Airport Biometrics: A Primer (2021)

DETAILS

0 pages | 8.5 x 11 | PAPERBACK
ISBN 978-0-309-49810-4 | DOI 10.17226/26180

CONTRIBUTORS

Solomon Wong, Ellen McClain, Josh Cohn, Roeland Visser, InterVISTAS Consulting, Inc.; Airport Cooperative Research Program; Transportation Research Board; National Academies of Sciences, Engineering, and Medicine

SUGGESTED CITATION

National Academies of Sciences, Engineering, and Medicine 2021. *Airport Biometrics: A Primer*. Washington, DC: The National Academies Press. https://doi.org/10.17226/26180.

ACKNOWLEDGMENTS

The research for this document was conducted through one or more programs administered by the Cooperative Research Programs (CRP) of the Transportation Research Board (TRB) of the National Academies of Sciences, Engineering, and Medicine:

- Airport Cooperative Research Program (ACRP) research is sponsored by the Federal Aviation Administration (FAA).
- Behavioral Traffic Safety Cooperative Research Program (BTSCRP) research is sponsored by the Governors Highway Safety Association (GHSA), and the National Highway Traffic Safety Administration (NHTSA).
- National Cooperative Highway Research Program (NCHRP) research is sponsored by the American Association of State Highway and Transportation Officials (AASHTO), in cooperation with the Federal Highway Administration (FHWA).
- Transit Cooperative Research Program (TCRP) research is sponsored by the Federal Transit Administration (FTA) in cooperation with the Transit Development Corporation.

Recommended citation: Wong, S., E. McClain, J. Cohn, and R. Visser. 2021. *Airport Biometrics: A Primer*. Pre-publication draft of ACRP Research Report 233. Transportation Research Board, Washington, D.C.

AUTHOR ACKNOWLEDGMENTS

The research reported herein was performed under ACRP Project 03-55 by InterVISTAS Consulting Inc. InterVISTAS Consulting Inc. was the contractor for this study, aided by Ann Cavoukian and Jeff Baldwin as trusted advisors Ellen McClain, Josh Cohn, Anna Fantoni, Rene Hopstaken and William Jones were senior investigators. The other authors of this report are Nelly Alandou, David Cojocar, Rene Hopstaken, Tamas Kolos-Lakatos, Phuc Le, Richard Meijer, Brian Mohr, Alisa Silven, Koen Spaanderman, Alex Thomson, and Roeland Visser, supported by Sandy Hayes, Derek Marazzo, Brooks Lai, Wahyu Hariyono and Celia Lin. InterVISTAS would like to thank Simon Wilcox, Jackie Lu, Patrick Gendreau, Frederico Cabrara, Annet Steenbergen, Andreas Hoogeveen, Isabelle Lellieur, Samuel Ingals and Justin Phy, Marcelo Garcia and Paul Clark for their willingness to contribute to this Primer.

Contents

Chapter 1

Introducing Biometrics

Biometrics is one of the most powerful, but misunderstood technologies used at airports today. The ability to increase the speed of individual processes, as well as offer a touch-free experience throughout an entire journey is a revolution that is decades in the making. Biometrics can be a fundamental building block for key aspects of airport infrastructure. But like many foundations, it must be built on a range of considerations beyond technology – process, human factors, policies, to name a few.

Considering biometrics in airports alone would be inappropriate: the technology must also be understood against the backdrop of the use and misuse of emerging technologies. From unlocking a smartphone to the automated recognition of individuals from a library of personal photos, the power of biometric recognition is widespread in our digital lives. At the same time, abuse of powers and flaws in recognition technologies have been widely publicized. Database breaches which enable the misuse of identity information as well as the limitations of certain technology types have given rise to public anxiety about facial recognition. Oversimplification and misunderstanding of technology uses have created an environment where several public entities have elected to outright ban the use of biometrics. Technology firms too have reacted by pausing activities leveraging facial recognition conducted in concert with law enforcement agencies as society-at-large determines some of the parameters to better manage the potential misuse of biometrics.

Biometrics in Aviation

So where does this leave aviation and the use of biometrics at airports? The Airport Cooperative Research Program (ACRP) commissioned “Airport Biometrics - a Primer” to be authored to encapsulate the range of issues and opportunities associated with the use of different forms of biometric identification. The Primer is prepared by experts with a deep understanding of technical issues, but also the range of policy and business case aspects that require consideration by those seeking to introduce the use of biometrics for their operation.

