Government Business Council

The Changing Face of Law Enforcement Investigations

Biometrics In the Department of Justice and Department of Homeland Security

Red Hat | intel

INTRODUCTION

Federal law enforcement agencies have historically leveraged biometric information to aid in investigations, enforcement of authorized access to prevent fraud, or as validation for entry or services. The Department of Justice (DoJ) and Department of Homeland Security (DHS) are increasingly using biometrics as central tools in their missions. However, biometric information can be difficult to access — siloed, specific to agency use, stored in a back office, or otherwise not field enabled, much less for real-time access. Given new requirements, along with new biometric markers, agencies must rethink their approach to storing, automating, and delivering secure platforms at scale for rapid analysis and field forward identification.

SIDEBAR: BIOMETRIC MODALITIES

- Fingerprints
- Face
- Iris
- Palmprint
- Voice
- DNA

CURRENT MISSION

Department of Homeland Security

Created in the wake of the 9/11 attacks, DHS's mission focuses on counterterrorism, responding to emergencies, and securing America's borders, both physical and technological.

Toolkit

Office of Biometric Identity Management (OBIM)

- Lead designated provider of biometric systems for DHS
- Largest biometric repository in the U.S. government (IDENT)

Automated Biometric Identification System (IDENT)

- 260 million unique identities
- Processes more than 350,000 biometric transactions per day[1]

Biometric and Identity Technology Center (BITC)

- BI-TC provides objective biometric and identity capabilities to DHS, enables operational components to cost-effectively use new technologies, and informs strategic planning and acquisitions of new biometric and identity capabilities.[2]

Department of Justice

The Department of Justice is tasked with enforcing and defending the law, providing federal leadership in preventing and controlling crime, and to ensure fair and impartial administration of justice for all Americans.

Toolkit

Criminal Justice Information Services (CJIS)

- Technology hub based within the Federal Bureau of Investigation (FBI), providing biometrics and other technological services to law enforcement branches of the DoJ.

Next Generation Identification (NGI)

- Combines biometric identification services and criminal history services, including more accurate fingerprint retrieval, rapid search capacity for wants and warrants, and iris and palm print repositories.[3]

Biometric Center of Excellence

- Central program for advancing biometric capabilities for integration into operations, through strengthening criminal investigations and enhancing national security. Program focuses on championing technology development, collaboration and information sharing, and enhancing law enforcement end user capacities.[4]

AGENCY PRIORITIES

Interoperability

Building frictionless interoperability between DHS, DoJ, and the Department of Defense (DoD) is a top priority, focusing on biometric data sharing that supports homeland security, defense, and justice missions. Standards developed in 2016 by the National Institute of Standards and Technology (NIST) provide a common language and standardized format for both data and the collection process, allowing for easier search and retrieval processes.[5] The focus on interoperability has also led to programs such as:

- Single-search interoperability between the DoJ-owned Automated Fingerprint Identification System (AFIS) and NGI, and the DHS-owned IDENT, allowing law enforcement agents to quickly identify whether those passing through border crossings have a criminal history.
- Mandated data sharing between DHS and the FBI as part of the VisaWaiver program.
- Combined DNA Index System (CODIS), an FBI-run system combining multiple agency databases of DNA to allow national sharing of DNA profiles
- "Fusion centers" that can gather, process, and analyze cross-agency information at both the federal and state level.

Moving to the Edge

Biometric technology is allowing law enforcement officers in the field to access data more quickly than ever. From handheld devices that can rapidly match fingerprints against a database to facial recognition technology that uses artificial intelligence and machine learning to identify individuals of interest, law enforcement officers are increasingly able to access biometric data at the edge. Scalability and flexibility are crucial to this process.

Frictionless Access

Frictionless access to data is the new gold standard of identity access, and crucial to law enforcement priorities. Rapidly accessing biometric data to confirm identity assists law enforcement agents at every level of government to assess risk, manage identification, and manage border security.

"The value of technology quickly becomes apparent when focusing on the challenges and hurdles to information sharing. From defining the common data standards to facilitate common understandings and interpretations of information, to protecting privacy rights through electronic management and enforcement of access controls and retention policies—adequate technology planning and utilization can be a critical enabler to sharing information responsibly and fostering safer communities."

— **Fusion Center Technology Guide**[6]

NEW PRIORITIES

As the new administration begins its tenure, some priorities within DoJ and DHS have already shifted. Both agencies have changed tack on immigration biometric use; in early May the new administration withdrew a proposed DHS rule that would have expanded department authority and requirements for collecting biometrics, and also suspended biometric requirements for certain applicants. However, both agencies recognize the benefits of biometrics, and some priorities remain crucial to their missions.

