FEDERAL IDENTITY LEARNING AGENDA: OUTCOMES FROM THE 2021 FEDID CONFERENCE

By Ben Smith and Duane Blackburn

The federal government has relied upon accurate identity management for a long time—arguably since the first-ever tax on personal income was implemented during the Civil War. Over the last thirty years, however, it has become a fundamental aspect of numerous federal programs, with foci ranging from terrorist identification to enhancing customer experience in citizens' interactions with federal agencies.

Interagency coordination began in earnest in the mid-1990s when the Biometrics Consortium was chartered within the National Security Council (NSC) infrastructure "to serve as a Government focal point for research, development, test, evaluation, and application of biometric-based personal identification/authentication technology." This charter formally expired with early actions taken in the subsequent Bush administration, with the Biometrics Consortium reconfigured as the government's annual identity conference (now known as the Federal Identity Forum, or FedID).

Immediately after the terrorist attacks on 9/11, enhanced identity capabilities soared to the forefront of federal priorities. The National Science and Technology Council (NSTC) established a Subcommittee on Biometrics and Identity Management, which subsequently served as a central coordinating activity for federal identity activities for nearly a decade. This Subcommittee:[1]

- Coordinated federal research, development, test, and evaluation activities by the federal government, including issuing "Challenge" documents in 2006[2] and 2011[3] to serve as governmentwide policy and as a mechanism to drive discussion and collaboration with non-government entities on priority community needs;
- Coordinated federal agency participation in national standards development bodies, and the United States' position in international standards bodies;
- Issued an NSTC policy that established a federal registry of standards,[4] which federal agencies were required to use in their systems;
- Collaborated with federal Privacy Officers to refine the use of Privacy Impact Assessments as a means to assess and mitigate privacy impacts on planned and in-use federal identity systems;

- Coordinated interagency data sharing and interoperability policies among federal systems protecting the nation from known and suspected terrorists (note that this activity was later transferred to the NSC);
- Developed a Glossary of biometric and other identity terms,[5] and mandated that agencies follow it, so that federal government communications on this new technology would be consistent;
- Absorbed the Biometric Consortium into its activities; and
- Published introductory-level documents that explained biometric technologies, issues, applications, and federal programs to the general public.[6]

This Subcommittee expired roughly ten years ago and there has not been similar Executive Office of the President–led coordination in the ensuing time. But that does not mean that interagency coordination has ceased![7] The interagency still gathers throughout the year to exchange information and provide mutual mentoring, and FedID continues with an annual conference and occasional special activities (such as developing the document Biometric Face Recognition: References for Policymakers in December of 2020[8]).

This document follows in the tradition of the NSTC's prior Challenge documents, with the concept now commonly referred to as a Learning Agenda. The goal is to focus the FedID community on overcoming priority issues or capability gaps. There are two key differences in this document to keep in mind:

1. Unlike prior Challenge documents, this document is not formal federal government policy. It is intended to be an unofficial, yet hopefully helpful, guide.
2. This document similarly was not developed through a formal interagency process led by the White House. Instead, it is based on presentations and attendee discussions during the 2021 FedID conference, which the interagency purposefully designed so that the community could benefit from this document. It has not been formally reviewed or approved by federal agencies.

The remainder of the document highlights three areas of primary concern raised during FedID 2021. This is most certainly not an exhaustive list of important issues for the FedID community but is nonetheless a positive step in helping the community coalesce around a set of modern issues that needs prioritized attention. Each section has introductory text, example federal activities, and a series of questions that need community attention.

Identity Proofing/Fraud Prevention

Discussion

The COVID-19 pandemic has spotlighted known, but often unprioritized, identity challenges within government benefit programs and has accelerated the need for both robust remote and in-person contactless identity proofing schemes to assure identity and reduce fraud. The Small Business Administration (SBA) issued more than $1 trillion in loans in 2020, up from a normal average of $25–30 billion. Geofencing was used to evaluate traffic on the SBA website and detected an unusual number of overseas visitors, indicating potential fraudulent claims. Identity theft related to government benefits rose nearly 3,000% last year. Artificial Intelligence (AI) is being used to spoof voice and video to facilitate fraud, money laundering, and the spread of disinformation. The Joint Financial Management Improvement Program estimated

that the federal government paid out $206 billion in improper payments in 2020 and expects to see a significant rise in 2021.

