Biometric Monitoring is Booming in The Workplace, Raising Ethical and Legal Questions For HR

HR Brew | Sam Blum | March 4, 2022

Getty Images

Workers have few legal protections when it comes to biometric data collection, but there are some notable exceptions.

Here's a question courtesy of the rapid advancement of 21st-century technology: What do factory workers at Apple production plants in China, middle managers in the US participating in corporate wellness programs, and warehouse workers potentially have in common? Sure, they're all working for pay, but they could reportedly be providing their employers with troves of data related to their personal health, in addition to other sensitive information, such as scans of their fingerprints.

According to market research firm the IMARC group, the global biometrics market reached a $27.97 billion valuation in 2021, and is expected to reach nearly $75 billion by 2027.

Central to that gargantuan monetary figure are the eyeballs, heartbeats, and physical movements of people across the world, and—increasingly—employees who are clocking into work with their fingerprints or opening company devices with scans of their faces. The World Bank defines biometric data as "automatic recognition of individuals based on their biological or behavioral characteristics."

Liz Brown, an associate professor of law and taxation at Bentley University, told HR Brew that she believes the increasing reliance on these tools in the workplace could be a cause of concern for employees "because companies' use of this data is not transparent."

Biometric monitoring in the workplace "started with manufacturing and warehouse workers, but the range of biometric monitoring is expanding to cover all kinds of workers," Brown said. "It's a way of gathering information about workers who largely don't have well-recognized privacy rights."

Compared with US consumers—who still have fewer legal protections against a variety of data collection practices compared to citizens of the European Union—workers have even fewer rights when collection of biometric data slides into misuse, said Brown. "To the extent that people have privacy rights, [it's] usually as consumers, not as employees," she explained.

When biometrics break bad. Michel Roig, president, head of payment and access at the Swedish biometrics firm Fingerprint Cards, recently explained to the Society for Human Resources Management why companies covet biometrics: "Biometric technology only gives access to authorized users, is difficult to steal and spoof, and does not allow scalable attacks, reducing the risk of hacks and breaches through stolen credentials."

Companies also rely on biometric data to mitigate the threat of "time theft," which "occurs when an employee is paid for work they have not actually done, or for time they were not actually at work," according to the payroll system provider EPAY Systems. The payroll and attendance management platform Kronos markets its biometrically enabled timeclock system as a way to keep this specific phenomenon from happening, writing in promotional materials, "Without biometric technology in place, employees can clock in for one another, or buddy punch."

Many of Kronos's clocks, which are used in hospitals, city government offices, supermarkets, and more, scan employee fingerprints to allow them to clock in to their shifts. A class-action lawsuit filed in an Illinois federal court in 2019 alleges that Kronos breached the Illinois Biometric Information Privacy Act (BIPA) by failing to get employees' permission to scan their fingerprints, or providing information on the use of those scans, at a Chicago-area supermarket and packaging facility, the Cook County record reported last year. Kronos didn't return an HR Brew email request for comment.

Mark P. Carey, an employment attorney based in Connecticut, said that when it comes to fingerprint-scanning processes, employers often are "not telling [workers] what they're going to do with their data. They don't get their consent, and they don't give any policy."

Biometrics encompass more than just clocking into a shift, however. One of the seemingly less-assuming ways a company might collect employee data is through a corporate wellness program or fitness challenge, Brown said. When workers use wearables like smartwatches owned by employers, companies can market the wellness strategy to "incentivize people to be healthy," but the data might be collected "because the employer thinks more physically active employees [will] be less expensive to provide health insurance," Brown said. According to the Kaiser Family Foundation's 2021 Employer Health Benefits Survey, out of the total number of companies offering health benefits, 26% of smaller companies with 50–199 employees and 38% of larger firms "provide workers the opportunity to complete a biometric screening."

Lack of a legal landscape. Both Carey and Brown explained that legal protections around the use of biometric data are thin for most workers in the US. One exception is Illinois's Biometric Information Privacy Act (BIPA), passed in 2008, which requires employers to inform employees in writing of the biometric data being collected and its intended use and to then obtain written consent from workers; it also, forbids employers from selling or otherwise profiting from the information, and allows workers to take a company that violates the law to court.

The law has enabled many workers in the state to seek legal damages against employers over alleged privacy violations. In 2019, there were 28 complaints filed in federal court over BIPA violations, but that number grew to 80 in 2020, Bloomberg Law reported last year. Other states, such as Texas and Washington, have laws that are similar to BIPA in that they prohibit data collection without prior consent or notice but "neither include a private right of action and both authorize their respective state attorney general to enforce the law," according to the National Law Review. BIPA, on the other hand, "includes a private right of action" over violations.

Brown called the legal landscape "fragmented" regarding privacy rights. The National Biometric Privacy Act was introduced to the Senate in 2020 and referred to the Committee on the Judiciary; the bill would bring "broader protection, subjecting companies in all trades and industries to strict biometric data compliance" at the federal level and not just state jurisdictions, according to JD Supra.

Still, Brown is concerned about the current makeup of biometric privacy in the workplace. She said, "I think most people overestimate the amount of privacy protection that the law actually provides to them."