CYBER RESILIENCE CYBERSECURITY DATA MANAGEMENT DATA PRIVACY

Face Facts: Are Biometrics Key to Deleting Passwords for Good?

Facial recognition and other biometric technologies have been proposed as replacements for traditional passwords. How viable are these technologies and what are their vulnerabilities?

Richard Pallardy, Freelance Writer

June 27, 2024

15 Min Read

Editor's Choice

re Sabotaging
ur Cybersecurity Stance

MARCOS ALVARADO VIA ALAMY STOCK

Everyone hates passwords. Even with the advent of password managers, keeping track of the dozens of strings of characters necessary to manage daily online activities is a burden. Passwords are constantly compromised by data breaches and resetting them has become a prevailing irritation of modern life.

Half the time, it barely seems worthwhile. The advent of the computer password at the Massachusetts Institute of Technology during the 1960s precipitated decades of irritation, theft, and even physical danger in the case of security breaches.

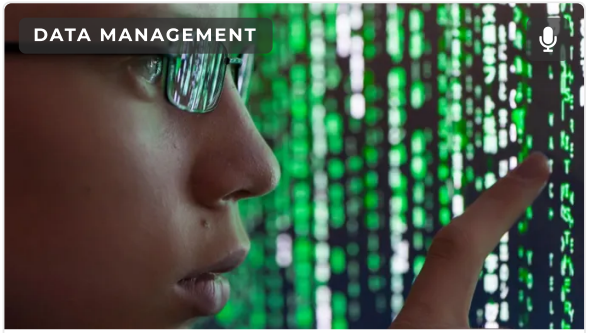
by **Lisa Morgan**

JUN 20, 2024 10 SLIDES

2024 InformationWeek US IT Salary Report: Profits, Layoffs, and the Continued Rise of AI

by **InformationWeek Staff**

JUN 4, 2024 1 MIN READ



Who Owns Me: Data Monetization, Data Privacy, and Data Ownership

by **Joao-Pierre S. Ruth**

JUN 10, 2024

IT LEADERSHIP

To paraphrase “Sex and the City” character Carrie Bradshaw: Some of us can’t help but wonder ... what is the point when the sites that are claiming to protect your data are going to get hacked anyway?

Most users deploy variations of only a handful of passwords or variations thereof, making them even more vulnerable to bad actors who would exploit them. And people on average have about 170 passwords. Some 49% of data breaches are attributable to stolen credentials according to Verizon. Passwords are not just an annoyance to the user. Between 2019 and 2021 alone, the time spent by IT teams on password management grew by 25%.

People are allowed to get into systems by three general mechanisms: something you know -- a password; something you have -- a physical security key; or something you are -- your face, your fingerprint, or your behavior.

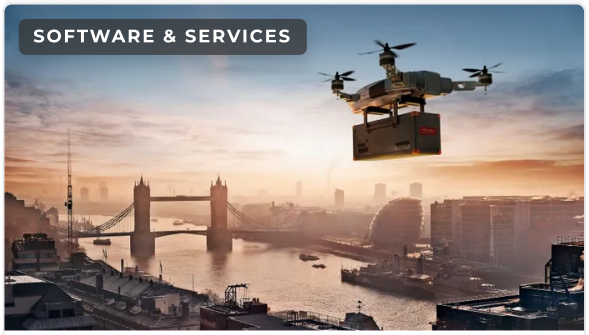
Related: Biometric Data Privacy: Instagram to Pay $68.5M in Class Action Settlement

Biometric technologies such as facial recognition and fingerprinting have been proposed as viable alternatives to typing in those impossible-to-memorize lines of characters that allow us to safely access our accounts. In 2001, the MIT Technology Review predicted that biometrics would be one of the technologies most likely to change the world. It seems that they were correct, for better or for worse.

Biometric passwords are supposedly harder to steal or to fake than passwords. Indeed, whether it is your face, your voice, your irises or your

9 Future of Work Concepts That Need More Attention

by **Lisa Morgan**



Will Home Drone Deliveries Ever Become Practical?

by **John Edwards**

JUN 21, 2024 5 MIN READ

White Papers

IT Service Desk Overwhelmed?

fingerprints, your biometrics are completely unique. And they offer that most valuable of qualities: convenience. Stick your phone in your face or squish your finger against the screen and you're in. Snap a selfie and your banking information appears.

Indeed, facial recognition and its cousins seem like miraculous solutions. Science fiction is rapidly becoming science reality. Apple, Intel, Microsoft, and many other tech leaders have already included biometric options in their products. But they come with their own complexities and, at least according to some experts, are unlikely to fully replace traditional passwords in the near term.