The federal government has attempted to implement federated digital identity solutions a couple of times with limited success—e-authentication, FICAM—but differing security needs led to difficulties in developing a solution that is both robust enough to serve these diverse needs while being lightweight enough to be usable. Federation requires strong policy backing to guarantee the right of use for credentials while also strongly protecting individuals' privacy.

Example Federal Activities

Department of Health and Human Services has implemented the XMS external user management system, which uses credential service providers (login.gov, ID.me, etc.) to ensure compliance with the National Institute of Standards and Technology (NIST) 800-63-3 standards. It is not currently capable of credentialing/ID proofing international users, but it is on the roadmap.

The Internal Revenue Service has rolled out the 800-63-3–compliant Secure Access Digital Identity platform for identity proofing of taxpayer access to financial services.

The Census Bureau has been identified as a model for other government agencies fighting mis- and disinformation online following its rollout of rumors@census.gov. The commitment to privacy and confidentiality is a legal obligation and a core component of Census' institutional culture and includes consideration of future privacy threats to citizen data. After discovering that statistics released about the 2010 Census may allow for reconstruction of individual records, the Census Bureau instituted a disclosure avoidance protocol for future data releases. This makes re-identification and reconstruction more difficult by reducing precision, removing vulnerable records, or adding uncertainty to the data (aka differential privacy).

Questions and Issues for Priority Attention

1. What countermeasures are being developed, or need to be developed, to mitigate AI-facilitated fraud and money laundering?
2. How can we strengthen remote identity proofing to reduce fraud in finance, voting, etc.?
3. Can the Social Security Number be converted into a digital identity credential that can be used across service channels to create a seamless taxpayer/citizen experience with greater security against fraud?
4. Can we develop a lightweight trust framework that serves the needs of diverse customers and organizations in a federated environment?
5. Can the federal government implement a system to leverage state databases to authenticate digital ID?
6. Multiple groups have developed digital vaccination cards with varying levels of interoperability. How can the community converge these initiatives to create a universally accepted, verifiable health information approach that benefits patients without raising privacy concerns?
7. Further R&D is needed with regard to federated identity across federal government programs, to include appropriate/strong security and privacy protection.

DoD, Intelligence, Homeland Security, and Law Enforcement

Discussion

This domain has been the primary focus for the FedID community for twenty years, resulting in many substantial impacts on national

security programs. Even with these successes, priority needs remain, including modernizing applications to better ensure privacy and equitable outcomes.

Example Federal Activities

Biometrics in Multi-Domain Operations (MDO). In recent years, joint requirements to counter irregular threat networks in Iraq, Afghanistan, and Syria drove joint forces to employ biometrics and complementary forensic capabilities to enable the identification of insurgents and terrorists. While biometrics has been a critical enabling capability for countering irregular threats during recent campaigns, its inherent versatility provides Army forces with a combat-proven capability that can contribute to friendly forces gaining information advantage over competitors and their proxies during MDO on the future battlefield. Biometrics contributes to maneuver forces' continuous operational preparation of the environment by providing commanders with critical biometric data that promotes their situational understanding of adversaries during competition and enemies during armed conflict. Biometrics also enables cross-domain reconnaissance and security by enhancing sensing and identification of threats while distinguishing threats from friendly and neutral personnel and forces. Lastly, biometrics enhances the accuracy and precision of targeting in complex environments, such as dense urban areas, during cross-domain maneuvers in large scale combat operations.

Biometrics Automated Toolset – Army. A handheld device used to collect, process, and reference multimodal (face, finger, iris, voice) biometric information, which enables matching in five minutes or less; seeking to improve to three minutes or less. The Biometrics Interoperability and Standards Compliance Office has developed a mobile app and a capture app that have passed Joint Interoperability Test Command testing. The mobile app is Android-based and integrates face, finger, and iris biometrics. The capture app is government off-the-shelf, web-based enrollment software that allows the use of nearly any local or remote finger, face, and iris sensors. There are current pilot programs for an SUV-mounted (incognito) 2D/3D LIDAR face detection and an RFID biometric access card in which the RFID chip does not transmit until biometric information stored on the card is verified. Other efforts include data cleansing, deduplication of biometric data, identification of biometric anomalies, and an integrated biometrics palm scanner.