Modernization: Move to Cloud

DHS: Migration of central biometric database to GovCloud

- First step in major overhaul of legacy system from Automated Biometric Identification System (IDENT) to Homeland Advanced Recognition Technology (HART)
- HART, which will be rolled out in four increments, will be the official system of record for national biometric data.
- New cloud-based architecture is designed to be scalable to accommodate the projected increase in data volume.[9]

DOJ: Justice Information Sharing Technology

- FY 2021 budget justification includes funds to continue technology modernization and migration from legacy systems.
- The Joint Automated Booking System (JABS)/Civil Applicant System (CAS), which provides biometric services to DoJ stakeholders and other agencies, will be moved into the cloud in 2021.[10]

DHS: Customs and Border Patrol Entry/Exit

In a post-9/11 world, knowing who was entering and exiting the country became a matter of national security. Customs and Border Patrol (CBP) invested heavily in technology and data analytics, and in 2013 Congress asked the agency to find a frictionless way of using biometrics to confirm traveler's identities. The result was the Entry/Exit program, which automates matching travelers' faces to photographs on file. The algorithm has about 99% accuracy, using a limited search to ensure accuracy and rapidity without compromising privacy.[8]

DOJ GLOBAL PROTECTIONS PROGRAM

Managed by the FBI's Biometrics Center of Excellence, the program collects high-value biometrics obtained from foreign law enforcement partners on both domestic and foreign individuals of interest; equips the Quick Capture Platform, a team that can deploy in under four hours to assist with rapid identification services for emergency operations; and offers a Mobile Biometric Application (MBA) that can be used with FBI smart devices to scan fingerprints for rapid identification. The program's tools allow agents at the edge to immediately access the information that they need to address both domestic and and international threats.[7]

CONSIDERATIONS

Among exciting developments, agencies are also working to maintain public confidence in their use of data and biometrics.

Data Protection

As biometric identification continues to grow, so too does the need for strong privacy protections. Increased data sharing between agencies, while serving the mission, can expand the threat surface and presents a tempting target for malicious actors. Several government oversight bodies have emphasized the need for DHS and DoJ to improve their data protection policies. The Homeland Security Advisory Council's Biometrics Subcommittee reported in December 2020 that DHS needed to take further steps to protect its biometric data, also suggesting that distinctions in protection needed to be clarified between biometrics used for identity matching or background checks, and data collected for law enforcement and intelligence purposes.[11] Other concerns have been raised about the new HART database, including the question of data ownership, lack of caveats for foreign access, and deepfakes that could thwart facial and iris recognition software.[12]

Public Trust

There is still considerable concern from the general public about the use of biometrics by both the government and private industry. Lack of national legislation, as well as a lack of transparency by government agencies like DHS and DoJ, can weaken public trust that these agencies are using their data correctly.

Some cities and states have banned certain uses of biometric identification, such as facial recognition, citing privacy concerns and racial biases. Lawsuits have been filed in dozens of states challenging biometric use by both law enforcement and private industry, including in Illinois under the state's Biometric Information Privacy Act, among the more comprehensive laws in the country on biometrics. Agency priorities must include finding the fine line between security and transparency to alleviate public distrust.[13]

Spotlight On: ICE/HSI

As the largest investigative unit in DHS, HSI (Homeland Security Investigations) uses its unique immigration and customs legal authorities to protect the United States from illegal activity with a border nexus. This activity includes immigration crime; human rights violations; human smuggling; smuggling of narcotics, weapons, and other types of contraband; child exploitation; financial crimes; cybercrime; and export enforcement issues.

CONCLUSION

Biometrics are playing an increasingly large role in DHS and DoJ operations, as both agencies are looking for ways to scale up and modernize their abilities. As the new administration's leadership focuses on their biometric priorities, ensuring privacy, security, and flexibility will be central to their strategies. They will also be looking to the tools that will help them get there — tools that are scalable, rapid, and easy for investigators to use. Moving biometric operations and storage into the cloud may be a gamechanger.

ABOUT GBC

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

EMAIL GBC

ABOUT REDHAT

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

LEARN MORE

ABOUT INTEL

Intel, a world leader in silicon innovation, develops technologies and initiatives to advance how people work and live. Second-generation Intel Xeon Scalable processors with Intel Optane DC persistent memory form the reference design platform for SAP HANA. It delivers optimal performance, security, flexibility, and total cost of ownership to meet today's data center needs. Make better business decisions faster with an intelligent data management strategy from Intel and SAP.

ENDNOTES

1. https://www.dhs.gov/obim

2. https://www.dhs.gov/science-and-technology/BI-TC

3. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

4. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence-1

5. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_technology_guide.pdf Council of Foreign Relations. “The Overlooked Military Implications of the 5G Debate.” April 25, 2019. https://www.cfr.org/blog/overlooked-military-implications-5g-debate

6. https://www.nextgov.com/cio-briefing/2020/07/cbps-outgoing-biometrics-lead-law-enforcement-use-facial-recognition/166629/

7. https://www.nextgov.com/it-modernization/2020/05/homeland-securitys-biometrics-database-its-way-amazon-cloud/165186/

8. https://www.nist.gov/industry-impacts/biometric-standards-law-enforcement

9. https://www.justice.gov/doj/page/file/1246466/download/

10. https://www.dhs.gov/biometrics

11. https://www.dhs.gov/sites/default/files/publications/final_hsac_biometrics_subcommittee_report_11-12-2020.pdf

12. https://www.fedscoop.com/dhs-biometrics-system-privacy-risks/

13. https://iapp.org/news/a/u-s-facial-recognition-roundup/