

August 2015

Shaping the Strategic Landscape on Technology for the National Security Enterprise

Scott Aughenbaugh

This paper and the discussions that provided input to it were made possible by the generous support of Safran USA.

Executive Summary

In the spring of 2015, the Center for Strategic and International Studies (CSIS) hosted a roundtable discussion with key subject-matter experts to develop practical, actionable recommendations for ways to shape the future of biometric and identity intelligence in the security landscape. Against the backdrop of a changing security landscape, the group exchanged views on some of the key challenges that leaders must address when considering the future role of biometrics and identity intelligence in security. Roundtable participants discussed the future of American security and intelligence capabilities and how biometrics is poised to evolve. Participants also explored ways in which the U.S. government could leverage this technology and where there might be opportunities that have not yet been realized. Participants discussed what privacy concerns and individual rights policymakers should consider when looking at adopting future biometric approaches. This paper outlines several recommendations for steps that leaders can take to shape the future security landscape of identity intelligence including: (1) expand use of biometrics to improve cybersecurity through multimodal systems and incentivize private use; (2) develop practical ways to increase information sharing; (3) build a robust strategy for biometrics within the Department of Homeland Security to link multimodal biometric authentication in the face of new cyber challenges; (4) consider changes to contract vehicles and experiment with new acquisition models or risk severely outdated legacy architectures at a time of declining budgets; and (5) recognize the value of software as a service (SaaS), commercial off-the-shelf (COTS), and cloud-enabled systems as possible standard bearers going forward.

Introduction

While it is common to start security-related discussions at 9/11, biometrics as a concept dates back over a millennium as we have sought out ways to link someone's physical and behavioral characteristics to an object, such as using fingerprints for business transactions and marking our work. The development of modern systems in the twentieth century generally improved as

Moore's Law continually shrunk computers and sensor systems over the last 40 years and greatly improved their performance. For example, we extended beyond automation of fingerprint identification into new modalities of face, palm, iris, voice, and DNA in the 1990s alone.¹

Since then, there has been a great deal of interest in using biometrics to verify identity. Given that biometrics are bound to an individual, they are seen as being more reliable and not as easily lost, stolen, falsified, or guessed, making them more secure than other identity verification systems. Due to their security, speed, efficiency, and convenience, biometric authentication systems will continue to be incorporated into standards for access control. We have used these methods to augment security screenings with systems like TSA Pre✓® and add new layers of verification to important government ID systems. Thus the proliferation of technology over the last 30 years has provided new opportunities to use biometrics and identity intelligence in countering terrorism, fighting crime, preventing welfare fraud, and enhancing physical and logical access security.

Biometric and identity intelligence will continue to be a component of security; however, the government and general public are at a point of uneven adoption and knowledge of these new technologies. Historically, as you look at adoption, the market penetration rate has increased with many major new technologies in the United States—as certainly was the case in the movement from mobile phones to smart phones.² Today sensors and software applications are installed in every large U.S. federal agency, yet leadership is having trouble convincing their organizations of the systems' effectiveness, creating challenges to new deployments and hampering the understanding of the abilities of newer systems. As an example, in the course of our discussions some senior officials were unaware that the time scale for DNA matching, which was used to track down two escaped convicts to a cabin in June 2015, had gone from weeks to days and hours.³

The general public understanding of biometrics is also continuing to evolve as new commercial off-the-shelf hardware technologies from traditional providers like Microsoft and Apple are extending other opportunities in identity management that will make biometrics more commonplace. Standard versions of software, like the recently released Microsoft Windows 10, will include a native option for using one's face, fingerprint, or iris to log in to the operating system or web applications. As a result, the public user base will continue to have new and significant interactions with these systems and the increased privacy and security they may provide. Will this increase our level of confidence in technology while at the same time increasing the number of future risks?

¹ National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, "The History of Biometrics," August 7, 2006, <http://www.biometrics.gov/documents/biohistory.pdf>.

² Andrew Hunter and Ryan Crotty, *Keeping the Technological Edge: Leveraging Outside Innovation to Sustain the Department of Defense's Technological Advantage* (Washington, DC: CSIS, June 2015), 5, http://csis.org/files/attachments/150626_tech_edge_report.pdf.

