Is Biometric Technology Worth the Security Risk?

Should we continue to develop more advanced biometric technologies, or should we stop and simply use older methods of security, such as passwords?

Background

Introduction

In recent years, the development of biometric technology in our everyday lives has grown tremendously. Biometric verification analyzes physical characteristics that are unique to each individual as a means of authentication. A popular example of biometric technology is Touch ID found on Apple iPhones and iPads. Touch ID has the ability to unlock a user's phone with just a scan of their fingerprints. Additionally, Touch ID is an integral part of Apple Pay, which allows users to pay

with their phones instead of carrying around payment cards. To purchase an item, users simply hold their device up to a wireless payment terminal while holding their finger on TouchID. Using their fingerprint to verify the use of the payment card, transactions are completed in an instant without ever pulling out their wallets. As society becomes more reliant on biometrics as a means of authentication, the demand for protection against theft has been subject to debate.

What Are Biometrics?

With technology progressing at an exponential rate, biometric technology has become more prevalent in our lives. Biometrics utilizes body parts that show minimal change over time; common biometric identifiers include fingerprint scans, retinal scans, and voice recognition. For example, a fingerprint scanner takes a multitude of images of a fingerprint, mapping out ridges and curves. The map is then converted into code that is stored on the device or cloud database for future verification. Biometric information is stored as data, similarly to passwords, but instead of letters and numbers, patterns and characteristics are saved as a series of numbers. Essentially, an encrypted image or sound acts as a password. Biometrics has become very popular because of how easy and secure it makes accessing high security items, such as bank accounts. With advances in biometric security features, we may soon be paying for our groceries using our earlobes.

The Debate

Biometric security has been regarded as the most secure identification measure due to its life-long sustainability and uniqueness to a person. In other words, biometric identifiers are nearly impossible to fraud, and are therefore more secure compared to the traditional password method that is designed using attackable software. In a New York Times article titled "From Man to Machine", it is calculated that the chances of two people having identical irises is about 1 in 10^78, which drastically reduces the probability of yielding false identification. In addition to accountability, biometric security is often favored because of its convenience and efficiency. Imagine you're standing in line for Christmas shopping, wouldn't it be much faster if everyone can make transactions only by pressing their thumbs on a small device?

While the use of biometric authentication would revolutionize everyday life with added efficiency and convenience, it would be accompanied by an increased privacy risk. According to a recent article in *Wired*, while passwords and traditional security measures are private by nature, "biometrics… are inherently public." Our bodies are on display all the time; body parts used for biometric identification, such as fingers and eyes, can be accessed easily in comparison to protected passwords and security badges. The Biometric News Portal also points out that once "a set of biometric data be compromised, it is compromised forever." The possibility of government misuse of this technology is another downside to the widespread use of biometric security. The FBI's biometric database, which includes criminal and noncriminal photos and fingerprints, has been criticized for its infringement of privacy according to a 2014 article from Fast Company. Overall, the threat biometrics poses to personal privacy may outweigh the convenience it brings.

What do you think should be done with biometric technology? Should we continue to expand on it, or should we stop and simply use older methods of security, such as passwords?

California Academy of Science. *Do Now*. https://ww2.kqed.org/learning/2016/11/18/is-biometric-technology-worth-the-security-risk/

Article 1

Biometrics Are Coming, Along With Serious Security Concerns

By April Glaser 03.09.16. 03.09.16

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 Project plans 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 workshop to 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 paper that 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 partnered with 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.

Wired Magazine. https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/

Article 2

Someday Soon, You May Pay Your Restaurant Bill With A Retina Scan

by Jared Linzon | January 6, 2015 — 6:40 AM

The past 30 years have seen payments shift from cash and checks to debit cards and websites, and most recently to mobile phone apps, including Apple Pay and Venmo. But in a few years, you may not need anything you weren't born with.

Some mobile technology and financial companies are hoping a quick imprint of your finger, scan of your eye or tap of an armband that links to your heartbeat will be easier and safer than using plastic.

Once used for doing high-level security clearances and criminal record checks, unique biometric identifiers — including fingerprints and iris patterns — are just starting to make inroads as payment.

Already, companies like Apple and Samsung have implemented fingerprint-scanning features in their latest smartphones. Their goal? To replace your need for schlepping around a credit card (in favor of a phone number) and remembering a PIN (swapped for your fingerprint).

Meanwhile, banks in the United Kingdom, Poland and elsewhere are set to release credit cards, online banking features and even ATMs where customers can approve payments or withdraw cash by scanning their finger and having their vein network read as a form of ID. In some cases, companies have recently started rolling out this technology.

Interest in this area has been driven, in part, by what seems to be a never-ending series of warnings about the problems with traditional credit cards and passwords. In the past year alone, more than 40 million credit card numbers have been stolen from Target and another 56 million from Home Depot. These breaches, combined with those involving millions of stolen passwords, have raised serious concerns at the helm of what financial analysts say is an imminent switch to biometric payments.

But are biometric payments any safer?

"The problem with fingerprints is that you can never change it, and you don't know how it will be used in the future, so that limits your willingness to try new things that are driven by that thumbprint once it's been stolen," says Blane Warrene, an independent financial services technology analyst. "There's a lot of Pandora's box in this that has to be thought through."

Such privacy issues are part of the reason the technology has taken off in emerging markets like Turkey and Russia rather than the West, *The Guardian* notes.

