Biometrics in government: Enhanced security and convenience for citizens

AWARE

Table of Contents

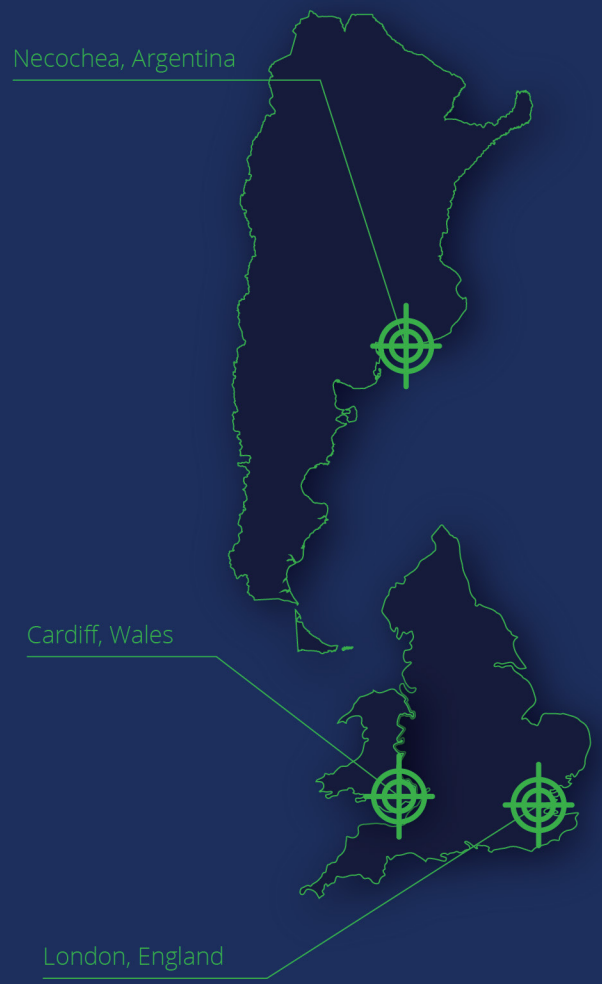
A brief history of biometrics

Fingerprint-based identification began in law enforcement. An Argentine detective first solved a crime using a latent print (left behind by the perpetrator) in 1892. In 1901, detectives in England and Wales officially began using fingerprints in criminal identification.

Their use snowballed from there. By 1946, the FBI managed a library of **100 million fingerprints**, according to the U.S. Marshals Service. The agency developed the Automated Fingerprint Identification System (AFIS) in the 1970s to manage the massive and still-growing collection more effectively.

AFIS became "Integrated AFIS" (IAFIS) in 1999 to help law enforcement agencies share fingerprint data over state lines. After the events of 9/11, fingerprint identification in the U.S. migrated from law enforcement into border protection and VISA screening.

Today, governments worldwide use biometrics for many other purposes, including border management, defense, employee screenings, healthcare, security, and more.



Law enforcement

In the U.S., IAFIS is a national database that lets state and local law enforcement agencies from all over the country search fingerprint records beyond their jurisdiction. These include live prints captured during a booking or latent prints collected as evidence at a crime scene.

The FBI more recently developed **the Next Generation Identification (NGI) program** to support facial recognition and iris recognition. Surveillance footage of a suspect's face can be compared to a national database of mugshots to establish identity. In 2013, **the FBI Iris Pilot** also began capturing iris images at correctional facilities to build a database of yet another biometric modality.

The common thread among fingerprint, face, and iris is they're unique biological identifiers with exceptional identity-matching performance. This makes them a valuable resource for identification in law enforcement.