Homeland Security Investigations – War Crimes Hunter. A system is designed to capture media depicting human rights violations being posted online, identify the perpetrators in the media, and prevent their entry into the United States. The War Crimes Hunter system and other HSI Innovation Lab activities have led to improved investigative outcomes and significant time savings on manual data entry. War Crimes Hunter scrapes websites for war criminal activities, detects and clusters faces from the collected media, formats faces of individuals of interest into packages using standard schemas, and exports formatted face packages to U.S. government partner forensic labs for identification and further information sharing.

Department of Justice's Next Generation Identification (NGI). This service recently completed an eight-year pilot to collect iris images with other biometric data during prison intake procedures. The program has been endorsed by the FBI director and Criminal Justice Information Services (CJIS) Advisory Policy Board to move to full-scale implementation. Four states are currently qualified to submit iris images to the NGI database, and more are coming online

as they acquire the necessary technology to participate, which includes a near-infrared camera and software required to connect the iris and fingerprint records. The National Palm Print System, also part of NGI, is matching palm prints with existing tenprint records. Forty-nine states, two territories, and the District of Columbia are participating, with more than 50 million images currently in the database.

Questions and Issues for Priority Attention

1. How does the intelligence community assure identity to ensure proper data organization/ flow – i.e., providing or getting to the right data at the right time in a constantly-changing operational environment?
2. What initiatives exist or are being considered to develop military and civilian biometric experts at echelon in the Army and other services?
3. What other identity technologies can support the warfighter in urban environments?
4. How do entities share information to ensure a single identity is not committing fraud across different agencies, states, etc.?
5. Further research is needed on the exploitation of multimedia data ("digital exhaust") and behavioral biometrics.
6. How do we ensure interoperability of fingerprint images from new contactless collection devices with legacy databases?
7. How do we modernize biometric-based programs to accommodate evolving concepts and best practices with respect to privacy and civil liberties?

Face Recognition

Discussion

Face recognition (also referred to as facial recognition) is receiving substantial attention by legislators and policymakers throughout the country, fueled in part by advocates that would like to see the technology banned. By its very nature, face recognition will never exist without legitimate associated concerns, so its use must include the appropriate safeguards and strong privacy protections from the beginning. It is clear that the community must enhance and mature its activities in this regard.

Unfortunately, much of the current legislative and policy analyses will not help the community advance towards that goal as they're driven not by data and evidence-based analysis, but rather on misguided assumptions of their capabilities and Hollywood-inspired visions of operational systems that use them. Common issues within written analyses include inaccurately conflating face recognition with facial analytics technologies, technical bias with prejudicial bias, algorithm performance with how systems function in practice, and operational process errors with the core technology, along with a failure to recognize the breadth and depth of existing technical and operational analyses, policies, and best practices. As the Center for Strategic & International Studies recently remarked, the "level of confusion and misinformation in the FRT [face recognition technology] discussion is astounding."[9]

Face recognition, like all biometrics, is inherently probabilistic.[10] No algorithm can be completely accurate,[11] nor have a complete lack of differential performance across demographic groups (such as gender, race, or age).[12] But face recognition algorithm capabilities surpassed that of non-expert

humans many years ago and the accuracy rates for top algorithms are extremely impressive, with error rates continuing to be halved roughly every three years. Measured differential performance is also falling, with some identification algorithms having undetectable false positive differentials.[13] There is, however, great variance across different algorithms on both overall accuracy and differential performance (particularly on race). While some algorithms exhibited undetectable differences, others were very much detectable and concerning—highlighting a need for both enhanced development of those algorithms and studious selection of algorithms for use in operational systems. It is important to note that U.S. government agencies closely monitor the results of the NIST Face Recognition Vendor Tests (FRVT) to help them select algorithms for further analysis in advance of potential operational use.

Example Federal Activities

U.S. Customs and Border Protection (CBP). DHS has a legal mandate to biometrically record all foreign nationals who enter and exit the United States. Years of testing have demonstrated that biometric facial comparison technology is the most secure, efficient, and cost-effective way to fulfill the Congressional mandate while protecting the privacy of all travelers. CBP built a highly accurate, cloud-based facial biometric matching system—the Traveler Verification Service (TVS)—that supports Entry/Exit operations at air, land, and sea. CBP can offer "identity as a service" to its air travel partners and the Transportation Security Administration wherever traveler identity verification is required throughout the air travel journey such as check in, bag drop, security checkpoint, and boarding to further secure and streamline travel and support the travel recovery efforts. U.S. citizens can voluntarily participate in the biometric facial comparison process, and their photos are deleted within 12 hours. To date, CBP has processed more than 100 million passengers using facial biometrics, detected over 117,000 visa overstays, and prevented almost 1,000 impostors from entry to the United States. Building off the success of its air travel innovation efforts, CBP has implemented facial biometrics in the debarkation process in partnership with the major cruise lines and deployed a 1:1 facial biometric program in pedestrian lanes at select land borders.

