How cross-jurisdictional search services strengthen biometric identification

AWARE

Introduction

Governments worldwide rely on passports and the relatively limited biographic information they contain for identification of citizens in a variety of critical applications, such as immigration and border management.

But they are increasingly using biometrics to augment their identity proofing efforts.

Biometrics such as a fingerprint, face, and iris are more unique, consistent, and fraud-resistant than simple biographics like name and date of birth, making them useful as a conclusive identifier.

This is not surprising, considering that the most critical data on passports is arguably the facial image; without it, a passport is useless.

Interagency search services

Biometric identification is a powerful resource. When a government agency searches a live biometric sample against its own biometric data, it can definitively identify a match or lack thereof with a high degree of certainty, even among a database of tens of millions of individuals. The utility of biometric identification is substantially enhanced when searches occur across disparate sources.

This is because the reach of a biometric search is limited to only those individuals that have been previously enrolled into the system. These databases take time to build. By gaining the ability to search other databases, agencies can make use of data that has been previously collected by others. Access to external databases is typically facilitated not by sharing or duplication of biometric data in databases, but rather through the provision of services that allow the owner and host of biometric data to perform a search as a service to the inquiring party. In this model, sharing of personal data can be minimized. For example, an agency of country A wants to know definitively if an individual visiting from country B is found in that country's law enforcement history.

This is typically enabled by the country A submitting a biometric search request containing the biometrics of the subject to country B, which responds by conducting a search and conveying its results to country A. The FBI's Integrated Automated Fingerprint Identification System (IAFIS) is an example of an organization providing interagency biometric services. It processes electronic submissions from more than 18,000 federal, state, local, tribal, and international agency partners.

Governments worldwide rely on passports and the relatively limited biographic information.

AWARE

The FBI originally intended for IAFIS to be a criminal database without necessarily anticipating how it might be used in other areas, such as border management.

Many of these are law enforcement entities that submit biometrics collected during a booking or investigation to the database so that later on, other agencies might match a print from a crime scene or booking to an existing record in IAFIS.

A small police force in Idaho, for instance, can positively identify someone who was booked in a New Jersey county more than a decade ago.

By expanding the reach of a biometric search beyond jurisdictions, security and law enforcement entities can cooperate on preventing and solving crimes just as they do in so many other ways, particularly for smaller organizations. Large agencies also greatly benefit from the local focus of smaller ones.

Enabling large-scale interoperability

As effective as it is, IAFIS is focused only on domestic law enforcement. Interoperability outside this domain is critical for many scenarios. The FBI originally intended for IAFIS to be a criminal database without necessarily anticipating how it might be used in other areas, such as border management.

This became apparent after the events of 9/11. Lawmakers began questioning if there was a way for the U.S. Department of Justice, parent agency of the FBI, and the Department of Homeland Security,

parent agency of what was then the Immigration and Naturalization Services (INS), to cooperate on investigations. At the time of the 2001 attack, each agency managed separate biometric databases – DoJ managed IAFIS; INS managed the Automated Biometric Identification System (IDENT).

In the interest of national security and of force-multiplying the identification prowess of two enormous biometric databases, DoJ and DHS enabled interoperability between IAFIS and IDENT in the early 2000s.

AWARE

Biometric data exchanges in action

IDENT is a growing DHS database of fingerprints, photographs, names, dates of birth, and nationalities of more than 200 million people who have entered, attempted entry, or left the U.S.

The IAFIS-IDENT data-sharing effort is one of several early efforts to improve U.S. government agencies' abilities to successfully ID someone who might be present in a different database.

For context, IDENT is a growing DHS database of fingerprints, photographs, names, dates of birth, and nationalities of more than 200 million people who have entered, attempted entry, or left the U.S. Its purpose is to identify individuals attempting to enter or leave the country who may be on a watchlist or who have a criminal record in the U.S. IDENT's Interoperability with IAFIS provides an additional element of information in a search: what is this person's history with U.S. law enforcement?

This greatly increases the likelihood that information useful to preventing fraud and crime will be found, if it exists.

Examples of large-scale, interagency data-matching efforts outside the U.S. include the following:

The Five Country Conference (FCC) High Value Data Sharing (HVDS) Protocol

The United Kingdom, the U.S., Canada, Australia, and New Zealand began the FCC to provide biometric data interchange services for immigration and law enforcement purposes. Each member state can search fingerprints belonging to 3,000 individuals in other member states' databases every year.

If a successful match is made in an existing database, identity information, travel document information, criminal records, resident status, and transaction history (e.g., a visa application) can be shared with the member state that issued the request.

Eurodac (European Dactyloscopy)

This system applies to all European Union member states. Its purpose is to biometrically document asylum seekers and irregular border crossers. Every person who applies for asylum in an EU member state will have his or her fingerprints submitted to the Eurodac central system, where they become searchable by any and all EU member states. This makes it easier to assess asylum applicants and perform background checks.

Eurodac and law enforcement agencies in member states can also compare fingerprints linked to criminal investigations about serious crimes such as murder and terrorism.

Visa Information System (VIS)

The purpose of VIS is to share visa data in the Schengen Area (26 European countries that have abolished the need for member-state citizens to present passports at the border). Every individual who applies for a visa in one of the Schengen-Area countries must provide fingerprints and a photograph along with their written application materials.

The VIS biometric matching system helps verify the identity of a visa applicant. It can flag individuals attempting illegal "visa fishing" – applying for entry to multiple countries at the same time, under multiple aliases, or with stolen travel documents.

AWARE

Interpol

The exclusive purpose of Interpol is to facilitate cooperation between law enforcement efforts of different nations. It manages a biometric database that allows authorized users in member countries to submit fingerprint data to check for an existing record. It's been a successful program, having made more than 2,000 positive identifications in 2017 alone.

Biometrics without borders

> **Implementation of this U.S.-developed standard enables interoperable biometric data exchanges across jurisdictions and between disparate systems; more simply, it makes interagency search services possible.**

All of the interagency efforts introduced above share a common goal: cross-jurisdictional cooperation.To support this endeavor, many agencies throughout the world leverage ANSI/NIST ITL1-2015. Implementation of this U.S.-developed standard enables interoperable biometric data exchanges across jurisdictions and between disparate systems; more simply, it makes interagency search services possible.

Standards such as ANSI/NIST ITL 1-2015 along with advanced biometric middleware like Aware's BioSP will likely facilitate even greater interagency data sharing. Case in point, the U.K. recently selected BioSP to support data sharing between different biometric matchers used by law enforcement, border management, and immigration in the U.K. via a central services system.

In the coming years, other agencies will likely follow suit in the interest of vastly improving the performance of biometric identity verification.

Interested in learning more? Visit www.aware.com/contact/

Sources:
https://archives.fbi.gov/archives/news/testimony/overview-of-fbi-biometrics-efforts
https://www.hsdl.org/?abstract&did=703348
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/557896/biometric-data-sharing-v7.0.pdf
https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en
https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en
https://www.interpol.int/INTERPOL-expertise/Forensics/Fingerprints
https://www.prnewswire.com/news-releases/aware-to-provide-biosp-and-services-for-uk-government-biometric-matching-platform-300674292.html

AWARE