Border management

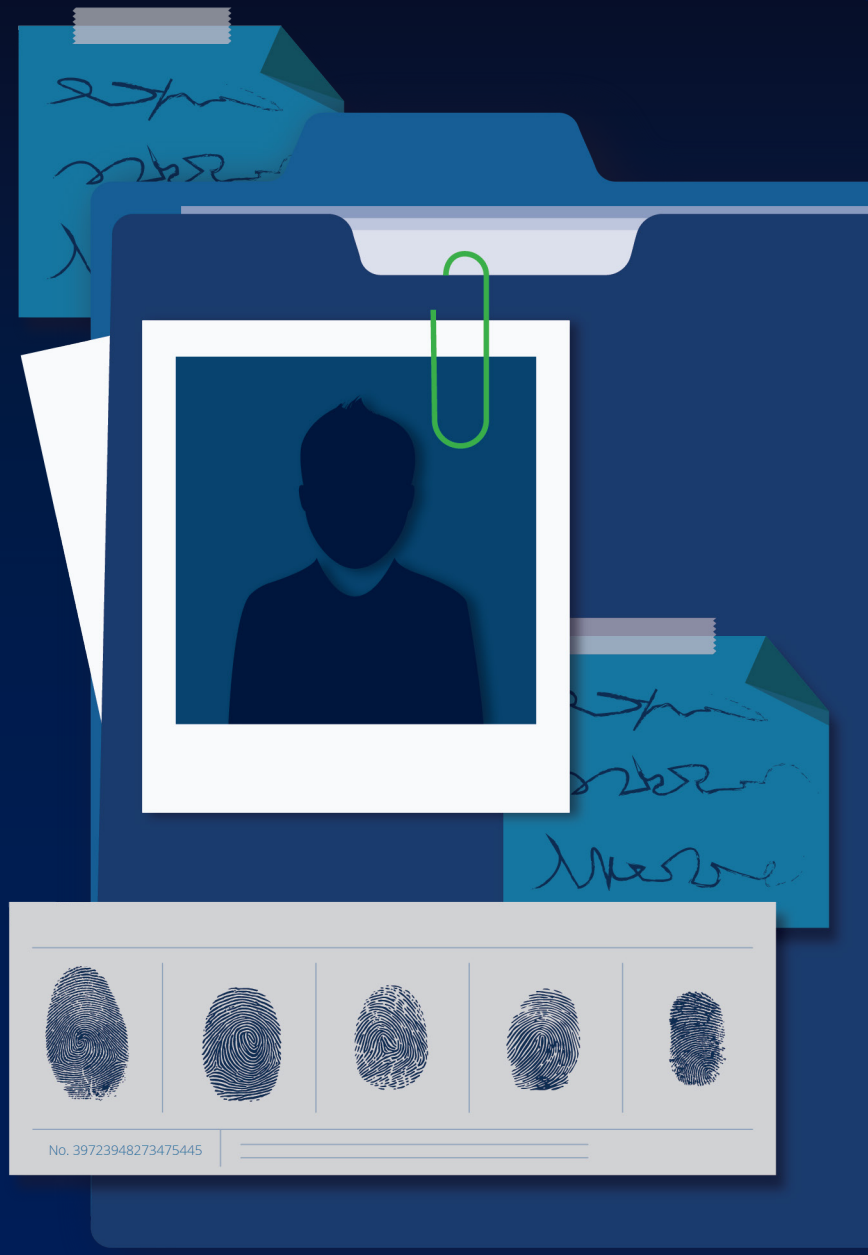
Government agencies also use biometrics to verify identity at international borders. In some countries, visa applicants must provide biometric samples to be searched against criminal databases and immigration records.

For example, the Canada Border Services Agency **collects fingerprints and photographs** of individuals from Europe, the Middle East, and Africa who apply for:

- **Temporary resident visas**
- **Work permits**
- **Study permits**
- **Temporary resident permits**
- **Permanent residence**

Canada will extend the policy to include Asia, Asia Pacific, and the Americas in 2019. Their biometric system is **built upon Aware products**, including BioSP, a biometric services platform.

Biometrics are more reliable than biographic data in paper-based documents in identity verification at the border. An applicant can be screened for past immigration infractions or criminal convictions with greater accuracy and confidently cleared for entry.