FBI/CJIS' Interstate Photo System and Face Operation Service. All local, state, and federal law enforcement programs are eligible to access this system, provided they agree to abide by the program's policies (Fourth Amendment protections, sharing and storage restrictions, etc.) and are trained to use the system. Results are not to be used for positive identification, but for leads in context with other evidence. Face Operation Service is aimed at FBI special agents involved in FBI investigations and carries the same policies as IPS. It is interoperable with other federal agencies and their photo repositories.

Department of Defense (DoD) Automated Biometric Identification System. This system processes and stores multimodal biometric information from various collection assets, matches new biometric inputs against shared data, and shares information with approved partners in the DoD, interagency, and international partners. DoD is also developing long-range (70–200 meters) face technology and long-range thermal recognition to about 500 meters.

Questions and Issues for Priority Attention

1. How do we continue to enhance the accuracy of face recognition algorithms, while also minimizing performance differentials?
2. How can AI help identify and correct record crosslinking (i.e., biometrics of one individual being added erroneously to the record of another)?

3. How do we protect against facial morphing and other presentation attacks designed to defeat face recognition algorithms?
4. How can we best educate legislators, policymakers, key stakeholders, and the general public on the appropriate use of face recognition technologies, applications, and potential benefits and issues, so that the needed debate can become evidence-based and productive?
5. Research is needed to enable potential end users to more maturely establish performance requirements (such as overall accuracy and tolerable levels of differential performance) for specific applications and to implement safeguards to identify and mitigate errors.

About the Authors

Ben Smith is Manager of Homeland Security at AFCEA, which provides a forum for military, government and industry communities to collaborate so that technology and strategy align with the needs of those who serve. Mr. Smith manages several defense, national security, and technology events while also overseeing AFCEA's Cyber and Homeland Security Committees.

Duane Blackburn leads science and technology policy for MITRE's Center for Data-Driven Policy, which brings objective, evidence-based, nonpartisan insights to government policymaking. Mr. Blackburn previously served for eight years (across two administrations) in the White House Office of Science and Technology Policy (OSTP), with identity being one of his portfolios.

For more information about this paper or the Center for Data-Driven Policy, contact policy@mitre.org.

References

[1] Biometrics in Government Post-9/11. 2008. National Science and Technology Council, https://www.hsdl.org/?view&did=235185.

[2] The National Biometrics Challenge. 2006. National Science and Technology Council, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/biometrics_challenge_document.pdf.

[3] The National Biometrics Challenge. 2011. National Science and Technology Council, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/biometricschallenge2011.pdf.

[4] NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards. September 2007. White House Office of Science and Technology Policy, https://www.nist.gov/system/files/documents/2017/04/12/nstc_policy_bio_standards.pdf.

[5] Biometrics Glossary. September 2006. White House Office of Science and Technology Policy, https://web.archive.org/web/20161220230838/http://biometrics.gov/Documents/Glossary.pdf.

[6] Biometrics "Foundation Documents." September 2006. White House Office of Science and Technology Policy, https://apps.dtic.mil/sti/pdfs/ADA505048.pdf.

[7] Activities on specific issues have continued, such as the CIO Council's work on ICAM and the NSC's work supporting terrorist identification. The Office of Science and Technology Policy also recently released a Request for Information on Public and Private Sector Uses of Biometric Technologies, focusing predominantly on equity issues. More information is available at https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies.

[8] Biometric Face Recognition: References for Policymakers. December 2020. FedID, https://www.mitre.org/sites/default/files/publications/biometric-face-recognition-references-for-policymakers.pdf.

[9] J. Lewis and W. Crumpler, Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape. 2021. Center for Strategic & International Studies, https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape.

[10] Biometric Recognition: Challenges and Opportunities. 2010. National Academies Press, https://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities.

[11] While evaluation results can approach 100% in some test protocols, statistically there is still margin for error, however small.

[12] It is not statistically possible to test to a "zero" error rate. One can approach zero, with the closeness limited by statistical significance measures within the test protocol.

[13] P. Grother, M. Ngan, and K. Hanaoka. FRVT Part 3: Demographic Effects. 2019. National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.