Incorporating Biometric Technology in Aviation: The Journey to Touchless U.S. Air Travel

Background

The connection between aviation and biometric technologies in the US began in earnest with the 9.11 terrorist attack. Immediately after, Congress established the Department of Homeland Security (DHS), and, among other developments, established Customs and Border Protection (CBP) and the Transportation Security Administration (TSA).

This was followed by the following legislation, which mandated the use of biometrics for US Entry-Exit, and authorized TSA to use biometrics for passenger screening:

- The Enhanced Border Security and Visa Entry Reform Act of 2002 (PL 107-173).
- The Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458).
- The Implementing Recommendations of the 9/11 Commission Act of 2007 (PL 110-53).

This paper will provide a brief history of biometrics and aviation from 2001 to the present, with a focus on recent events since 2017, when a major and ongoing policy debate erupted over the CBP decision to use facial recognition in Entry-Exit (as well as the TSA decision to use facial recognition for passenger screening).

Early Developments

From the outset, the incorporation of biometric technology into aviation was focused on US-VISIT Entry-Exit (now Biometric Entry-Exit). For almost the first decade, the focus was mainly on biometric Entry into the USA, driven by the urgency to prevent another 9.11.

A National Counterterrorism Center (NCTC), and Terrorist Screening Center (TSC) were established, along with watch lists and no-fly lists. Fingerprinting was already part of US Naturalization but became standard for all US Visa vetting and was collectively managed within US-VISIT under the IDENT database.

There was little visible progress during this time on Biometric Exit, even though it was one of the key recommendations of the 9.11 Commission. It was a big issue, there was no precedent on how to proceed, and there was no obvious affordable solution.

According to staff deeply involved in the program, there were also concerns that the technology, fingerprints at that time, was not yet ready and that rushing implementation would be a major mistake that might have long-term negative consequences. Initial pilot results had been unsatisfactory.

The situation started to turn in 2011 when DHS headquarters concluded it could not develop the program on its own and directed CBP, Policy, and Science & Technology to use their respective expertise to collaborate to develop a technology solution. This collaboration did ultimately lead to a solution. From CBP's operational perspective, it was essential for the solution to provide a law enforcement benefit, namely, real-time (fingerprint) matching.

Once the technology evolved to the point that real time matching became feasible, DHS in 2013 transferred responsibility for the US Biometric Exit program to CBP and, based on subsequent promising pilots, Congress appropriated $1 billion in 2016 to facilitate moving forward.

In 2017, CBP made the creative and important decision to use facial recognition to their future operations beyond the traditional use of fingerprinting. Facial recognition is the least intrusive of the alternatives and has no criminal connotations. The technology had become highly accurate, as reflected in NIST facial recognition testing, and it would enable a faster more efficient process. Most significantly, CBP had accessible facial galleries through the Department of State US Passport and Visa photos to pre-stage departure galleries and facilitate the boarding process.

Emergence of the Privacy Activists

Although the privacy community has always opposed biometrics, security issues were not in the forefront. The decision to use facial recognition in Exit changed that and the activist community, capitalizing on the existing anti-tech mood (misuse of personal data by big tech and massive data breaches, not involving biometric technologies) mounted a forceful challenge to facial recognition.

With considerable funding, resources, and effective messaging, they have been visible and successful in raising significant, albeit misinformed, concerns about the technology. The result is various federal legislation proposing bans and moratoriums as well as a considerable number of state and local legislative proposals, several of which have passed.

In response, IBIA, as well as other stakeholders, mounted an aggressive outreach, education, and networking program to debunk the privacy arguments and build support for the use of facial recognition in aviation. Industry has made notable progress but there is still more to do.

Arguments of the Privacy Activists

The privacy groups raised an array of arguments, a number of which were patently absurd and largely ignored, such as there is no security threat that justifies the US Exit program and no

reason to check people who are departing, ignoring the fact on 9.11, a large, heavily fueled, aircraft did catastrophic damage immediately following departure.

Technology performance and privacy concerns are the two (2) mainstay arguments.