Three over-arching clarifications regarding the Primer should be noted:

- This study is not about mass surveillance: The word “biometrics” is often conflated with mass surveillance. In other words, some media and public conflate the use of biometrics in the context of personal identification for individuals who “opt-in” with a model used typically in law enforcement to use video to surveil individuals contrary to their privacy interests.
- This report is a living document: biometrics technology has accelerated significantly over 25 years at airports in the United States and continues to evolve. The concepts described herein are directional in nature, but there should be consideration for a living Primer to also incorporate overall trends/changes in the future. This report will benefit greatly from an update in due time.
- There are no absolutes: biometrics is also often misunderstood due to the complexity and the number of choices required for an individual deployment. The overall system architecture requires much

consideration before effective deployment, which extends beyond details such as the choice of biometrics technology to be employed (e.g., fingerprint, iris, or hand geometry).

Objective of This Primer

The objective of the Primer is to help aviation stakeholders, especially airport operators, to understand the range of issues and choices available when considering, and deciding on, a scalable and effective set of solutions using biometrics. These solutions may serve as a platform to accommodate growth as well as addressing the near-term focus regarding safe operations during the COVID-19 pandemic.

Fundamentals of Biometrics

Definition of Biometrics

Biometrics are biological and behavioral characteristics of a person, which can be used in a system to recognize someone or verify someone's identity, by those characteristics. Thus, its main purpose is to accurately identify individuals, typically enabling access to a controlled environment.

Types of Biometrics

The earliest use of biometrics dates from the 1860's, with unique patterns (i.e., dash and dot signals demonstrating behavioral characteristics) used by telegraph operators to identify senders/authenticate messages. With the advent of sensor technologies and computing power, automated devices used to identify a person based on certain unique characteristics proliferated in the past three decades.

Biometric identification consists of verifying the identity of a person. One needs to capture an item of biometric data from a person. It can be a photo of their face, a record of their voice, or an image of their fingerprint. This digital biometric is now in a data format that can be stored for use by algorithms. Often though, biometric data is stored as a biometric template, where the biometric data is encoded, for instance, as a random sequence of numbers and letters.

There are many different types of biometrics used to create unique templates for each individual. Some of the common types of biometrics include fingerprint, iris, facial and voiceprint recognition. Many of these are increasingly found in consumer electronics such as smartphones or laptops to unlock devices for use, or to confirm mobile payments. Emerging forms of biometrics include DNA matching, patterns of walking, and other forms of site-specific applications to capture unique traits/behaviors of individuals. A non-exhaustive selection of biometrics is explained below.

Iris Recognition

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both irises of an individual's eyes, whose complex patterns are unique, stable, and can be seen from some distance.

Facial Recognition

A facial recognition technology can identify or verify a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given images of faces within a database. It is also described as a Biometric Artificial Intelligence-based application that can uniquely identify a person by analyzing patterns based on the person's facial textures and shape.

3D Hand and 3D Finger Geometry

3D hand and finger geometry exploit discriminatory information provided by the 3D structure of the hand, or, more specifically the fingers, as captured by a 3D sensor. The advantages of 3D hand and finger biometrics over traditional 2D hand and finger geometry (more typically know as fingerprint) are authentication techniques, improved accuracy, the ability to work in a contact free mode, and the ability to combine this form of authentication with facial recognition using the same sensor.

Hand Geometry

Hand geometry is a biometric that identifies users by the shape of their hands. Hand geometry readers measure a user's hand along many dimensions and compare those measurements to measurements stored in a file.

Voice Recognition

Voice biometrics works by digitizing a profile of a person's speech to produce a stored model voiceprint or a template. The tones collectively identify the speaker's unique voiceprint. Voiceprints are stored in databases in a manner like the storing of fingerprints or other biometric data.

DNA Matching

DNA matching is a complex technique that can be used to identify someone or verify someone’s identity. DNA matching requires highly specialized laboratory equipment and is not readily (or quickly) achieved. Further, techniques that use DNA may offer much deeper and far reaching capabilities – with extensive research being done to map the human genome stored in our DNA – because someone’s DNA can provide much more information about that person than they are often comfortable sharing, even on a personal basis. DNA can store information about heritage, physical characteristics but also elements related to one’s health such as elevated risks to diseases. For the reasons above, DNA matching is not (yet) applied in the airport environment and is not a candidate for biometric applications that require speed and efficiency.

Nonetheless, DNA matching is mentioned here, as it is used in other fields such as (forensic) research applications within criminal justice cases, challenges in paternity and other cases that use this technique, either as a last resort, or because of the high accuracy of identification it can provide. Future use of DNA for biometric technologies in aviation is most likely only in the distant future, not the least because the storage of one’s DNA in a database, by private or public sector would likely be subject to many legal challenges.

Practically, there are various methods for analyzing DNA to establish if two samples are the same or different. These methods are often referred to as DNA fingerprinting. For example, two sample pieces of DNA can be studied in the laboratory to determine if they have portions in common, and thus overlap with one another.

Combinations of Biometrics

At times, one biometric is insufficient and a combination of two or more biometrics is used. This combination raises the level of security and is sometimes utilized to control access to high security buildings or areas, such as vaults.