³ Susanne Craig and Andy Newman, "DNA Matching 2 Escapees Is Found in Cabin 15 Miles from Prison," *New York Times*, June 22, 2015, <http://www.nytimes.com/2015/06/23/nyregion/escaped-convicts-manhunt-new-york.html>.

As we consider these perspectives, the question of what the future landscape of biometrics and identity intelligence will look like becomes more pertinent. The once-segmented industry continues to consolidate, and large system integrators will divest the staff devoted to this technology due to flattening budgets and commoditization. At the same time, over the next decade, there will be an explosion of growth in the use of biometrics information in the commercial and personal sectors as it is increasingly incorporated into off-the-shelf technology. This also has the potential to supplement the use of the traditional modalities of face, fingerprint, iris, palm, and voice with a suite of new modalities such as Rapid DNA, vein, gait, and ear. Will new biometrics continue to evolve in the U.S. government in the same way? Will the legal, political, and resource framework on how to deploy them still lag behind?

Key Challenges

Biometric technologies have substantial potential for improving security by providing a means to identify and verify people in many different contexts. However, the implementation of biometric technologies for increasing national security raises numerous practical and policy questions. There is legitimate public concern that biometric technology can be misused to invade or violate personal privacy or other civil liberties. Some important questions to consider included: How can we improve database connections and the network security? Can biometric systems be narrowly tailored to their tasks? Who will oversee the programs? How will consistency between data collected be controlled? How can we fit commercial advances to government needs if it is hard to share publicly or develop clear technology requirements? In discussing these questions, CSIS roundtable participants generally believed that there are three overarching challenges that will need to be addressed:

1. *Collection and database interoperability:* In the current security landscape, the threshold for data quality and retention varies substantially across not only different agencies but also different departments. As a result, the ability to coordinate a consistent strategy is not only more complex, but an impractical option. The multiplicity of digital systems for sharing templates not only complicates data access across agencies, but also internationally. As a result, a gap exists in data and information sharing due to the federated nature of our systems. Currently there are mechanisms and bodies that attempt to obtain consensus on data standards and transmission, such as the American National Standards Institute and National Institute of Standards and Technology. However, many of the systems for transferring the files have yet to move beyond manual file transfer protocol (FTP) websites. In order to take better advantage of current and future biometric/biographical data to enhance security, the connections between databases will need to be updated and better organized to resolve conflicts between systems of record and avoid pertinent information falling through the cracks generating false positives or negatives. Furthermore, as security becomes more reliant on digital information, data sharing will require enhanced protection creating new questions of how the data will be managed.

2. *No strategy and resource allocation alignment:* Government has historically been known for its inability to change policy due to advancements in technology. However, in order to take full advantage of the possibilities that biometrics can offer, it is important to identify the strategic importance of biometrics. The technology is available, but the legal, political, and resource framework on how to deploy and implement in many of the current concepts of operations (CONOPS) is lagging behind. Furthermore, there needs to be a better unity of effort not just between departments, but also between government and private companies. Currently, there is a gap between funding and what is expected from the technology. To complicate matters even more, the requirements for technology are hard to share in some instances, making it difficult for the commercial sector to develop in a space that is not well defined. Companies are not only dealing with a lack of funding but also tasked with creating a product without clear requirements. Given that more of the expertise in this field is moving toward the commercial sector and away from government, government needs to take better advantage of using commercial advances and manipulating them to fit their own needs.
3. *Public mistrust:* With biometric collection becoming more convenient as technology advances, there needs to be a better dialogue between government and the public. As new advancements in technology become commercially available we need to be more proactive in both demonstrating the experience and explaining what will be collected and retained. Will they be more likely to accept biometrics when it affects their everyday life, such as in more secure banking or faster screening? What indicators are we willing to share? A number of surveys suggest a majority of citizens in the United States, and in key ally countries, are willing to share biometric information if we can improve our processing for travel and border crossings making life more convenient and secure.⁴ Discussions of trust are an important debate in society, with fears of an obtrusive government over-stepping its bounds, but we should focus our attention on the commercial devices that will be our biometric interfaces and make sure they are properly protected. As an example, at the August 2015 Black Hat Conference, FireEye researchers released a paper detailing how devices like the HTC One Max were improperly storing fingerprints.⁵ The perception of convenience vs. intrusiveness will play a key role in how accepting the public will be when it comes to offering up biometric data.
4. *Contract vehicles and acquisition:* U.S. government contract vehicles and acquisition processes are likely outdated for this field. As sensors have become cheaper, the software, platforms, and computing times have become more important, and they are being constantly updated. As a result, the commercial sector has made major advances in cloud-based and SaaS models, and for all the interest they receive from the U.S. government, they find it hard to execute agreements. When new systems are combined with a lack of clear strategy and requirements it can be almost impossible to procure. New models have the potential to help lower upfront

