



Petty Officer 1st Class Katy Jones, a Navy sailor with the 22nd Marine Expeditionary Unit Female Engagement Team performs a fingerprint scan.

HOME // SECURITY

SECURITY

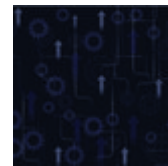
How the Government Uses Biometric Authentication Technology

From fingerprints to facial recognition, agencies turn to a person's physical characteristics to verify identity.



by **Elizabeth Neus** 

Elizabeth Neus is the managing editor of *FedTech*. Before joining *FedTech*, Elizabeth was a reporter for Gannett, covering health care policy and medicine. As a Gannett editor, she worked on publications and magazines focusing on everything from defense to agriculture to travel to shopping. The Washington Nationals are her team; 80s Brit pop is her sound.

Latest Articles

Imagine Nation ELC 2019: RPA Adds Needed
'Employees' To Strapped Agencies



Imagine Nation ELC 2019: EEOC, USDA Receive The Latest TMF Awards



How To Effectively Implement Zero Trust Security



Multifactor Authentication Helps Agencies Boost Cybersecurity

Biometrics technology first gained a stronghold in government in the late 1800s, when police officers began to use fingerprints as a way to identify suspects. Since then, **government use has expanded** to include ID verification of federal employees, travelers and in some cases, the average citizen.

The technology has grown more sophisticated, recognizing unique features in the eyes, the face and [even the way a person behaves](#), and the government is looking for ways to incorporate those new capabilities and biometric data into identification practices.

But there are also **questions about the accuracy** of the technology, and about the protection of privacy and civil liberties when facial recognition technologies are used to identify people for investigations. Nevertheless, biometrics remains the wave of the future.

"The era of the password is drawing to an end," writes Walker Van Arsdale on [CDW's Solutions Blog](#). "While we've relied on secret pieces of information to safeguard our access to information and systems for decades, it's clear that **password security is no longer adequate**."

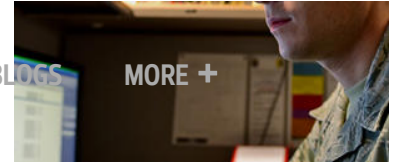


**Introducing
The Cybersecurity
Insight Report.
Orchestrated by CDW.**

**DOWNLOAD THE
REPORT NOW!**

What Is Biometrics Technology?

Biometrics technology **uses a person's unique, relatively unchanging physical characteristics** as a form of ID, rather than having the person rely on a forgettable and hackable password. It's often used as the second factor in multifactor authentication.



CLOUD

**Air Force
Wants to
Accelerate
SaaS
Deployments**



CLOUD

**SaaS
Streamlines
Operations at
DLA, State and
Treasury**

ADVERTISEMENT

Trending Now

**USDA, DOD
And GSA
Gain**

TOPICS

AGENCIES

TIPS & TACTICS

VOICES

FEATURES

VIDEO

IT BLOGS

MORE

scanned — then the computer runs that image against a pattern-recognition database. The system taps into that database, and if the person's biometric data matches what's on record, he gains admittance to the building or the network.

While most biometric data is used for employee identification, **it's also rolling out in areas besides the workplace.** Most smartphones can be unlocked with a glance by the verified owner; laptops by companies including Acer and Dell include a fingerprint reader for security. Guests to Disney parks use their fingerprints to gain entry in addition to a ticket.

However, while the iris and the fingerprint are unchanging physical characteristics that can be easily matched, **faces are less simple to identify** using biometrics technology.

Facial recognition algorithms can have [trouble identifying women and people of color](#); grow a beard or put on a pair of glasses, and that can confuse the algorithm as well. (There are, however, [glasses under development that contain facial recognition software](#).)

In the government arena, a [June 2019 Government Accountability Office report](#) determined that the FBI needed to do more robust testing of its facial recognition technology to make sure it was as accurate as the FBI claimed.

"As the size of a photo database increases, the accuracy of face recognition searches performed on that database can **decrease** due to lookalike faces," the report states. "At the time of our review, FBI's test database contained 926,000 photos while [its operational database] contained about 30 million photos."

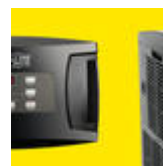
How Is the Federal Government Using Biometrics?



DOD, State Department See Benefits From Shifting Global Operations To The Cloud



SEC, USCIS Turn To Telework For Flexibility And To Lure Top Talent



Review: Tripp Lite's SRCOOL12K Keeps Computer Systems Cool

travelers. The agency uses biometric technology to detect and prevent illegal entry, to verify information on visa applications and to keep legal travel and trade moving smoothly.

Since 2016, U.S. Customs and Border Protection [has been working with airlines](#) to use facial recognition technology as part of the preboarding screening process; [at least five airlines now use it](#), largely for international flights ([it's voluntary for American citizens](#)).

In 2017, President Donald Trump signed [an executive order](#) requiring that **the top 20 U.S. airports use biometric technology and facial recognition by 2021** for all international passengers. Earlier this year, he signed the [National Strategy to Combat Terrorism Travel](#), which calls for the increased use of biometric technology and data to stop terrorists from entering the U.S.