Understanding the Differences Between Detection, Matching, Identification, Verification and Authentication?

When dealing with biometrics, there are a lot of words used to outline the expected outcomes of the technology. From detection to authentication, each has different connotations from the concept of operations through to the application of law. Specifically, the description of each word is follows in terms of the use of biometrics:

- Detection answers the question: “Is a biometric being sensed?” Often, a specific part of the biometric technology is in place only to process from sensors whether a biometric is presented, i.e., is there a finger on the fingerprint scanner? Is there a face in front of the camera? If so, the biometric can be digitally recorded. Detection does not specify whether a biometric is scanned, used, stored or retained.
- Matching is the step that may follow detection of a biometric. In this case, the biometric is scanned, stored at least temporarily (as a template or not) and used for the purpose of comparing with a second (similar type of) biometric. The second biometric must be present or stored, in order to be compared and matched. A positive match is when the two biometrics exhibit sufficient likeness, to pass a specific matching threshold.
- Identification answers the question: "Who are you?" The identification process implies the use of a matching process of a scanned biometric and comparing it to a set of stored biometrics, with the intent of discovering the identity of the person to whom the scanned biometric belongs.
- Verification answers the question: "Are you really who you say you are?" The process also implies the matching of two biometrics, one scanned and the other either on file, or presented by the same person in the form of a token (e.g., an e-Passport). Because both biometrics are presented, verification only aims to prove a positive match between the two, rather than discover the identity of the person to whom the biometric belongs. In this case, the actual biographic information does not have to be linked to the biometric, or stored with the biometric. It should be noted that facial recognition is a common type of biometric verification. The difference between the two is exemplified for the facial biometric in the following:
  - Facial recognition is a software driven application that looks at facial points and contours to analyze and compare two face biometrics and make an attestation of likeness.
  - Facial verification is considered as a form of biometric verification by definition and looks at unique biological characteristics so one's identity can be verified.
- Authentication answers the question: “Is this identity credential/document authentic?” This implies the checking or verifying of the authenticity of an identity document or credential; for example: is the passport fake or real? Passports, much like many currencies, have elements and attributes that allow an expert to prove the authenticity of the document. e-Passports also have a digital attribute that allows for automated checking of the document’s authenticity, i.e. whether the document is indeed issued by the right issuing party or government. Biometrics are typically not used in the authentication process.
- Validation is at times confused with verification (and/or authentication). A slight distinction is important to clarify here: validation looks at whether the specifications that are evaluated are appropriate to accomplish the goal, while verification checks if the specifications are met. For example, in the case a passport is used to verify identity, one checks if the specifications (e.g., the name printed in the passport) matches with what the person claims his/her/their name to be. In validation, one may conclude that a passport is an adequate tool to verify one’s identity, because the characteristics of the passport (printed name in the document) can be used to accomplish the goal of identity verification.

Using Biometrics – What is the Purpose or Objective?

For biometrics to function, there are three main modes of usage:

- One-to-one (1:1) matching: verifying a biometric based on a previously registered identification document (i.e., is this really the same biometric as on the identification document?)

- One-to-many (1:N) matching: verifying a biometric or identifying an individual out of a large database of biometrics/people (i.e., in case of verification: is the biometric presented also in the database? In the case of identification: to whom does the biometric presented belong?
- One-to-few (1:few) matching: verifying a biometric or identifying an individual out of a subset of a database of people.

Figure 1-1: The three types of biometric matching commonly seen today

There are substantial differences between the three types of matching. One-to-one biometrics has an individual approaching a door, a checkpoint or other mechanism. For example, a previously registered template is compared to a live photograph to verify access rights.

On the other hand, one-to-many is exemplified through mass surveillance techniques such as those integrated in closed circuit television cameras for law enforcement and national security. This mode works through leveraging camera technologies to identify individuals in view of a camera, often without their knowledge.

One-to-few is different from one-to-many because it uses a subset of a larger database to verify or identify individuals. This database is smaller due to a selection prior to the comparison.

While each type of biometric matching has privacy implications, each is rooted in a different technology type. One-to-many requires a substantial amount of data storage and computation power. India and China's drive towards a mandatory national biometric system will require large amounts of information to be collected and protected to enable recognition of billions of individuals.

One-to-few is less computationally intensive as it uses a subset of a larger database. Instead of comparing an image to the whole database, a selection of profiles can be used when it is known ahead of time who will be expected. At an airport, most passengers have booked their flight well in advance allowing for the potential comparison to the passenger manifest as the population of the "few."

One-to-one biometrics is the least computationally intensive of the modes and has a range of options for data storage, including databases, smartcards, or the microchip on an e-Passport.

How Are Biometrics Collected and Stored?

