Forget Passwords and Badges: Your Body Is Your Next Security Key

Biometric scanning and AI advances mean security systems could use traits from your gait to your gaze to unlock your company's building and systems

By Danny Lewis

4 min. read · View original

The technology could do away with the hassle of forgotten badges and regular password resets, and fortify companies' protection against cyberattacks. But it also raises concerns about ways the data could be used beyond security—and whether employers should have this level of insight into their workers' bodies and behavior at all.

Today some doctors offices use palm scanners to check in patients, while a face or fingerprint unlocks a smartphone. Facial recognition has become more common in airports, stadiums and concert venues. In coming years, security-industry executives say, advances in artificial intelligence and sensor technology could help

organizations use multiple pieces of biometric data at once—like the pieces of a puzzle that make up an employee.

Eye scans featured heavily in the 2002 sci-fi film “Minority Report,” which Lazzouni calls one of his favorites. In the movie, Tom Cruise’s character accesses his highly secure workplace with the technology, which later comes back to haunt him. Despite the movie’s dystopian slant, Lazzouni says he finds it exciting: “All you need to do is to just look into the reflection of that device that you are looking at, and it could read your iris and automatically give you all of the access that you need for whatever you need to interact with.”

Aside from convenience, security experts say biometrics offer stronger protection for buildings and data than a keycard or a password can. “It’s easy to copy an employee’s password, but it’s really hard to copy an employee’s face that’s actually moving,” says Rhon Daguro, the chief executive of

, which makes identity-verification and digital-security systems.

Future office-security systems could simply lock out people who aren’t recognized or cleared, Daguro says. “We have a log of your face, so we have exactly who’s walking in and out of the building, which you can’t do with a password,” he says.

itself uses no passwords at its workplace, Daguro says. “We open up the laptop, the camera turns on, we put our face in the window, and all of a sudden we’re logged in.” The policy reflects the company’s commitment to and trust in the technology it is developing, Daguro says. It also means that biometric scans are a requirement for those who work at authID. Employees consent to the policy when they join, Daguro said in an email. And any biometric data gathered by the company—whether for authID’s clients or its employees—is anonymized and encrypted, he says.

Biometric scans are an important deterrent as attempts to hack corporate systems have become more frequent and sophisticated, says Andrew Shikiar, an executive director of the FIDO Alliance—for Fast Identity Online—an industry association that develops digital-security standards. Tech giants such as Google,

,

and

are among members of the group, whose aim is to reduce reliance on passwords. Instead, they are pushing for the use of passkeys, in which a piece of encrypted code on a physical device, such as a phone or laptop, is unlocked with the user’s biometrics.

“Face images, liveness detection, iris scans, vein scans, heart rate, everyone has a unique pulse or some biorhythms that uniquely mark you as you, and can be used for sign-in purposes,” Shikiar says.

As secure as it may be, biometric technology also means using your most personal and permanent data, bringing privacy risks. “When it comes to biometrics, we want to make sure that people know what’s being collected, they know what purposes it’s being used for, and they can ask for it to stop if they become uncomfortable with it, ” says Hayley Tsukayama, associate director of legal activism at the Electronic Frontier Foundation, a nonprofit organization that advocates for civil liberties in the digital world.

Even the best technology makes mistakes, Tsukayama says. If the software confuses someone’s identity, it will be important that workers have the right to appeal. The stakes are particularly high with biometric data, she says. “No one can issue me new fingerprints. No one can issue me a new face. And so if that information is hacked, for example, and in a format where other people can use it, that’s the whole game.”

A combination of encryption and government regulation on how biometric information is collected, used and stored is needed to lay the

groundwork for the biometric-security industry, both Lazzouni and Daguro say.

Nevertheless, consumer technology has a way of easing people's concerns about sharing personal information, much as smartphones have helped normalize facial recognition, security-industry executives say. They see a future where security will go beyond the iris scans of "Minority Report" to a chip placed inside the body.

The advent of chips that monitor health could eventually pave the way for using those same biometrics to pass through security systems, Daguro says. "Nobody will put a chip in your body just for identity, but they'll put your chip in your body for knowledge or for health or to help live a better lifestyle. And then the convenience will be a fast follow."

Write to Danny Lewis at daniel.lewis@wsj.com

Instead of posing for a photo and setting up passwords, in the future a new employee might spend a few minutes supplying biometric information. Face scanned, gait analyzed, spoken phrase recorded and *voilà*: Your body becomes your security key.
Biometrics experts envision a seamless experience. "As soon as you arrive at the parking lot, your geolocation is fed into a system from the phone that has been given to you. As soon as you come through the front door, facial recognition could open the door and could also unlock your computer," says Mohamed Lazzouni, the chief technology officer at