BURNS McDONNELL

WHITE PAPER

Six Critical Questions to Consider When Incorporating Biometrics Into Airport Passenger Facilitation

By Todd Shutts and Mike Zoia

A world in which airline passengers can walk through security checkpoints and board flights using only their faces as identification may be closer than some might think. Biometric identification systems not only improve airport security by verifying passenger identities, but also make seamless passenger journeys possible by bringing exponential improvements to the travel experience.

Biometric ID programs have the potential to revolutionize passenger facilitation globally. They make a seamless travel experience possible, empowering passengers to check-in, drop checked bags, pass through security checkpoints, board planes and, in the case of international flights, clear customs without showing a physical ID or boarding pass, resulting in reduced queue times.

For many airports, airlines and other aviation industry stakeholders, the benefits of automating repetitious passenger identification checks are counterbalanced by concerns for protecting passenger privacy. The technology certainly is on the industry's radar: In 2018, 77% of airports and 71% of airlines said they were planning major programs or research-and-development initiatives during the coming three years involving biometric identification management, according to SITA, a firm that provides tech services for the industry.

As all stakeholders consider options and decide next steps, there are critical questions each one must consider.

Is a biometric ID program worth the investment?

Think of biometrics as an enabling technology. In its most basic form, it involves installing LAN or Wi-Fi-networked cameras that capture digital images of passengers and send them to the Traveler Verification Service (TVS), which is the biometric matching service of U.S. Customers and Border Protection (CBP). The service compares the new photo with Department of Homeland Security (DHS) holdings. These biometric systems also integrate with airline reservation and departure control systems through network interfaces or serial connections. Software typically includes a computer vision component that uses machine learning, such as a convolutional neural network and data management. Beyond that, airports and constituent stakeholders have a variety of

additional layers of technology that can be added to create additional value, improve the passenger experience and achieve greater returns on investment.

Currently, most U.S. airports with biometric ID systems use them to comply with CBP requirements for capturing photos of international passengers arriving or departing on international flights. CBP rules do not currently allow private parties to retain these images for their own business purposes.

Consumer privacy and regulatory compliance must be top of mind for airports and airlines who plan to scale biometric initiatives beyond border management applications. Privacy by design and cybersecurity best practices are critical when evaluating biometric use cases across an airport campus. But there are ways to extend secure biometric practices into other use cases on the airport campus. Technologies already exist that make it possible to not only automate various passenger touchpoints, such as TSA boarding pass, ID check, bag drop and self-boarding, but to also share passengers' digital information along the many steps of the travel journey.

Beyond meeting regulatory compliance, what are other ways airport operators are beginning to apply biometric technologies?

Airports around the world are seeking to answer that very question through a series of tests and full-scale biometric ID system deployments. A facial biometrics system undergoing trials at the Madrid airport, for example, enables travelers to identify themselves at both security control and boarding gates with their biometric profile, eliminating the need to present travel documents. At Los Angeles International Airport, a biometric program is being deployed as part of a new self-boarding process. Using biometric identification, it is possible for the airline's departure control system to make a boarding decision regarding a particular flight and a given passenger without reviewing an ID.

In late 2019, Delta Air Lines went a step further, introducing the U.S.'s first completely biometric terminal at Hartsfield-Jackson Atlanta International Airport. There, passengers flying Delta direct to international destinations now have the option of using facial biometrics technology as their ID from the curb to the gate. As with the other examples, the long-term goal is a seamless passenger journey from the moment they enter the airport campus to the moment they leave following their return flight. By linking mobile loyalty apps, the digital data collected might someday allow passengers to automatically order their favorite drink at an airport coffee shop upon arrival or have a ride awaiting them after retrieving their checked luggage.

Other boundary-pushing efforts could include using biometrics to improve the physical security of an airport's landside operations or to ease parking congestion. Biometrics technologies could also play a role in future irregular operations (IROPS) by helping redirect passengers impacted by flight delays and cancellations that have a ripple effect across airports. Biometrics plays a key role in support of several U.N. Sustainable Development Goals such as Good Health and Wellbeing, Industries, Innovation and Infrastructure, Peace, Justice and Strong Institutions and Partnerships for the Goals. Two primary examples are using biometrics to combat human trafficking and to curb the spread of infectious diseases.

Should airport operators wait until the industry agrees upon a single, global biometric ID standard?

There are currently initiatives underway to create such a standard, including the International Air Transport Association (IATA) One ID, International Civil Aviation Organization Traveler Identification Program (ICAO TRIP) and World Economic Forum Known Traveler Digital Identity (KTDI), among others.

Still, the majority of today's airport biometric programs are being developed in relative isolation. One airline might choose to develop a system that aligns with its concept of operations, boarding procedures and other standard procedures. Another airline in the same airport could, in theory, take a different approach that more accurately reflects its own procedures. Depending on the exact use case and the airport's governance model, those programs could operate independently of the biometric ID program the airport operates to comply with CBP regulations or other international mandates.

This is possible because no universal standards currently exist for data collection, management, ownership or sharing for nongovernmental, passenger convenience-driven biometrics applications. A move to a single, global biometric ID standard

could reduce the potential for confusion that would be created by a fragmented approach to biometrics. It could also help to foster uniformity across airports with respect to many aspects of passenger facilitation.

Establishing a global standard, however, will be no easy task. Stakeholders may face different privacy and legal issues and may not universally agree on how this technology will be deployed, nor on how stakeholders might use, share and integrate the data they collect in the process. The newly published and adopted ISO/IEC biometric Standard Series 39794, for example, will likely be adopted by ICAO as the basis for its 9303 standard on machine-readable travel documents. Technology standards for image resolution, exposure and other quality issues remain to be developed, and the accuracy of facial matching algorithms across demographics must also improve. Any global biometric standards will require privacy policies and rules that address how, where and for how long data is saved. A framework is also needed to define and clarify roles for all stakeholders.