Biometrics are typically captured by a camera, a microphone, a scanner or some other sensing device and turned into a digital signal. This signal is then transmitted to a computer chip that can process the signal with software to create a digital code called the biometric template. The biometric template is not a copy of the biometric scan itself, but rather converted by an algorithm to a unique data file. The critical issue regarding biometric data security relates to the location of the stored biometric templates. It is considered best practice for actual sensor data to be discarded upon creation of the biometric template. The biometric templates are typically stored in a database, a mobile device or on a token. A token is the generic term used to describe an item that one can carry with them on which a biometric template is stored, such a passport, ID card, memory stick or similar.

In this Guidebook we identify four distinct types of storage:

- Locally on a mobile device
- On a portable token such as a chip on an identity pass
- Centralized on a database server
- Distributed data storage

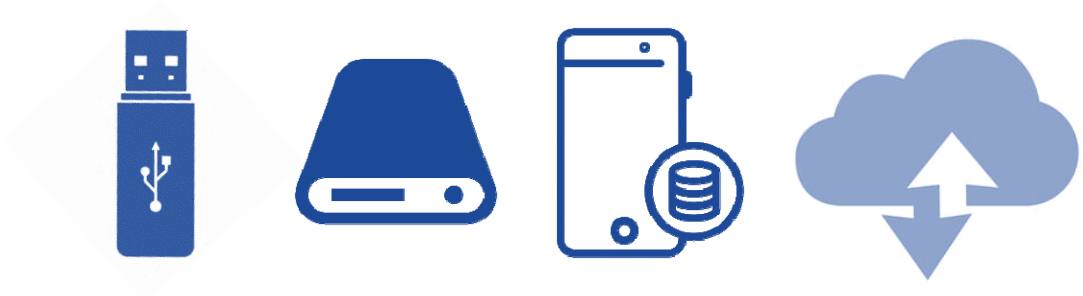


Figure 1-2: Where a system stores the biometric data is critical in the design

A locally stored biometric template can only be used on that device, e.g., using a fingerprint to unlock a phone. Biometric templates can also be stored on a database server in a data center. This method is typical for large corporations using biometrics to grant its employees access in office buildings or secured facilities. Storage on database servers comes with a higher risk, as multiple templates are stored in one location. Biometric templates can also be stored on a portable token such as a USB drive, an access card (e.g., Global Entry® or an e-Passport. Finally, biometric templates can be stored in distributed data storage. This method stores biometrics templates on a local device and on a server, both of which must be accessed concurrently for authentication. Because of the split nature of this biometric template storage method, hacking is nearly impossible and therefore this method is highly secure.

Although encryption of the stored data significantly improves security, determining who has access to the encrypted data and how the data is used is a critical issue. With respect to the privacy retention and sharing of personal information, civil liberties groups and the Electronic Frontier Foundation have challenged the need to collect and use facial information. The legal, policy and privacy aspects related to the collection, use and retention of biometrics are elaborated in Chapter 3.

Current State of Biometrics

We are in an era of mass adoption of consumer biometrics, with most common devices providing the option of password-based unlocking mechanisms or the use of facial recognition or other biometrics to unlock devices. At the same time, several governments have elected to use biometric technologies to enforce social order. For example, in Shenzhen, China facial recognition is used to issue jaywalking citations as well as collect fines – all taking place before an individual reaches the other side of the street.

Some entities and individuals seek an outright ban on the use of biometrics, which some consider analogous to banning the use of passwords for computers. Accordingly, it is important for organizations to define the range of biometric use cases, respecting both laws and regulations, as well as best practices for privacy-protected interface with passengers, employees, or consumers to ensure potential risks are proportional to the benefits. The privacy discourse to date focuses, in part, on the retention and sharing of personal information. Chapter 2 explores the U.S. use cases and Chapter 3 addresses the legal, policy and privacy issues.

Vision for Biometrics at Airports

With the fundamentals of biometrics described in the previous section, this section narrows the scope to the application of biometrics within the airport environment. The current vision for biometrics at airports dates from the late 1990's, and accelerated in different phases centered on e-Passport adoption in the 2000's as well as alternate forms of storing biometric information in the 2010's.

Through this time period multiple initiatives advanced common interests across stakeholders, including but not limited to:

- The Simplified Passenger Travel Interest Group involved a discussion among airlines, airports and governments to explore mechanisms for the implementation of biometrics.
- International Air Transport Association (IATA) OneID is aimed at providing passengers with a seamless experience with enhanced security for governments and reduction of costs for airlines and airport operators.
- IATA and Airport Council International's (ACI) New Experience Travel Technologies (NEXTT) vision extends the biometric vision to other use cases for baggage handling both on and off-airport, as well as applications of artificial intelligence.
- The International Civil Aviation Organization's (ICAO) Digital Travel Credential (DTC) standard envisions new opportunities from its passport standards documents.
- World Travel and Tourism Council's Safe and Seamless Traveler Journey initiative aims to enable a seamless, safe and secure end-to-end traveler journey through systematic biometric verified identification at each stage of the journey replacing manual verifications.