- Facial recognition is 'biased' against women and dark-skinned people and women, based on two (2) flawed studies.
- Facial recognition algorithms are not perfect (not good enough to use).
- Human recognition is all that is needed**.**
- Facial recognition is a step away from a surveillance society**.**

Debunking the Privacy Arguments

Debunking the arguments focused on the recent test results on facial recognition algorithms by the National Institute of Standards and Technology (NIST), the premier global testing institution. They put to rest the fundamental misrepresentations of the activist arguments that the algorithms are biased and not good enough and confirm the high accuracy levels of facial recognition.[1] These results underscore the benefits of facial recognition and the serious risks to public safety and national security of a ban or moratorium on the technology.

- **Facial recognition is not 'biased'**. Unlike human beings, machines are not biased; there are 'performance differences', the term NIST uses, across population demographics. Recent NIST testing shows significant progress reducing performance variation across the board and that demographic differences of high-performing algorithms are virtually undetectable.[2]
- **The position that algorithms are not perfect cannot be taken seriously.** No machine system or person is perfect. In the real world, the pertinent question is whether automated facial recognition, which augments human decision-making, is far better than the alternative of human recognition only. For many critical public safety activities, it is simply not acceptable to limit performance to human capability, or existing systems, or alternatively to not perform the activity at all.
- **Automated facial recognition is indisputably more accurate than current human recognition only systems.** Measured accuracy of human visual passport inspection is notoriously low, determined by some to be in the range of 80% or less (for example, Passport Officers' Errors in Face Matching).[3] The top performing algorithms

[1] Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NISTIR 8280, (pp. 1–79). doi: 10.6028/nist. ir.8280 Re

[2] Op. cit. (pp. 3, 8)

[3] White D, Kemp RI, Jenkins R, Matheson M, Burton AM (2014) Passport Officers' Errors in Face Matching. PLoS ONE 9(8): e103510. https://doi.org/10.1371/journal.pone.0103510

outperform mean performance of all human groups including skilled forensic face examiners. NIST has identified 5 algorithms, which work against very large databases with millions of subjects, that have an accuracy rate of 99% or better.[4]

Automated facial recognition can do important things that humans cannot, like identifying missing and exploited children and disoriented adults.

- **Facial recognition is not synonymous with surveillance**. This is a misconception promoted by the privacy activists based on hypothetical statements, not facts, to generate anxiety.

  Video surveillance cameras are in wide use today and capture entire scenes for later playback if needed. Facial recognition, on the other hand, is only about the identification of a human face and the ability to match it to a single known facial image. Facial matching is only useful to match against a known gallery of quality facial images to those submitted to it for matching. There is no database of all faces so an unknown individual will still remain anonymous after a non-match. The reality is that a very large swath of the population is not on file anywhere in the US.

  In aviation, international agreements dictate the use of the Passport photo to verify identity for international aviation border crossings. Facial recognition simply automates a process that has been in use since the late 1940's, but it is much more accurate.

The privacy activists know all this. They simply ignore the facts and reiterate their erroneous and misleading arguments, which continue to receive traction among a certain percentage of the political and media elite.

However, there are subtle changes in perspective in Congress. Several senior members, who remain nervous about facial recognition, have decided not to advocate banning its use in aviation because of technology's essential benefits to law enforcement, border security, public safety and now health as well. Covid-19 is also changing the landscape. Such signs are also evident at the state and local levels.

The Present

Covid-19 has dealt a blow to all aspects of our lives. The aviation and travel and hospitality industries are among the hardest hit industries, requiring major redesign to rebuild the industry and to regain passenger confidence in secure and healthy air travel.

[4] "Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification," Grother P., Ngan M., and Hanoka K., 2020/01/22, Pp 26-29

Biometric technologies are an important redesign element to enhance security, convenience, and, now health as well, with a focus on touchless modalities – facial recognition, iris recognition, and contactless fingerprints.

The flight check-in process is the face of airports and also a place where today covid-19 can thrive, unless redesigned. Starting at check-in, airports are crammed with people in long lines with numerous touchpoints and physical document exchanges, bringing the risk of transmitting the virus.

As the face of airports, and the health of passengers at stake, the incorporation of touchless biometrics at check-in is now critical and should be accelerated. In turn, the redesign and rebuilding of airports and the travel and tourism industries is a critical element for rebuilding the economy.

To build political and public support and funding for this crucial redesign of check-in, it is essential now to expand collaboration among stakeholders and expand education, outreach, and networking activities in Congress, DHS, and the Administration.