BIOMETRICS ARE COMING, ALONG WITH SERIOUS SECURITY CONCERNS

YOU'RE BUYING A pair of jeans. At the register, instead of reaching for your wallet or phone, you pull back your hair. The cashier holds a camera up to your ear. The camera confirms a match to a photo in a database, all of which is linked to your bank. Transaction complete.

This futuristic scenario is actually not so far-fetched, and it's coming sooner than you might think. Research on biometric tech has amped up, leading to mobile apps that read various unique-to-you body parts to help verify your identity, raising all kinds of security and privacy concerns, and it's still an open question as to how government and manufacturers are going to address it all.

But back to that ear scan. "Ears are unique," says Michael Boczek, the President and CEO of Descartes Biometrics, a company that specializes in mobile ear detection security apps. "It's stable and enduring, which means it changes very little over the course of one's life. That's also true of fingerprints, but less true of facial recognition."

Just because someone might be able to use their ear at checkout doesn't mean it's necessarily going to happen anytime soon, though. "Biometrics are tricky," Woodrow Hartzog, an Associate Professor of Law at Samford University told WIRED. "They can be great because they are really secure. It's hard to fake someone's ear, eye, gait, or other things that make an individual uniquely identifiable. But if a biometric is compromised, you're done. You can't get another ear."

Databases get hacked all the time, from the IRS to Target to hospitals and banks, and until some of the very real security concerns surrounding the use of biometric technologies are better ironed out, you wouldn't be wrong to worry about linking data about your body parts to online accounts.

Biometrics? Back Up

Biometric identification refers to any technology that does one of two things: identifies you or authenticates your identity. For identification, an image is run against a database of images. For authentication, an image has to be accessed from the device to confirm a match. The latter is typically used for unlocking computers, phones, and applications.

Since Apple introduced its incredibly usable biometric identification with Apple's home button fingerprint sensor in 2013, the appetite for biometrics has expanded rapidly. Now MasterCard wants to use your heartbeat data to verify purchases. Google's new Abicus Projectplans to monitor your speech patterns, as well as how you walk and type, to confirm that it's really you on the other end of the smartphone. Other apps are looking at the uniqueness of vascular patterns in the eyes or even a person's specific gait to verify identities.

The idea isn't actually new. Police have been fingerprinting for over 100 years and have used digital biometric databases since the 1980s. But until the 2013 iPhone, consumer-level biometric verification was largely limited to unlocking devices with fingerprints. And those sensors were in awkward places, like on the back of a phone or next to the trackpad on laptops.

Mobile biometrics have also piqued the interest of investors. Reports surfaced that the Swedish biometrics company responsible for fingerprint identification in most Android devices, Fingerprint Card AB, saw a 1,600 percent increase in its stock in just the last year alone, making the company one of the best performing stocks in Europe in 2015.

Securing the Public

Although many experts say biometrics are intrinsically secure (since no one else can have your ears or eyes), Alvaro Bedoya, Professor of Law at Georgetown University, argues otherwise. "A password is inherently private. The whole point of a password is that you don't tell anyone about it. A credit card is inherently private in the sense that you only have one credit card."

Biometrics, on the other hand, are inherently public, he argues. "I do know what your ear looks like, if I meet you, and I can take a high resolution photo of it from afar," says Bedoya. "I know what your fingerprint looks like if we have a drink and you leave your fingerprints on the pint glass." And that makes them easy to hack. Or track.

Law enforcement agencies are particularly aware of how public your body parts actually are. A technology like that ear-scan, which can be used to make shopping easier in one scenario, can be used by the police in another. The FBI has been building a biometric recognition database that it hoped to have filled with 52 million facial images by 2015, with thousands more images added every month. The Department of Homeland Security is working with U.S. Customs and

Border Patrol to add iris scans and 170 million foreigner fingerprints to the FBI's national database. And local police departments are also in on the biometrics game. The *LA Times *reported that the police department in Los Angeles invested millions of dollars in 2015 to expand biometric identification capabilities for officers in the field, and according to research from the Electronic Frontier Foundation, numerous other police departments have mobile fingerprint identification already deployed.

Even Boczek says that police are interested in his ear verification software. He explained that it would allow a police officer with a body-mounted camera that sits mid-chest to capture images of someone's ear to scan when they approach a driver's window. In fact, he says this technology is currently being tested by police departments in Washington state.

Writing the Rules

The use of data about your body parts is largely unregulated.

Last summer, the National Telecommunications and Information Administration held a workshopto craft a voluntary code of conduct for the operation of facial recognition technology. Trade associations were there, representing companies like Google and Microsoft, as well as advocates and experts. But they didn't get far. Before the meeting was over, everyone from the public interest community walked out.