Broadly, there are also different visions for biometrics amongst entities in the United States. The U.S. Chamber of Commerce Facial Recognition Policy Principles in December 2019 point to "facial recognition technology as an enormous potential to enhance security and safety and enable innovation across a wide variety of sectors including transportation, retail, hospitality, and financial services." The Department of Homeland Security (DHS) and Customs and Border Protection (CBP) have also articulated a long-range vision for biometrics, as have individual airlines. To simplify the vision of biometrics specific to aviation, the following vision is offered:

"Biometric technologies are the collection of tools to establish trust in identity, seamless flows, and touchless airport experience."

Breaking this vision into its four components:

- Collection of tools: the use of biometric technologies is not simply one mode of operation, it is a family of different tools/devices/storage mechanisms, each with different implications.
- Trust in identity: from credit card fraud to intercepting imposters, there is a greater trust biometrics can offer. This indirectly connects to improved security and safety in the aviation system.
- Seamless flows: for the promise of a single form of identification, biometrics can ensure that the amount of document fumbling is minimized (passport, visa, health forms, etc.).
- Touchless airport experience: from the status of COVID-19 immunization, to other ways of enabling airport retail to function, biometrics can augment minimized contact with disease-transmission media, surfaces, or staff.

Interoperability and Scalability

With the overall trend of biometrics moving to multi-stakeholder solutions, interoperability means a single biometric system that can be used by airlines, governments or third parties through an airport environment and the ability for identity verification to be used throughout the journey.

Interoperability examples in other industries provide examples to the aviation industry. In banking for example, there was a point in time in the 1980's when every bank had a separate system for every ATM.

Over time, interoperability was available so that you could use a Bank of America ATM card at a HSBC Bank in France.

Biometrics is similar, but perhaps more complicated due to the potential for future use cases to be added. For example, if an identity verification system is used for airline check-in, the Transportation Security Administration (TSA) security check and flight boarding, this is a deployment that could be in place for several years before adding additional phases. Scalability planning dictates a pathway to enable more modules to be added, for example for rental cars, airport retail or even other uses outside airports. A private third-party that has demonstrated scalability is CLEAR® which offers identity verification as a service through a paid membership, with clients including Major League Baseball and National Football League, using the same biometrics for airport applications.

Related to interoperability is the common use of processes, installed systems and facilities at airports. Often characterized as being able to use self-service kiosks and check-in desks for all airlines at an airport, common use applies to a much broader set of facilities and sets a common standard for their design and operation. The benefits of common use are as relevant to biometric technologies and solutions as they are to traditional facilities and include spatial savings, time savings (e.g., leading to shorter minimum connection times), and improved passenger experiences. For more on the design, implementation and benefits of common use systems and facilities at airports, refer to the ACRP Report 30 on common use, and to the to be published report following the ACRP 03-52 research project.

Chapter 2

How Advanced Is the Employment of Biometrics at Present?

Summary

Chapter 2 describes the many ways biometrics are employed in airports: process facilitation; access control to secured areas; tailored customer services to the individual user; commercial use by retail/concessions vendors; and fraud identification and risk mitigation to minimize loss.

Ten case studies illustrate the variety of biometric technology use in airports today. Those case studies showcase uses at five U.S. airports and five other uses at airports world-wide. The case studies highlight: (1) a potential template for current and future models for touchless and cashier-free retail at airports; (2) the VeriFLY initiative that combines the idea of reservation systems together with QR codes to provide queue access and other possible passenger processing uses; (3) a trusted traveler model for true identification of low-risk, pre-approved travelers that have been vetted in advance; (4) an example of a public-private partnership in handling biometric/biographic data for employee vetting for TSA approval of Secure Identification Display Area (SIDA) badges; (5) an example of the power of end-to-end facial recognition in one system that offers benefits for border processing, check-in, TSA and other processors; (6) a Canadian-Netherlands pilot illustrating the potential of the Digital Travel Credential for global travel; (7) implementation at multiple terminals at London Heathrow for a more seamless experience and offering scalability for international application; (8) Easy Airport which illustrates how biometric uses can be designed and refined to meet airlines' business needs, including during COVID-19; (9) an example of an effective communication strategy with passengers and the general public about biometric use; and, (10) one of the earliest examples of biometric data use in Aruba's Happy Flow.