Related: Preparing for the Post-Password World

Along with these innovations have come a suite of hacks that attempt to get around them. The creepy silicone masks from "Mission: Impossible"? They're real, at least according to one study. The face-swapping AI technology that allowed someone to impersonate a politician on live television in the British thriller series "The Capture"? It's almost here. Or has it already arrived?

As unsettling as biometrics may be, they actually have a long history and some have suggested that we may be able to adjust their usage to levels that are at least more ethical than the most dystopian projections suggest.

InformationWeek delves into the development of facial recognition and other biometrics, along with their current and future applications, with

insights from Dominic Forrest, chief technology officer at biometrics solutions provider iProov, and Kyle Helles, partner and attest practice leader at cloud-based security and compliance solutions provider BARR Advisory.

What Are Biometrics?

Biometrics are measurements of various components of the human body and how they relate to each other. In the case of fingerprints or facial recognition, they describe the size and distance of various physical features -- the distance between the eyes and nose, the width of the lips, the gaps between the ridges on your fingers. Even skin texture is now used as a verifying feature. Finger veins, patterns on the palm and patterns of heat emitted by the body have also been used. These are physiological biometrics.

Related: What the Fawkes: Facial Recognition, Digital Masking, and AI

Biometrics can also describe such features as gait or typing speed -- how your limbs and digits interact with the environment in unique, highly individual ways. Vocal characteristics, signature recognition and patterns of lip movement are also used. These are behavioral biometrics.

These characteristics must be discernible by computerized sensors and then converted into quantifiable data.

Facial recognition is perhaps the most recognizable of these technologies, followed by fingerprint scanning. Crucially, face detection and facial

*The Need for Modern Observation in Complex Cloud Environments

2022 State of Network Management

2022 State of ITOps and SecOps

More Reports >

recognition are two different things. Face detection is what occurs when you post a picture to a social media site and its algorithm determines that a human face is present so you can tag that other person's socials. Facial recognition is far more sophisticated … it can actually discern an individual using their distinct biometric characteristics.

Humans have 43 muscles in their faces and can create more than 10,000 expressions using them. In combination with the bony structures beneath the muscles, they offer a unique signature that can be used for verification. Early versions of facial recognition used two dimensional images to match faces but now three-dimensional imaging is preferred due to its greater accuracy.

A facial recognition program scans an original, verified image of a user's face for particular characteristics and then matches it to the new image taken in order to verify that the user is authorized to access. The same is true of fingerprints, iris scans and other means of physiological biometric analysis. Behavioral biometrics match such factors as the recorded speed or pressure of typing a series of words or the timing and spacing of when someone's feet hit the ground.

Though physiological biometrics are unlikely to change over time, at least in terms of the features actually measured, behavioral biometrics are more mutable and thus present challenges in terms of verification over long periods.

How Biometrics Work

The first step in any biometric technology is capturing a baseline set of features or behaviors. Using either photographs or video, patterns are discerned and recorded. These patterns are stored by the program and then matched when the user attempts to access the system.

As sophisticated as contemporary image capture is, the images captured must be standardized to be efficiently matched to stored data. So, with facial recognition, a program must first identify the image as a face, orient it properly to match the features that truly identify the person depicted.

The two templates are matched and scored according to the features stipulated by the program, whether they be the distance between the eyes, nose and jaw, the distance between the ridges in a fingerprint, or the typical time and rhythm of typing out a series of words. If the qualities are a sufficient match, the program grants the user access. If not, they are denied.

In order to capture an image of a face suitable for matching to the stored data, an array of technologies must be deployed. In the case of Apple's FaceID, the picture is taken and analyzed by the combined efforts of an ambient light sensor, flood illuminator, infrared camera, proximity sensor and dot projector. The dot projector in particular is essential in locating the facial landmarks that establish that the face looking into the camera represents the person who is entitled to access the system.

Because of the variables that may occur in capturing the live data -- the shadows and differing angles depicted in a photo of your face for example -- these programs undergo extensive training in order to eliminate false negatives. So, too, false positives must be eliminated. You don't want your

identical twin sneaking a look at your DMs. Programs have been refined to pick up even minor variations that might not be noticeable to human observers, such as patterns of wrinkles, skin texture variations and scars.

