RBJ RBJ.NET ROCHESTER BUSINESS JOURNAL
Part of the BridgeTower Media network FEBRUARY 15, 2021

Biometrics in the workplace: Privacy challenges and a roadmap for successful compliance

Biometric information is all around us. It enables us to tag friends and family in photos on social media, unlock our phones, pay for groceries and track our workouts. The technology is already beginning to take hold in the workplace as well, as more employers wish to capitalize on quick and reliable employee identification, security and productivity tracking. This article examines the most common biometric applications in the workplace, as well as some of the major privacy risks, and provides guidance for successful compliance with the various authorities that govern the use of this technology.

What is biometric information and how is it collected?

Biometrics are unique physical characteristics used to identify a specific individual. Definitions provided by state privacy laws vary somewhat, but the two most broadly used are "biometric identifier" and "biometric information." "Biometric identifier" refers to records of biological characteristics used to identify an individual. "Biometric information" is a more flexible, catchall term and could refer to information based on an individual's biometric identifier and information used to create an identifier. Examples of biometric data include imagery of the iris, finger or face; fingerprints, facial scans and voiceprints; and some less obvious records such as keystrokes, gait patterns and sleep data. Biometric technology is widely used in the workplace. A 2018 Spiceworks survey found that 62% of companies polled in North America and Europe already use biometric verification in the workplace. An additional 24% of companies planned to use biometric verification in the workplace by 2020. While smartphone verification may be one of the more common manifestations of the technology, biometrics are used in other contexts as well. Employers may collect and use biometrics to power facial recognition video surveillance; permit access to buildings, machinery and IT systems; and track employee productivity and timekeeping.

Aside from use in everyday workplace settings, biometrics are often collected through employee participation in corporate wellness programs. A 2019 Kaiser Family Foundation survey found that 84% of large U.S. companies (200+ employees) and 50% of smaller U.S. companies offered a wellness program to their employees. Through these programs, employers may collect biometrics via employer-supplied fitness trackers, comprehensive health questionnaires or health screenings to measure blood pressure, blood sugar, BMI and more.

While there are many reasons to leverage biometrics in the workplace, including enhanced security and streamlined verification, this technology also presents risks and regulatory compliance challenges. For instance, employers that decide to collect biometrics should consider numerous state, federal and international laws, many of which have extraterritorial effect, and determine what, if any, obligations they impose on the collection, use, dissemination and deletion of biometric data. Although employment law issues are outside the scope of this discussion, it is important to note that New York Labor Law prohibits fingerprinting as a "condition of securing or of continuing employment" (this has implications for, among other things, how employers enforce the use of biometric timekeeping systems). The use of biometrics further presents a variety of privacy risks, including: identity theft and fraud; surveillance and location tracking; and inadvertent or malicious disclosure of sensitive personal information. Finally, employers that decide to collect employee biometrics, especially in the context of wellness programs, must learn how to guard against employment discrimination based on sensitive health and lifestyle-related insights.

Navigating privacy laws that govern the use of biometrics

The General Data Protection Regulation (GDPR), the European Economic Area's comprehensive data privacy law, adopts a broad definition of biometric information and classifies such information as "sensitive data." Article 9 of the GDPR requires extra safeguards, including obtaining explicit consent, when processing sensitive data. In addition to the GDPR's general obligations regarding consent, notice, minimization and deletion, businesses processing biometric information must also conduct a privacy impact assessment prior to doing so.

Although the United States does not currently have an all-encompassing GDPR counterpart at the federal level, the Americans with Disabilities Act (ADA), Health Insurance Portability and Accountability Act (HIPAA) and Genetic Information Privacy Act (GINA) all govern the use of biometrics in certain situations. The ADA requires employers to keep employee medical information private and maintained as a "confidential medical record" separate from an employee's other files. Further, the ADA may prohibit employers from releasing biometrics and other health information to third parties. HIPAA, which includes biometric information in its definition of "personally identifiable information," applies directly to employer-sponsored health plans and wellness programs operating under employer health plans. Biometrics collected within these contexts are subject to HIPAA's Privacy Rule, as well as the technical, administrative and physical safeguards mandated by its Security Rule. Finally, GINA prevents employers from using genetic information in making employment decisions and from requesting, purchasing or disclosing genetic information.


Anna Mercado Clark


Mario Fadi Ayoub

Federal laws aside, employers must remain cognizant of obligations imposed by state privacy laws. New York State-based businesses should pay special attention to New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), as well as the New York State Department of Financial Services' Cybersecurity Regulation ("DFS Regulation"), the latter applying to a narrow subset of persons operating under the authorization of New York's banking, insurance or financial services laws ("Covered Entities"). The SHIELD Act mandates reasonable administrative, technical and physical safeguards for the storage, use and disclosure of consumer data, including biometrics. The SHIELD Act also requires written agreements between third parties and Covered Entities. The DFS Regulation requirements include the creation of a cybersecurity program, contracts with third-party service providers to ensure the security of nonpublic information, and periodic and secure disposal of biometric information and other data no longer necessary for business operations.

New York State businesses should also look to other state laws governing biometrics, specifically Illinois' Biometric Information Privacy Act (BIPA) and the California Consumer Privacy Act (CCPA). Both acts have extraterritorial reach. BIPA applies to any business operating in Illinois or any business that collects data from Illinois consumers. The CCPA applies to any entity that does business in California, providing it meets set thresholds for annual revenue, revenue generated from data sales or amount of data processed. Both acts establish specific obligations that Covered Entities must meet when collecting, disclosing, storing or deleting biometric data. BIPA categorically prohibits the sale of biometric data, and the CCPA specifically requires "reasonable safeguards" for the storage and protection of data.

Recommendations for using biometrics in the workplace

Despite the privacy risks and compliance considerations, biometrics do offer a streamlined method of security and authentication that has been widely adopted by employers around the world. Employers looking to join the trend and implement biometric technology in 2021 should keep four overarching considerations in mind:

1. Establish clear internal policies that streamline compliance.
2. Develop a third-party risk management program that establishes contractual requirements for third-party partners and service providers.
3. Explore alternatives to biometric verification and identification where the privacy risks may outweigh the benefits.
4. Examine employment law practice considerations, including employment discrimination concerns.

Anna Mercado Clark, CIPP/E, CIPP/US is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at aclark@phillipslytle.com or (585) 238-2000 ext. 6466.

Mario Fadi Ayoub is a member of Phillips Lytle LLP's Data Security & Privacy Practice Team. He can be reached at mayoub@phillipslytle.com or (716) 847-8319.