"Not a single trade association would agree that before you use facial recognition to identify someone by name, even if you don't have any relationship with that person, you need to get their consent," said Bedoya. "The industry associations in the room were taking a position that was well beyond standard practices."

The US government is dancing around the question of consent and how to oversee biometrics, with what seems like almost every agency in Washington addressing part of the issue. The National Institute of Standards and Technology has been evaluating the efficacy of biometric identification for years, focusing on face identification, fingerprint, voice, and iris scans. The Federal Trade Commission is leading the charge on data security. The FDA deals with the security of implantable devices, and the Department of Health and Human Services handles personal health information.

For now, it's legal in 48 states for software to identify you using images taken without your consent while you were in public. Texas and Illinois don't allow it for commercial use, but it's legal nationwide for law enforcement. And even

when consent is obtained, it's often done so in a way you may not be aware of: in the fine print of Terms of Service agreements that people routinely don't read.

"The law is written in such a way that that these agreements are routinely considered valid and that they are the way for companies to get permission to collect, use, and share your personal information," says Hartzog.

But companies have been self-regulating for sometime now. Google Executive Chairman Eric Schmidt, as Bedoya notes in an article he wrote for Slate, even once said that facial recognition was "the only technology Google has built and, after looking at it, we decided to stop." Microsoft's Xbox and Apple's iPhoto both have limited uses of the software on an opt-in only basis. We reached out to Apple and Google about this, but neither had comment. Microsoft responded that it keeps facial recognition opt-in because the company believes "it's important to be able to personalize and control your Xbox experience."

And then there's Facebook. With over 350 million photos uploaded every day, the company's research lab suggests that it has "the largest facial dataset to date"—powered by DeepFace, Facebook's deep learning facial recognition system, but Facebook has an agreement with the FTC that says it first has to first obtain "affirmative express consent" before going beyond a user's specified privacy settings.

Bedoya says, using such a system, it's not hard to imagine a future where someone walks into a car dealership, and immediately the dealership knows who they are, where they live, their income, their credit score—all thanks to Facebook. After all, there's already facial recognition software that brick-and-mortar shops can use to identify "return shoppers" and signal when "pre-identified shoplifters" enter the store.

Creepy, Public, and Unsafe?

Just as you can buy software to brute force your way through pins and passwords, hackers are already engineering ways to spoof biometric authentication. One of the big reasons we're not all using our bodies to verify purchases now is that the security isn't there yet.

When the Office of Personnel Management was hacked last year, 5.6 million people's fingerprints were compromised. Universities are hacked every year, medical records, the IRS, banks, dating websites, the list goes on. Biometric data isn't immune to these attacks. In fact researchers from mobile security firm Vkansee were able to break into Apple's Touch ID system with a small piece of

Play Doh just last month at the Mobile World Congress—similar to what security researcher Tsutomu Matsumoto a did with a gummy bear over a decade earlier with another fingerprint sensor. And researchers at Michigan State University just last month released a paperthat describes a method for spoofing a fingerprint reader using conductive ink printed with an ink jet printer in less than fifteen minutes.

Beyond the security question, there's also something just plain creepy about the technology. Case in point: MasterCard has partneredwith the biometrics company Nymi to test heartbeat authentication for credit card purchases. (That would be in addition to its selfie-and-fingerprint payment verification app it rolled out at Mobile World Congress). Or EyeVerify, which works by scanning the blood vessel patterns in the whites of your eye by using a selfie taken with a smartphone. Other mobile phone companies have built devices that use infrared cameras to scan irises.

"There's a question as to how viscerally people will respond to biometrics. The fingerprint reader seems to have caught on pretty well, because it was really useful and easy," says Hartzog. "When people feel creeped out they may be less gung-ho to adopt some kind of biometric."

And if you can get past the ick factor, then there's also the privacy question. Are you willing to use your unique bodily identifiers to link you to a purchase history? Think about how often you purchase items you'd rather keep private: porn, alcohol, drugs, condoms, a hoverboard.

"We enjoy shopping in relative obscurity," says Hartzog. "This is something that we might be able to accept for some purchases, but for it to be standard practice in America strikes me as a long way off." If you knew the political thinking of everyone you bought things from, you'd probably be slightly disturbed. As University of Washington law professor Ryan Calo expressed in a recent paper, a certain level of privacy allows us to do business with each other; it's part of interacting in a marketplace.

"We're probably not ready to hand over the keys to the entire biometric kingdom when we're not sure how this is going to work," Hartzog added. Eventually, we may be willing to exchange privacy for the convenience—but not just yet.