Deep learning approaches have been developed, allowing for the extraction of multiple angles from single images or only a small number of images, reducing the amount of time it takes to develop the baseline set of features against which future images will need to be matched. And now many programs use 3D modeling that captures features that remain constant over time such as the shape of the eye socket or the chin bone. Some of these programs can translate 2D and 3D images.

History of Biometrics

Facial recognition strikes many of us as a future-is-now sort of technology -- something out of a sci-fi film like *Minority Report*. But the rudimentary use of images and other recordings of human characteristics to identify people dates to thousands of years ago. It is believed that fingerprints and sometimes handprints may have been used to sign documents in ancient China and Babylon.

More sophisticated analysis of biometric features began in earnest some two centuries ago. Czech physiologist Johannes Evangelista Purkinje identified patterns in fingerprints in 1823 and by the late 19th century they were used in criminal investigations. The first wanted poster featuring a photograph -- Abraham Lincoln's assassin -- was printed in 1865. And the Pinkerton Detective Agency had developed a database of images of suspected criminals by 1870. French policeman Alphonse Bertillon began

developing a system of bodily measurements for identifying criminals in the 1870s as well. Facial recognition as we know it seems novel, but it is not as new as some might think.

Kyle Helles, BARR Advisory

“Facial recognition technology is decades old,” Helles says. “It has been refined over time through a combination of better cameras and improved photo and video quality, as well as improvements in the software used to map and identify individuals’ facial attributes.”

Scientists have been working on computerized facial recognition since the 1960s. Charles Bisson, Woodrow Bledsoe, and Helen Chan Wolf of Panoramic Research in California made early inroads into matching photographs of people using digital technology.

They concentrated on many of the same facial landmarks used today, such as the spacing of the eyes, nose, and mouth. During the course of their research, which was supposedly funded by anonymous intelligence agencies, they came up against the challenges that contemporary AI versions of facial recognition technology attempt to address -- lighting, angles and position all affected the ability of the program to match faces to images in the database.

Over the next 30 years, researchers honed the areas of the face that needed to be analyzed and developed complex algorithms in order to do so efficiently. Eigenfaces and Fisherfaces, developed during the 1980s and 1990s, began to refine the extraction of facial features from a series of images in a way that would adjust for suboptimal conditions.

In the United States, the Defense Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology (NIST) sponsored the Face Recognition Technology (FERET) program beginning in 1993. The program created a database of images that could be used by industry to experiment with facial recognition technology. This expanded to Face Recognition Vendor Tests (FRVT) beginning in 2000 and extending to 2017. These NIST programs assessed the viability of various facial recognition programs.

The introduction of deep learning techniques, such as convolutional neural networks, have resulted in massive gains in accuracy. Tests of multiple programs run by NIST in 2014 saw 4% search result failures. Those failures were at only .2% in 2018.

During this period, some of the first facial recognition technologies came to wider use -- significantly, Facebook began using facial recognition to identify users in photographs beginning in 2010. Apple's iPhone X introduced cellphone customers to facial recognition using its FaceID technology to unlock the phones in 2017. In the ensuing decade, facial recognition has been deployed by banks, employers, and various tech providers in an effort to provide what they view as safe, seamless access to sensitive information.

"Facial verification has evolved significantly over time. Some of the early methods used basic measurements and were prone to errors. The introduction of machine learning, and later deep learning, drastically improved accuracy," Forrest says.

The Advantages of Biometrics

Biometric technologies are believed by their proponents to offer more secure and efficient access to private information and to services that require its use. From banking to airport security to internal communications, the use of facial, fingerprint and palm recognition, among other modalities, create ostensibly seamless transactions.

"Facial recognition is generally more secure than a traditional password. This is because reliable facial recognition checks something that others cannot steal or replicate and is unique to you -- your face," Helles says.

"The rise in cybercriminals defeating traditional verification technologies, such as passwords and one-time passcodes, to commit fraud has led to the

commoditization of what were once deemed secure technologies. In the digital era, ensuring secure remote identity verification and authentication is paramount for organizations," Forrest adds.

The difficulty of duplicating biometric information may reduce the incidence of fraud. Passwords are easily stolen or extorted from users, either in cyberattacks or on an individual level. Further, consumers are not required to memorize or record passwords or PIN numbers, reducing the time spent accessing systems and the cost on both ends of resetting them if they are lost or forgotten. And passwords do not need to be entirely abandoned; they can offer a second layer of security in biometric systems. These technologies are relatively easy to integrate into most types of secure systems.