The ten case studies illustrate specific, and in most cases, unique applications and benefits of biometrics, lessons learned, identification of challenges, and key trends which include the following:

- Trend 1: The deployment of integrated and multi-stakeholder biometric solutions is increasing, given its greater potential benefits.
- Trend 2: Digital transparency and privacy concerns are adding to the complexity of implementation, particularly as the legal landscape changes.
- Trend 3: A focus on identity verification solutions is evident, in part, to distinguish from mass surveillance programs that also leverage biometrics.
- Trend 4: Global biometrics and standards are emerging from a variety of governmental and non-governmental entities which are addressing privacy, security, ethical, and technological concerns.
- Trend 5: Smartphones are expected to enable more use of biometrics through the on-device storage capability for biometrics, as well as the promise of the transmission of digital travel credentials.

Five Primary Use Cases for Biometrics at Airports

There are five primary use cases identified in the aviation sector, or more specifically, as implemented at airports around the world. These five use cases are each described in the subsequent sections and followed by 10 case studies that provide examples to one or more of the use cases identified. The chapter concludes with a vision statement for the use of biometric technologies, that highlights the significant potential to transform the future travel experience, as well as the airport.

KEY TAKEAWAY

The increased use of biometrics in everyday life can generally be assigned to five practical uses:

- facilitating and simplifying processes
- granting access to certain people to certain areas
- personalize interaction with technology
- expediting commercial exchanges
- guarding against fraud and improving security and safety

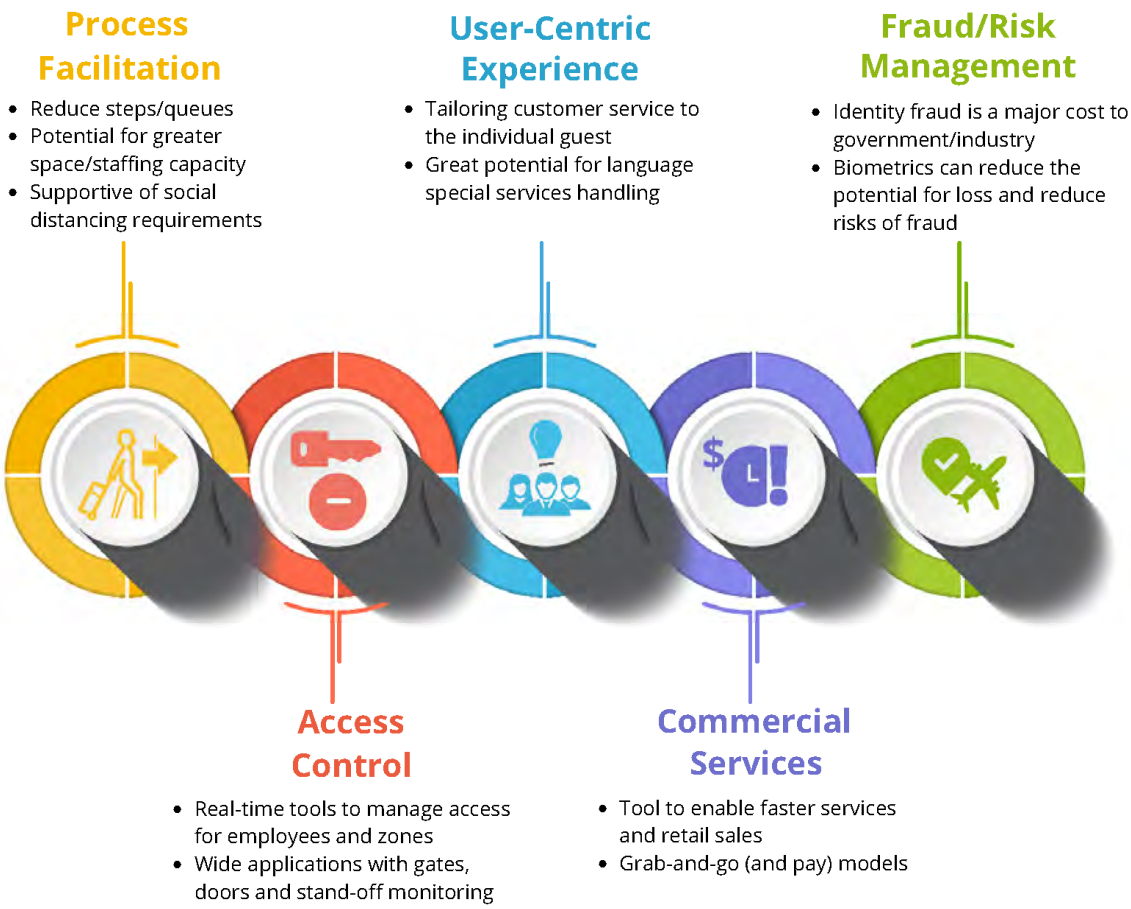


Figure 2-3: Overview of Primary Use Cases of Biometrics

1. Process Facilitation

The aviation system involves a series of steps and processes. Passengers, employees and suppliers need to record and demonstrate identity information several times through an entire workday or journey. While a document check requires on average 3-5 seconds of time, it is the multiplication of transaction times to present paper documents that can lead to difficulties, especially in a group environment. Adding five seconds per passenger may sound insignificant, but the practical effect can create a queue of hundreds of people if there is not a corresponding reduction in time identified elsewhere in the overall process.