⁴ Accenture, "Accenture Research Shows Citizen Support for Biometrics to Facilitate Travel and Secure Borders," Press Release, June 24, 2014, <https://newsroom.accenture.com/news/accenture-research-shows-citizen-support-for-use-of-biometrics-to-facilitate-travel-and-secure-borders.htm>.

⁵ Yulong Zhang, Zhao Feng Chen, Hui Xue, and Tao Wei, "Fingerprints on Mobile Devices: Abusing and Leaking," BlackHat.com, August 2015, <https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf>.

program costs and keep systems robust, yet government contracting agents may view them suspiciously and believe they carry undue risks.

5. *Privacy versus security*: While there are advantages to using these biometric systems as part of a cyber or insider threat strategy, there are certainly concerns about privacy and irreparable data theft. Some argue that once information is stolen, it cannot be retrieved if databases or transmissions are not properly protected, or that the data can be spoofed to present false positives using basic hacks like imprints on Scotch tape or 3D molds filled with Play-Doh that are accepted for fingerprint authentication.⁶ It is certainly true that we will always be continually pushed to improve biometric storage by the next generation of cyber thieves, as illustrated by the fact that 1.1 million fingerprint records were compromised in the recent OPM breach.⁷ While it is unclear how the OPM hackers may use this data going forward, this theft does solidify the need to begin moving toward adopting multimodal systems that also weigh the liveness of the record in its detection going forward.

Recommendations and Conclusion

The U.S. budget will be a constraining factor in the next decade. The United States has always had drawdowns after major conflicts and current trends lead to long-term pressure on discretionary spending.⁸ How we use our dollars in a fiscally constrained world will not be without risk or controversy, yet one thing is clear: the amount of people, packages, and interactions to track will continue to increase, thereby making our understanding of identity a very valuable commodity.

Groups over the years have recognized the value of identity intelligence and have issued recommendations for action that still needs to be executed, like the development and implementation of a biometric exit program to complement our entry system. Rather than dwell on the challenges of the past, the individuals consulted for this document came up with five recommendations for the future leadership of the national security enterprise.

1. *Expand the use of biometrics to improve cybersecurity*: Cybersecurity needs to move beyond network security and into biometrics. Our current authentication systems are broken, and more complex passwords are not a long-term solution. The government, as well as the commercial sector, must adopt multimodal biometrics. Now is the time to engage with the private sector to ensure that they use new government standards to improve interoperability. How can the government incentivize industry use of biometrics to improve cybersecurity? Is there a way to connect non-security biometric efforts from the private sector?

⁶ Ana F. Sequeira and Jaime S. Cardoso, "Fingerprint Liveness Detection in the Presence of Capable Intruders," *Sensors* 15, no. 6 (June 2015): 14616–17, <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4507655/>.

⁷ U.S. Office of Personnel Management (OPM), "OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats," News Release, July 9, 2015, <https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/>.

⁸ Clark Murdock, Ryan Crotty, and Angela Weaver, *Building the 2021 Affordable Military* (Washington, DC: CSIS, June 2014), 3–4, http://csis.org/files/publication/140625_Murdock_Building2021Military_Web.pdf.