Biometrics may reduce the levels of ATM frauds, for example. One survey suggests that there is one incidence of fraud per 3.5 million transactions. There are around 10 billion ATM transactions processed each year in the United States alone. ATM technology that uses biometrics can reduce fraud by eliminating the possibility of card and PIN theft. Banks in Japan have already introduced biometric technologies such as palm and facial recognition.

The Vulnerabilities of Biometrics

Built-in computer cameras may suffice in some cases, but biometrics do require specific devices to work in some contexts, such as entry to a building or access to an ATM. The devices themselves may malfunction, either simply breaking or inaccurately reading biometric information. For

example, lighting may affect facial biometrics and dirt and temperature may affect fingerprint scans.

Securing stored biometric information to prevent theft and misuse can also be costly. While more difficult to use, biometric data can be stolen or misused. In 2015, 5.6 million fingerprints were stolen from the US Office of Personnel Management in a massive data breach. Thieves may demand that victims unlock their phones or access their bank accounts using biometric data under duress. Conversely, there is ongoing debate over whether law enforcement is justified in forcing suspects to unlock their phones using biometric data.

While faking biometric information, particularly facial data, is more difficult than it used to be due to liveness verification, it has been done. Depending on the limitations of the recognition program, brute force attacks may be able to use many variations of a face in order to bypass it. In some cases, dictionary attacks may use images harvested from social media to create a convincing composite.

In 2017, a Vietnamese security firm was able to unlock an iPhone X using a mask that mimicked the user's face, "Mission: Impossible" style. And the mask cost only $150 to construct. There is even evidence of camera injection attacks that hijack computer cameras themselves and make it appear that live video is being captured. Similar technology is used in "The Capture".

Dominic Forrest, iProov

“The exponential growth of deepfakes and other AI-generated synthetic media poses a significant threat to remote identity verification,” Forrest says. “While various methods of verifying identity remotely exist, such as video call verification, face biometrics has proven to be the most secure, usable and inclusive method. Other modalities, such as voice, have proven to be particularly susceptible to generative AI.”

Programs may also encounter problems related to natural alterations in human appearance. They need to account for such changes as weight gain or loss and aging that can affect the dimensions of the face. People who are injured or endure other facial alterations will likely have to update their biometric information, which may be a complex process.

Biometrics have also been shown to have racial biases. Amazon’s biometrics were found to be more accurate when categorizing people by sex when they had lighter skin, for example. Other systems have been flagged for similar problems.

Addressing the Weaknesses of Biometrics

“Privacy concerns can be tackled with strong encryption, decentralized storage and privacy-preserving techniques. Scalability and cost issues are overcome through cloud computing and technological advancements,” Forrest claims. Notably, servers that do not store plaintext versions of images and restrict them to the user side may reduce theft by hackers.

Close up images of facial features may be far more difficult to fake, according to some research. It is challenging to extract the specific features used from existing photographs, such as those posted on social media.

Liveness detection has shown perhaps the greatest promise in ensuring that the user is who they say they are. “Robust liveness detection and active threat monitoring are crucial to defend against evolving deepfake attacks,” Forrest says.

Such techniques as patterns of eye blinking and the measurement of blood flow in the face are intended to ensure that a living person is sitting in front of the camera. In the case of fingerprint based biometrics, the activity of sweat pores has been proposed as one means of defeating spoofing attacks that use artificially constructed fingerprint patterns.

Detection of the noise created by converting video files used in spoofing attacks may help as well, as they will not match the noise generated by the camera ostensibly used to identify the user unless the fake video is created by that same camera.

Two-factor authentication, which may include the use of a password, will also create tighter controls while strictly biometric systems work out their kinks. “Multi-factor authentication is a great way to secure systems -- better than passwords alone. Biometrics are just one form of a second factor. Others include temporary PINs and passcodes that are randomly generated by solutions like Google Authenticator, or something physical like a badge,” Helles claims. But biometrics are not a cure-all.

“Human research and critical thinking skills are still essential when identifying potential threats,” Forrest says. “The ultimate solution lies in combining the strengths of both humans and automation.”

About the Author(s)

Richard Pallardy

Freelance Writer

Richard Pallardy is a freelance writer based in Chicago. He has written for such publications as Vice, Discover, Science Magazine, and the Encyclopedia Britannica.

Never Miss a Beat: Get a snapshot of the issues affecting the IT industry straight to your inbox.

SIGN-UP

You May Also Like

More Insights

Reports

2024 State of Networking Report

2024 InformationWeek US IT Salary Report

*The Need for Modern Observation in Complex Cloud Environments

2022 State of Network Management

2022 State of ITOps and SecOps

More Reports >