National defense

National defense also relies on biometric-based identity verification. For example, the U.S. Navy's Identity Dominance System (IDS)—also used by the Marines—includes a mobile, multimodal biometric collection system that captures, stores, and matches identity data belonging to unknown individuals, such as any person taken into custody during **a maritime interception operation.**

Ruggedized mobile devices are used to capture fingerprint, iris, and face data, which can then be used to identify individuals encountered in tactical environments. Aware **provided much of the biometric technology** in this system.

Biometrics are also commonly used to identify known individuals, such as newly enlisted service members and local civilian employees. The ability to perform fast and accurate identity verification of friendly personnel is in some cases as critical as identifying hostile or threatening individuals.

Human resources

Many U.S. federal government job applicants and contractors must undergo background checks to confirm their claimed identity and to verify they're not listed in criminal databases.

Biometrics enhance identity proofing for employee screening by searching biometric databases using fingerprint, face, or iris data. The Department of Defense, for example, recently implemented browser-based biometric identity-proofing across 3,500 locations **using Aware's WebEnroll solution.**

Private-sector institutions such as banks, defense contractors, utilities, and other critical entities can also leverage biometrics to verify applicant identities for the same purpose. This keeps people with criminal pasts or fraudulent identities from infiltrating roles that they're unqualified for, and out of positions where they could become liabilities or safety threats.

Enterprise security

Identity and access control is a security priority for government entities, which is why more U.S. government **agencies are investing** in biometric authentication, according to FedTech.

Biometric authentication is inherence-based, meaning it verifies identity using something the user is rather than something the user has. Cameras for face, microphones for voice, and fingerprint readers are now common on mobile phones, making multifactor authentication through mobile biometrics a logical next step to improve security in government agencies.

The U.S. Government issues common access cards (CAC) to military personnel and personal identity verification (PIV) cards to civilian personnel. These can be used together with mobile biometrics to enhance secure access.

In 2017, the National Institute of Standards and Technology (NIST) issued new **Digital Identity Guidelines** in Special Publication 800-63-3 that encouraged agencies to use biometrics for authentication. This could include access control using biometrics on a mobile device in conjunction with ID cards.

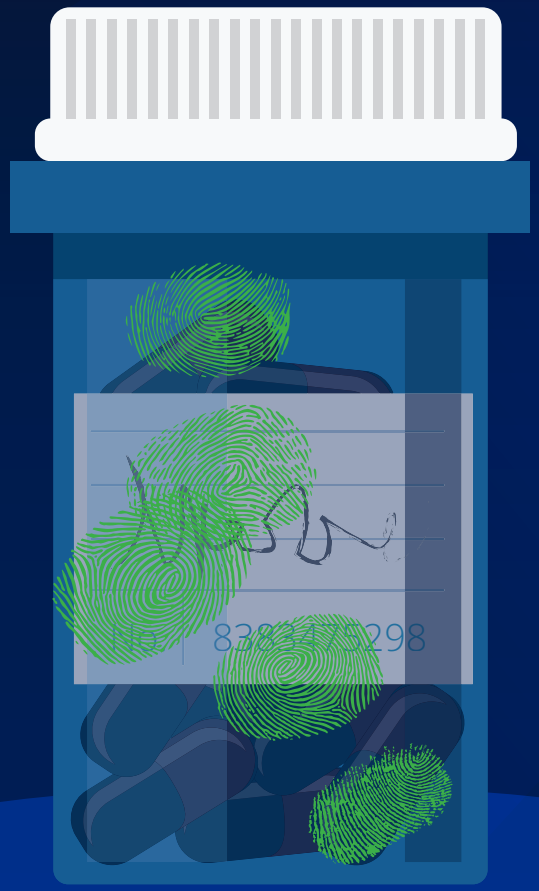
Healthcare

Biometrics are used by government-affiliated healthcare entities for security and fraud prevention.

