, including Illinois, Texas and Washington, have laws governing specifically the collection, retention, storage and use of biometric data.

For example, the Illinois Biometric Information Privacy Act (740 ILCS 14, et seq.) requires any "private entity" in possession of "biometric identifiers or biometric information" to:

- Publish a written policy for retention and destruction of biometric identifiers and information.
- Dispose of biometric identifiers once the purpose for collecting it has been satisfied or within three years of the individuals last interaction with the entity, whichever occurs first.
- Provide written notice to and obtain a written release from an individual before collecting or obtaining their biometric information or identifiers.
- Treat any biometric data "in a manner that is the same as or more protective than" the manner in which the entity "stores, transmits and protects other confidential and sensitive information."

Employees can bring a private cause of action for violating these requirements to recover, on a per violation basis, $1,000 for negligent violations and $5,000 for intentional or reckless violations, or actual damages, whichever is greater, plus attorney fees and costs.

Other states are considering enacting similar laws: Alaska and New Hampshire proposed legislation this year that would similarly regulate the collection, retention, storage and use of biometric data, including enabling private rights of action.

Recent litigation

Additionally, the plaintiffs' class-action bar recently has been suing employers over biometric data. For example, in March, employees filed a class action in the Northern District of Illinois against a supermarket chain for allegedly using a timekeeping system premised on fingerprints without obtaining employees' consent or publishing a retention and destruction policy.

In June, employees brought a similar class action against a hotel chain, and in July, an employee filed suit against a communications company for allegedly using hand scans without consent and disclosure. Employers with large numbers of employees face potentially significant exposure from this type of litigation.

Potentially implicated laws

Similarly, as biometric technology use advances, employers must consider its potential intersection with the Americans with Disabilities Act, Title VII, and privacy laws.

For example, certain employees may be unwilling or unable to provide biometric data based on a disability. Certain biometric data practices also may affect employees who lack or cannot access the source of the biometric data, are without fingers or eyes, are nonverbal, cannot straighten their fingers or position their head sufficiently for scans or have genetic or congenital conditions affecting the structure of their hands and/or faces.

And biometric scans may reveal information about existing medical conditions and medical predispositions, posing a risk for disability discrimination.

Another potential complication is an employee who is unwilling to provide biometric data. One court has held that an employer violated Title VII by not allowing the plaintiff to opt out of its hand-scanning attendance policy based on a sincerely held religious belief.

Finally, certain biometric tracking practices may present privacy concerns. Requiring employees to access biometric data each time they enter a room could be used to confirm how long an employee was in a restroom, in a break room, at a union meeting or complaining to human resources.

Lessons for employers

As employers continue to embrace biometric technology, they should consider certain practices to reduce litigation risk, including:

- Review applicable state laws on biometric data as well as laws governing employer obligations in the event of a security breach.
- Consider notifying employees, in writing, of the company's intent to use biometric systems and obtain employee consent.
- Address potential security policies and procedures governing how biometric data will be stored and safeguarded and when and how it will be discarded.
- Develop potential alternatives to data collection, where feasible, for employees who request a reasonable accommodation.
- If applicable, give the union or unions, if a collective bargaining agreement is in effect, sufficient notice before using biometric data and review the labor contract for potential limitations.