To move forward, the industry should adopt a unified approach in tackling these issues. A global biometric standard will require cooperation among airlines, airports, government agencies, suppliers and other stakeholders. One challenge will be to harmonize the many industry initiatives already underway. The objectives are to have internationally agreed-upon standards for all biometric modalities, while understanding there are broad diverse applications and respecting data privacy requirements across jurisdictions.

Given that it will take time to develop a global biometric standard, how do airlines and airports proceed in the meantime?

Perhaps the most important thing that airports and airlines can do is to find ways to work together.

To be useful in improving the passenger journey, biometric ID systems require access to shared, trusted databases that house the digital information collected. Airlines and airports may opt to leverage their own technology in partnership with CBP by using the TVS facial comparison service for identity verification for self boarding or self bag drop applications.

But airports cannot create databases in isolation. An airport typically does not know who its customers are until they physically present themselves when they arrive for their flights. Passenger information is maintained by the airlines. To be successful, airlines and airports will need to build stronger relationships and broker agreements built on trust. Trust between the U.S. government and traveling public is also key. DHS addresses the public's concern for privacy by issuing

Privacy Impact Assessments to notify how TVS collects and uses personally identifiable information and campaigns to help educate the public.

Another issue to be considered is timing: when and where to begin.

Most U.S. biometric activity to date has been driven by a congressional mandate to bring facial biometrics programs to the nation's 20 largest airports. Airports not bound by those mandates are typically choosing to incorporate biometrics into their capital programs.

In other words, large or growing airports with significant capital programs are likely to begin sooner than those with less construction activity. Because airports are in different stages of capital program planning and maturity, biometrics implementation will likely be uneven, short of federal mandates.

How will biometrics affect airport design?

Broadly speaking, biometric technology will alter airport design in two dramatic ways: queuing area space allocations, and guiding foot traffic patterns throughout terminals. With a biometric ID system, passengers will still be naturally metered through security, immigration or boarding but will not be required to queue for prolonged periods. This change may promote designs that focus on passenger flow in relation to accessibility, amenities, concessions, and services that current layouts don't consider.

Informing planning with biometrics calls for consideration of many variables and issues, such as:

Image quality – The success of a biometrics program depends on the ability to obtain good images of travelers. That ability can be impeded when reflections from floors, walls, windows and other surfaces create glare on images, rendering them unusable. Designers will need to incorporate

nonreflective surfaces in zones where images are collected. When recommending the skin of airport terminals, designers should consider not only aesthetic issues, but also how the glass or glazing they select will control heat and glare. Careful consideration must also be given to camera size and resolution, as well as other variables, from camera installation height to equipment security.

Wayfinding and signage – Airline passengers today follow established procedures for check-in, TSA clearance and security checks as they make their way through an airport to their boarding gate. Changing the process at touchpoints with new technology may create confusion and anxiety as passengers' natural instincts for queuing are disrupted. Designs must include wayfinding and signage systems to support the procedural changes biometrics creates. Since use of this technology may be voluntary, signage is also needed to help passengers understand their options and direct them how to opt in or out of its use.

Training – Front-line airline employees need training that goes beyond biometric ID system operations. These systems may call for new or modified boarding processes — especially if combined with other new technologies, such as self boarding at gates — both for passengers and airline staff. For example, passengers arriving at a gate to board a plane instinctively dig for their paper or mobile boarding pass with their heads down. Passengers are now learning to look up at the camera as they approach the boarding gate. New exception processes must be designed for passengers who opt out of a biometric ID system. Airline agents must also know who is and is not eligible to opt out and then be prepared to deny boarding to persons who can't opt out, but still refuse to board biometrically. Training must also address issues related to wayfinding and signage, and to the passenger questions and concerns that arise. Marketing and public affairs staff, likewise, must be prepared for inquiries from the media and general public on privacy concerns and data protection, including legal and technical information to support their responses.

How can airports implement biometric ID programs that improve the passenger journey without also raising privacy concerns?

For lessons in addressing the complexities and nuances related to passenger privacy, the aviation industry can look to other industries like technology and banking that have already successfully navigated this issue. Airports, like smart cities and retailers, already use cameras in the public domain for life safety, theft prevention, traffic management and other applications. Airports and airlines should involve their legal counsel in vetting regulatory requirements and associated risks, as cities, counties, states and federal regulations are constantly evolving.

For example, today's consumers use face recognition and fingerprint technology — both forms of biometrics — to unlock their cellphones and to gain access to secure locations at their workplaces. Human nature does not object when an hourly worker is asked to use a biometric time clock with finger scan reader to track and manage the employee's time at work. Recognizing the convenience, time savings and other benefits of these applications, few give the personal data required to complete these processes a second thought.

The challenge is to help inform passengers that the same technology that allows them to unlock their phone also can be used to obtain a virtual boarding pass. That will involve building passenger trust of how the data will be collected, where it will reside and for how long, and how it will be used. Passenger education on how these technologies can improve the airport experience should help to speed their adoption.

Given the voluntary nature of the private biometric ID programs now being deployed, it will likely also be a case of "seeing is believing." As travelers visit airports with facial recognition programs and experience the timesaving benefits, passenger acceptance is likely to grow.

How quickly will we reach the tipping point when passengers expect and demand biometrics? Only time — and the willingness of stakeholders to embrace these technologies — will tell.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction and craft professionals, architects, and more to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

888004-0324