For example, the Centers for Medicare & Medicaid Services (CMS) collects and submits fingerprints for search to the FBI for owners of suppliers and providers participating in Medicare, Medicaid, or the Children's Health Insurance Program (CHIP). This aims to identify practice owners who may have previously committed fraud or have other infractions on record.

The U.S. Department of Veterans Affairs, meanwhile, uses biometric authentication-based employee access control.

Biometric modalities such as face, fingerprint, voice, and iris can also be used for patient identification in healthcare environments. Providers can be more certain they're delivering care to the right person by verifying identity through a biometric scan.

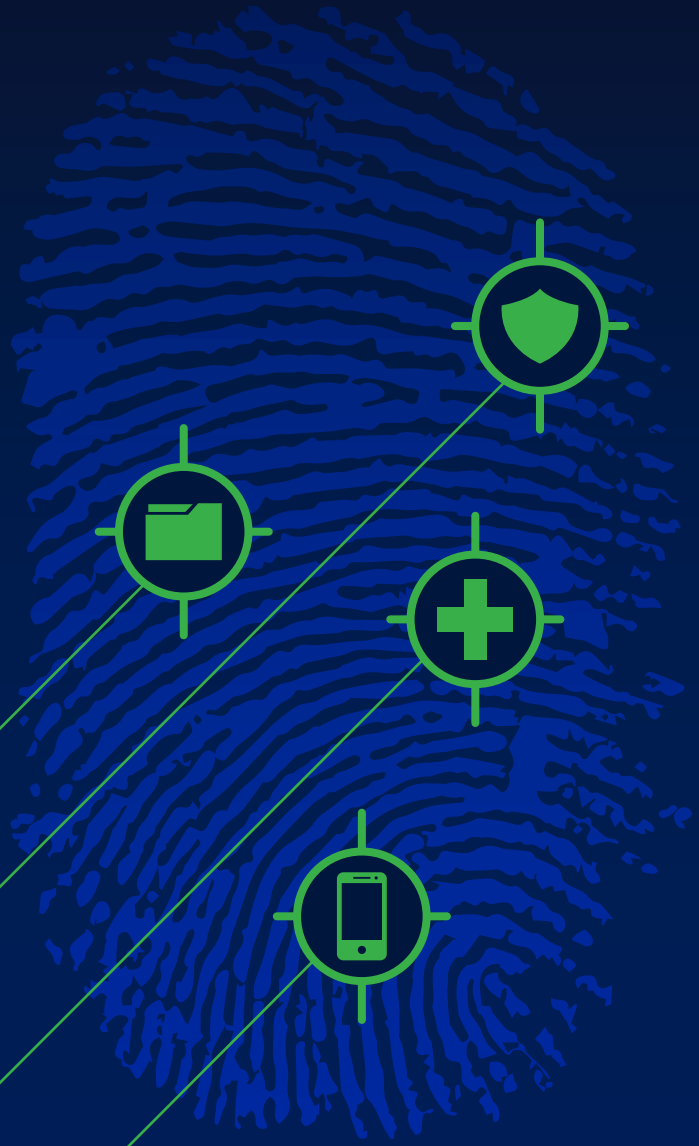


Conclusion

Use cases for biometrics among government agencies have diversified over the years. It began as a single modality—fingerprint—used primarily for law enforcement. Today, biometrics encompass many other modalities (face, voice, iris), and government agencies throughout the world use them in a wide range of security-related activities from law enforcement to border management, national defense, human resources, enterprise security, healthcare, and more.

This is partly because cameras, microphones, touch screens, and other sensors needed for biometric capture have become ubiquitous, including on mobile phones, and also because the performance of biometric matching algorithms has **improved so dramatically.** As a result, more government agencies use biometrics to determine identity with an exceptional degree of certainty.

Biometrics may not be new, but they are entering a new era of utility among government agencies, and beyond.



AWARE

www.aware.com/contact