Companies in this sector say they're trying to address security concerns while also making this new kind of payment technology easy to use.

"If biometrics are done right, we can get both," says Jamie Cowper, the senior director of business development and marketing for Nok Nok Labs, a Silicon Valley-based authentication company that has partnered with Samsung and PayPal.

That's why some industry players are keeping away from creating large, centralized banks of biometric information that would save your data. "If you build a big database of passwords or account numbers, you will get hacked," says Cowper.

Indeed, decentralized data will likely be the name of the game going forward for biometric payment companies. Nymi, for example, has partnered with MasterCard and one of Canada's largest banks to test its heartbeat-monitoring armband, which, when brought toward a payment terminal, could authorize a purchase.

Known as the Nymi Band, the $79 device is currently only available for preorder and features multiple layers of security that don't rely on storing the unique electrical activity patterns of someone's heart. CEO Karl Martin says the device uses biometric information to confirm a person's identity, then encrypts the information with a key that can be read only by a payment terminal or another device that it's communicating with.

Some companies see opportunity in potential skittishness about buying with your fingerprint: Deetectee Microsystems, another Canadian venture, aims to have people submit an application form (the length of which has yet to be determined) to confirm their identity, after which they would get a wearable device that would pair with their smartphone or computer. The device then could be identified by payment terminals up to 30 feet away, which would display your photo as a secondary form of ID.

The difference here, says Deetectee co-founder Brian Purdy, is that unlike iris scanners and facial recognition software that can identify anyone from a distance, users would be able to pick and choose who and what is allowed to identify them.

Article 3

Why biometrics are the key to driver authentication in connected cars

Dr. Salil Prabhakar, Delta ID Inc. February 7, 2017 4:10 PM

Until recently, biometric technology was not a part of our daily lives, but was relegated to sci-fi flicks — too futuristic-seeming to comprehend being used in our lifetime beyond specialized applications in law enforcement, government, defense, and enterprises. While it's not new, the technology only reached widespread adoption in the past 10 to 12 years, with multiple innovations targeting the mobile platform. Mobile phones brought to the forefront one of the biggest pain points in technology: remembering, forgetting, and recalling passwords. Biometrics provides a password the user never has to remember and is always available when needed.

In 2013, Apple introduced fingerprint recognition in the iPhone to make unlocking as simple as touching the front button. This opened the floodgates for biometrics, with the rest of the industry introducing the same on their own flagship smartphones. In 2015, Fujitsu/NTT DOCOMO introduced iris recognition in their smartphones in Japan, as an alternative to fingerprints, to allow a user to unlock the phone with just a look. Other companies, including Microsoft, HP, and Samsung, also added iris recognition to smartphones, and many other vendors have products in the pipeline.

And now, as in many other mobile experiences, biometrics is coming to a connected car near you.

In the connected car, different biometric technologies work better than others for various applications. Fingerprint recognition is naturally suited for cases in which the user touches some part of the vehicle: opening the door, starting the ignition, etc. Iris recognition is more appropriate in situations where a touchless interaction is more desirable.

Biometric driver authentication

The primary use case for biometric technology in cars is driver identification and authentication, which opens up new possibilities for interesting applications beyond vehicle security. With an increase in popularity of ride-sharing services, biometric technologies provide a way to authenticate the various users sharing the vehicle. The same is applicable in the case of fleets, where only authorized drivers should be driving a fleet vehicle.

Also, Uber and other similar services have to guard the safety of their passengers. A key aspect is guaranteeing that the registered and verified driver is the person driving the vehicle. Iris recognition integrated in rear-view mirrors provides a way to ensure only an authorized driver is indeed driving the vehicle at all times.

In addition to transportation services, payment services are also starting to use iris authentication. Mobile payment systems such as Apple Pay, Samsung Pay, and Google Wallet are already linked with credit cards, and mobile phones are being used in place of credit cards at payment terminals. An automobile can work in the same way. Once the car is connected to a payment system, biometric technologies can execute cashless payments at gas stations, coffee shops, and other drive-through stores, as well as in-car payments for purchases made via ecommerce or other sites accessed in the car.

The auto insurance industry is also rapidly moving towards using biometric driver authentication by applying premium rates specific to the driver driving the vehicle, based on the history and characteristics of the driver. Such an approach is expected to significantly benefit the safe driver who today pays premiums based on alternative approaches that take drivers of all profile into account. With iris-enabled rearview mirrors, a driver can be continuously identified and authenticated, ensuring the appropriate insurance rates are applied. This will make sure a new teenage driver has a different rate than more experienced drivers, even when they use the same car.

Personalization and autopilot-like alert

Biometric technologies can also be used for an effortless and more pleasing in-cabin personalization: setting the music, maps, and call history based on the preferences of the particular driver.

Iris recognition technology can also improve safety by monitoring drivers' eye movements for drowsiness and distraction. In autonomous vehicles of the future, such a system can not only alert the driver but also activate the autonomous mode to drive the vehicle to safety, if so configured by the driver.

Connected cars are bringing drivers more convenience and entertainment, but they come with security and safety issues. Biometric technologies such iris, fingerprint, and voice recognition can help drivers navigate a safer and more user-friendly driving experience.

Venture Beat. http://venturebeat.com/2017/02/07/why-biometrics-are-the-key-to-driver-authentication-in-connected-cars/