JONES DAY

COMMENTARY

NOVEMBER 2017

Biometric Data in the Workplace Could Trigger Privacy Litigation Wave

IN SHORT

The Situation: While biometric data (such as fingerprints, facial recognition technology, and iris scans) can be used effectively in the workplace, privacy advocates worry that anonymity could be undermined, and plaintiffs' lawyers are challenging the collection, use, and disclosure of biometrics.

The Result: Some companies are self-regulating their use of biometrics, and a number of states have enacted statutes regulating the use of this data.

Looking Ahead: In the absence of a a national biometrics regulatory regime, companies will have to adapt to the growing body of state-level statutes and case law.

Biometric data can be thought of as innate, unique, and immutable information about a person. The data, referred to as "biometric identifiers" in state statutes, includes unique attributes like a fingerprint, voiceprint, retina or iris scan, or scan of face geometry. Some recent court decisions have found that face geometry includes facial recognition technology used to sort photos and identify individuals within them.

Companies can use biometric data to control access to specific areas of a workplace, computer systems, or data. Biometric data can also simplify and protect the integrity of employee recordkeeping functions, such as when the employees arrive to and leave work. However, some privacy advocates worry that biometric data could be used to undermine anonymity or exploit consumers for commercial gain.

The Current Regulatory Environment

Although some companies have self-regulated their actions in the biometrics area, multiple states have passed laws regulating various aspects related to biometric data. The State of Washington recently became the third state to enact a statute regulating biometrics, joining Illinois and Texas. Several other states have considered or are considering statutes to regulate various aspects of biometrics.

In general terms, the existing state statutes impose conditions on collecting, disclosing, securing, and using biometric data; contain consent provisions; and provide for a private right of action (Illinois) or enforcement by state attorneys general (Texas and Washington). The Illinois statute provides that plaintiffs can collect $1,000 per negligent violation or $5,000 for each intentional or reckless violation. These statutory damages, along with an attorney fee provision, provide powerful incentives for plaintiffs' lawyers to file class action lawsuits. In addition, other more general state privacy laws may define "personal information" to include aspects related to biometric data, which could provide a basis for future developments in the case law even in states without statutes specifically targeting biometric data.

> Companies using or considering using biometric data should ensure that their use, retention, and disposal complies with the growing body of regulatory requirements and case law.

While there is no overarching federal regulatory regime, the Federal Trade Commission has issued a report, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, which outlines certain privacy issues related to the use of facial recognition technology. Other federal agencies may have an interest in the regulation of biometric data from security and privacy standpoints relating to biometric signatures used in clinical investigations of medical products (Food and Drug Administration), medical information (Department of Health and Human Services), and facial recognition technology (Department of Commerce National Telecommunications and Information Administration).

Litigating Biometrics

Companies using or considering using biometric data should ensure that their use, retention, and disposal complies with the growing body of regulatory requirements and case law.

To date, the most significant litigation has been brought under the Illinois statute, which is not surprising given the relief available to successful plaintiffs. Some of the cases have included franchised operations, no doubt because of the "deep pockets" of the franchisors. As such, franchisors in Illinois and elsewhere should analyze the tradeoffs between involvement in franchisees' biometrics operations and the desire to avoid potential liability under the newest theories of the plaintiffs' bar.

In addition, companies with operations outside the United States should consult and follow laws of foreign

jurisdictions, several of which regulate aspects of biometric data.

Whether Congress will at some point step in to replace a patchwork of state laws with a comprehensive federal scheme remains to be seen, although Congress has chosen not to do so in related areas such as data breach notification requirements.

THREE KEY TAKEAWAYS

1. The use and regulation of biometric data will likely grow in the coming years. Companies using or considering using biometrics should ensure compliance with the growing body of regulatory requirements and case law.
2. Franchisors should evaluate the potential tradeoffs between involvement in franchisees' biometrics operations and the desire to avoid potential liability under the plaintiffs' bar's newest theories.
3. A company that has operations outside the United States should also consult and follow laws of foreign jurisdictions relating to the use of biometric data.

CONTACTS


J. Todd Kennard
Columbus


Brandy H. Ranjan
Columbus


Jackson D. Lavelle
Columbus

YOU MIGHT BE INTERESTED IN: Go To All Recommendations >>


California Issues New Autonomous Vehicle Regulations


New Ibero-American Standards to Provide Consistency in the Protection of Personal Data


Protecting Your Identity After a Data Breach

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a legal institution with more than 2,500 lawyers on five continents. We are One Firm Worldwide℠.