2. *Increase information sharing:* The policy community should develop practical ways to increase information sharing among federal and state authorities and continue to improve partnerships internationally. While information has certainly improved over the years, it is still plagued with ownership challenges. We should focus not just on storing data for the unknown malefactor or future threat actors, but also seek to leverage information more effectively on “good guys” to improve security flows while still protecting their privacy, because biographical data alone is not enough. With more digital references and new ways to compute biometric templates, one-to-one authentication models can begin to move toward one-to-many identification that can improve their accuracy.⁹ We should certainly expand our partnerships with Canada and assist in the efforts of our traditional European allies using fingerprints and facial recognition to create smart borders. How do we plan to work with emerging allies in this space?
3. *Build a biometrics strategy:* The national and homeland security enterprise should construct a 5- to 10-year biometrics strategy building on the cross department and agency work done by the National Science and Technology Council (NSTC). While biometrics was not specially mentioned in the 2014 Quadrennial Homeland Security Review (QHSR), many of the programs that rely upon it were discussed as part of “risk informed, intelligence-driven approaches.”¹⁰ As these systems become more important for air travel, border crossings, and other functions at DHS, it is important that they strategize an implementation plan and an impact statement for the next 5 to 10 years. Which programs and CONOPS will be essential for the future DHS mission? How can we leverage the expertise of DHS Science and Technology, National Protection and Programs Directorate, Customs and Border Patrol, and DHS Policy to create a better research, development, test, and evaluation (RDT&E) environment to maximize the value of new technology trials, such as the Apex Air Entry and Exit Re-engineering (AEER) pilot?¹¹
4. *Innovate and encourage agile procurement models:* As much of the research and development continues to be done in the private sector, new models will be needed to ensure quality of competition in a recognized time of declining budgets. While there are many examples out there, new practices and knowledge can be a “needle in a haystack exercise” across government without the proper department paperwork available for new methods. There will be a premium put on the need to create on and off ramps, public-private partnerships, and multi-award indefinite delivery, indefinite quality (IDIQ) contracts to increase competition for task orders. The private sector has been experimenting with successful new ideas that have been implemented, such as Amazon’s work with the intelligence community, but that experience was not without controversy.¹²

⁹ National Institute of Standards and Technology (NIST), “NIST: Performance of Facial Recognition Continues to Improve,” June 3, 2014, <http://www.nist.gov/itl/iad/face-060314.cfm>.

¹⁰ U.S. Department of Homeland Security (DHS), *The 2014 Quadrennial Homeland Security Review* (Washington, DC: DHS, 2014), 35, <http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>.

¹¹ U.S. Department of Homeland Security, “Apex AEER Program,” <http://www.dhs.gov/science-and-technology/apex-aeer>.

¹² Frank Konkel, “The Details about the CIA’s Deal with Amazon,” *Atlantic*, July 17, 2014, <http://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/>.

Can we keep the technology innovative and fresh with the option to fail fast or will we risk outdated architectures at a time of declining budgets?

5. *Recognize the value of SaaS, COTS, and cloud-enabled biometrics:* These systems will be the standard bearers of information sharing and security going forward. Technology and industry are going through a major revolution that will help the acquisition of more functional and resilient systems in the future, making the jump to and cost of systems more attractive. As consumer devices like the Apple iPhone add fingerprint scanning and other biometric capabilities, the focus should shift to enabling their innovation and better coordination with private companies for the benefit of government systems. While there certainly will be attempts to extend the life of legacy systems over the next decade, dwindling resources will be too big an issue to keep this up forever and relative performance will suffer.¹³

While there will be challenges to implementing any changes in government, these practical recommendations will put us on a path to navigate both old and new areas of identity intelligence. Having better information sharing, strategy, cybersecurity, acquisition models, and faster ways to acquire technology will improve the future security environment for an enterprise looking to regroup after Iraq, Afghanistan, and the continual risk of international and domestic threats. While the challenges of privacy and public mistrust are unlikely to be solved overnight, one of the senior participants suggested the need for a new public/private commission on how to fix data collection and sharing. While more dialogue certainly will help, we should continue to be open with the general public on the nature of the challenges we face globally and the need for these systems in the domestic space to improve public understanding and acceptance.

Scott Aughenbaugh is a fellow with the International Security Program at the Center for Strategic and International Studies in Washington, D.C.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2015 by the Center for Strategic and International Studies. All rights reserved.

¹³ The Office of Biometric Identity Management (OBIM) did attempt something similar on “current and near future technologies, including mature modifiable COTS products” with a request for information (RFI) on November 6, 2014, https://www.fbo.gov/index?s=opportunity&mode=form&id=e0878cc1367eddf7c8863447c779aad3&tab=core&_cview=1.