During the COVID-19 pandemic and the recovery phase, these considerations are even more important to address social distancing and health screening requirements that can further elongate queues. Airport operators must also be mindful of the much greater level of exceptions handling. In other words, as the travel environment adjusts to new requirements or steps, there will invariably be missing forms or other steps passengers are unaware of that will require special handling, space, and time to resolve. The aim must be to have the vast majority of the population (95%+) able to proceed through airport processes without delay.

To unlock the potential for process improvements, there is a move to reduce sequential steps. Biometric use cases offer the potential to simultaneously process individuals without having to deal with sequential steps (and exceptions). The net result could be the elimination of passenger queues and converting these steps to a more automated process.

2. Access Control

Security is about safeguarding that which needs protection from harm, but also about allowing that which will do no harm. Determining one from the other is typically based on one of three things: who you are, what you have, and what you know. The latter two are best described as having a key (what you have) and a password or PIN code (what you know). Biometrics can be an added layer leveraging the physical features of an individual for identification or authentication purposes.

One of the most mature uses of biometrics at airports is access control – in other words, the automated authorization to proceed through a door to a secure area of an airport. A combination of a key card and a biometric is the dominant use case. While this use case may be conventionally thought of in the context of airport employees, there are a number of emerging use cases geared toward airline passengers.

Passenger access to a boarding gate or managing access to a premium lounge on the basis of biometrics are two prominent examples of passenger-facing access control.

3. User-Centric Experience

While identity management and process facilitation are geared towards confirming identity, an emerging use case for biometrics is customizing the user experience.

Aviation markets are increasingly segmented to the different market types and preferences. From millennials to older travelers, to different travel segments (leisure, business, visiting family/friends, passengers with reduced mobility), airports are increasingly offering customized experiences. Providing identity management to help differentiate the user experience, from brand loyalty to personalized experiences, there is a use case to ensure the experience is more streamlined and welcoming to travelers.

Some tangible examples include interaction with passengers to only display information relevant to the individual pertaining to flights, weather, preferred services and other direct communication (language, font size, etc.). Vendors have also demonstrated new screen technologies that can ensure that on-site wayfinding signage is customized and directed to specific individuals only – all powered with a voluntary biometric identification algorithm.

4. Commercial Services

Airports around the world depend on roughly 45% of revenues from non-aeronautical sources. This share can be higher for some airports (e.g., Las Vegas) that have a larger concessions program. While some world regions (Europe, Asia) have traditionally had a higher amount of retail/concessions/duty free revenue stream, there is potential for biometrics to increase revenue per passenger.

Increased revenues may be achieved through biometric-enabled use cases that are able to convert lost time into potential spending time by eliminating queues or waiting. Cashierless airport retail is a vision that has accelerated to an extent due to the COVID-19 pandemic. Increasingly between flights, a passenger can simply grab-and-go items of choice without needing to queue for payment. Biometrics and other tap-to-pay technologies can enable this reality.

Other groups are also converting dwell time in airports as opportunities to sell products for pickup at an arriving airport – which may be fueled by biometrics.

The realignment of commercial services in airports is demanding a touchless experience for any passenger-facing service, with a range of biometric use cases.

5. Fraud/Risk Management

Finally, the dominant area of biometric solutions for governments is the interdiction of criminal behaviors in travel. From CBP's ability to catch 300 imposters to date through facial recognition software, there are a range of use cases to help defeat criminal activity (US Customs and Border Protection, 2021).

Hundreds of millions of dollars are also lost annually by airport retailers and the airline industry overall due to fraudulent activities. Notably, the estimated cost of payment fraud to the airline industry each year is about $858 million, according to IATA. Whether it is credit card fraud at a store inside an airport or ticket fraud, there is a cost to the industry which the use of biometrics may mitigate.

In addition to combating criminal behavior, there is also an added aspect of risk management. Risk based security initiatives for TSA, for example, have the ability for biometrics to aid in linking different systems. Results of passenger security screening checkpoint scans, for example, can help to inform the level of baggage screening scans – a platform that may be supported by biometrics tied to departure control systems.

U.S. and Worldwide Lessons from Deployments

The following table presents an overview of the key highlights and lessons learned from ten case studies, in which the application and importance of biometric technologies are illustrated. These case studies provide a representative cross-section of the efforts and developments that have taken place in the United States, as well as in the rest of the world. Further details regarding each case study can be found in Appendices A-J.