Recently, the Transportation Security Administration has [tested automated biometric screening](#) at Los Angeles International Airport and McCarran International Airport in Las Vegas. The LAX test involved cameras and scanners placed at special automated security gates; the [Las Vegas test](#) captures images at the regular checkpoint **with the passenger's permission**.

CBP has **processed more than 19 million travelers** using facial recognition technology at airports and also at land crossings in the past three years, and has found a little more than 100 people who were trying to enter the U.S. by using others' identities, [reported The Hill](#).

"With facial comparison biometrics, CBP is ... **solving a security challenge while adding a convenience** for travelers," a CBP spokesperson told the newspaper.

DHS also shares its biometric information with the Justice and Defense departments to aid those agencies in their

according to its website.

TOPICS

AGENCIES

TIPS & TACTICS

VOICES

FEATURES

VIDEO

IT BLOGS

MORE +

That repository – the Automated Biometric Identification System, **processes more than 300,000 biometric transactions per day and holds biometric data on more than 250 million people.** DHS plans to upgrade the system and [move it to the cloud](#) so that it can potentially identify people through scars, tattoos and other physical markings as well.

[MORE FROM FEDTECH: Learn more about the Defense Department's biometric identification initiatives.](#)

While DHS and its component agencies are perhaps the most high-profile users of biometric data, other agencies are taking that road as well:

- The FBI calls its [Next Generation Identification](#) system “the world's largest and most efficient electronic repository of biometric and **criminal history information**,” with biometric data including fingerprint and palm prints, iris identification, facial recognition data and photographs of tattoos and scars.
- The Defense Department is testing the use of biometric data to help **verify employee ID**. The Air Force, for example, is considering using [artificial intelligence–powered facial recognition](#) to clear legitimate visitors and workers through the gates at its bases; and the DOD in general is interested in using biometric data as **the second factor in MFA**.

“I assume the technology is going to continue to get better and better, and will come to a point where it really is able to **fully automate a lot more identification** and decision making,” said Jeremy Grant, founder of the National Program Office for the National Strategy for Trusted Identities in Cyberspace at the National Institute of Standards and Technology, [in an interview with Federal News Network](#).

TOPICS

AGENCIES

TIPS & TACTICS

VOICES

FEATURES

VIDEO

IT BLOGS

MORE +

personal personally identifiable information that exists.

Strong endpoint security and encryption are among the most reliable tools.

But at present, biometric data itself poses an unsolvable security problem: "In the event of a breach, it creates a Herculean challenge because physical attributions such as **fingerprints cannot be replaced**," data security expert Kon Leong, CEO and co-founder at ZL Technologies, told [CSO Online](#).

The number of **hacks involving biometric data** — and the number of organizations compiling biometric data without the owners of that data knowing about it — is on the rise.

Most recently, a biometrics company used to provide physical security for defense contractors, banks and Scotland Yard found that [its worldwide database was improperly protected](#). More than 1 million fingerprints, facial recognition information and other personal data from [companies around the world](#) had been **leaked to a public website**.

In the noncriminal sector, agents with the FBI and Immigration and Customs Enforcement [have turned state driver's license databases into a facial-recognition gold mine](#), scanning through millions of Americans' photos without their knowledge or consent, newly released documents show. That has raised [civil liberties concerns](#).

"We need **strong legal safeguards** that guarantee civil rights, fairness and accountability," Kate Crawford, co-director of the AI Now Institute at New York University, wrote in the science journal [Nature](#).

Ironically, one way to make biometric data more secure is to **use passwords**, [reports GCN](#) — strongly encrypted so that if the data is stolen, the passwords that release it are

GCNreports.

TOPICS

ARTICLES

NEWS & ANALYSIS


FORUMS

VIDEOS

FEATURES

IT BLOGS

MORE +



Get More Insights Delivered
Right to Your Inbox.

Sign Up Now >>

More On **AUTHENTICATION** **DATA PROTECTION**
ENCRYPTION **IDENTITY MANAGEMENT**

Related Articles



Security

How to Effectively Implement Zero Trust Security

Security

Multifactor Authentication Helps Agencies Boost Cybersecurity

Security

3 Ways to Stay Ahead on Supply Chain Security

SPONSORS

[TOPICS](#) [AGENCIES](#) [TIPS & TACTICS](#) [VOICES](#) [FEATURES](#) [VIDEO](#) [IT BLOGS](#) [MORE +](#)

Technology Solutions That Drive
Government

[About Us](#) [Contact Us](#) [Privacy](#)
[Terms & Conditions](#) [Site Map](#)

FEDTECH:



CDW:



VISIT SOME OF OUR OTHER TECHNOLOGY WEBSITES:

EXPERTS WHO GET IT



Drive
Adoption of
Your
Collaboration
Solutions by
Tracking
These 3
Metrics

[Read the Blog](#)

Get
FedTech in
your Inbox

[Browse Email
Archives](#)

Subscribe
to FedTech
Magazine

[Browse
Magazine
Archives](#)[BACK TO TOP](#)

Copyright © 2019 CDW LLC 200 N. Milwaukee Avenue, Vernon Hills, IL 60061