KEY TAKEAWAY

The main takeaways from five U.S. and five international biometric case studies are presented, ranging from complex multi-stakeholder implementations, to simpler and more local solutions. Implemented solutions inform:

- granting enhanced retail experiences
- fast-tracking and improved security solutions
- health related separation
- complete biometrics enabled journeys, from the curb to the gate
- returning data ownership to the passenger
- seamless passenger flows, technology less intrusive in the journey
- governments implementing a nation-wide biometric identity
- and more…

Table 2-1: Case Study Overview Table

Case Study Number	Case Study Name	Case Study Highlight
1	Amazon Go "Just Walk Out" Cashierless Retail Experience	• Potential template for current and future models for touchless and cashier-free retail at airports • Some enrollment challenges may be resolved with simple two-step palm enrollment
2	Denver-Daon Biometric Partnership	• Combines the idea of reservation systems together with Quick Response (QR) codes to provide queue access • One of several platforms with the potential to link passengers to "health passport" information • Remote passenger screening pilot can also help meter the peaked nature of operations, even during a reduced traffic time period
3	CBP Trusted Traveler Programs at Airports	• Ability to facilitate not just U.S. citizens, but a range of country nationals (S. Korea, Canada, U.K., etc.) • Model for true identification of low-risk, pre-approved travelers that have been vetted in advance • Added benefits to facilitate these individuals through TSA via PreCheck™
4	Seattle-Tacoma International Airport and Designated Aviation Channeling	• Designated Aviation Channeling (DAC) model is an example of a public private partnership in handling biometric/biographic data • Evolution of protocols for handling personally identifiable information offers a good set of protocols
5	Curb to Gate Program by CBP and Delta Airlines at Atlanta International Airport	• Good example of the power of end-to-end facial recognition in one system • Demonstrated capability of leveraging biometrics without the need for re-enrollment • Specific measurements of benefits for border processing, check-in, TSA and other processors
6	Known Traveler Digital Identity at Aéroport International Montreal-Pierre Elliot Trudeau, Montreal, Canada	• Lessons learned on privacy of information and transmission to foreign governments, especially regarding legal frameworks between the project stakeholders

Case Study Number	Case Study Name	Case Study Highlight
7	The Seamless Passenger Journey at London Heathrow	• Scalability of platforms to also potentially work with transatlantic flights to the United States • Integration quality and deployment across multiple terminals is a significant model to emulate for smooth delivery
8	Risk Management During COVID-19 Using Biometrics, Carrasco Airport, Montevideo	• Ability to meet different airline business cases – some saving resources/re-dedication of resources through the biometric system • Add-on data portals provide added value for project partners • Used for the risk-profiling of passengers as part of efforts to control the spread of COVID-19
9	Digi Yatra and the Seamless Passenger Journey at Kempegowda International Airport	• Focus groups and simple communication “your face as boarding pass” • Model notable also for an “opt-out” pathway for those who do not elect to use biometrics
10	Happy Flow at Aruba International Airport	• Early implementation of biometrics with Happy Flow model to anticipate transatlantic preclearance • Some improvements on the mechanisms to conduct identity checks for participants • Broader vision for enrollments “on the beach” may not be supportable by all stakeholders

Case Study 1: Amazon Go Cashierless Retail Experience

Summary

Initiated by Amazon, the Amazon Go retail experience uses a combination of cameras, sensors, computer vision techniques, machine learning, and artificial intelligence techniques to create a checkout-free retail experience for its customers. The technology is also available for other retailers, referred to as "Just Walk Out". The customer's identity is verified when signing up through the Amazon Go app and entry to the store is gained by showing a QR code, one's registered palm biometric (for an Amazon Go store) or their credit card (for other retailers equipped with the "Just Walk Out" technology).

Source: Amazon

Figure 2-4: Overview of the steps to shop at an Amazon Go store

Program Concept

By leveraging computer vision and machine learning to track customers and distinguish between the items they pick, customers can be charged for their items without stopping at a cashier. The methodology does not rely on facial recognition but rather on movement tracking, and where available a biometric palm scanner.

Each customer, upon entry, is associated with a name, an account, and a consumer profile reflecting all interactions with items on the shelves (e.g., which items they view, pick up and buy, etc.). Future use of the customer's data is still undefined. However, the initial patent application included some examples where the customer's purchase history could be used to confirm which items are being picked up from the shelves by the user.

Table 2-2: Key Points for Amazon Go Case Study

Criteria	Overview
What	• Touchless checkout-free retail
Where	• 21 stores across the United States
Passenger Process	• Sign up through a mobile app and create Amazon account • Scan QR code, palm or credit card when you walk into store • Take items and "just walk out"
Who	• Amazon Go (Amazon)

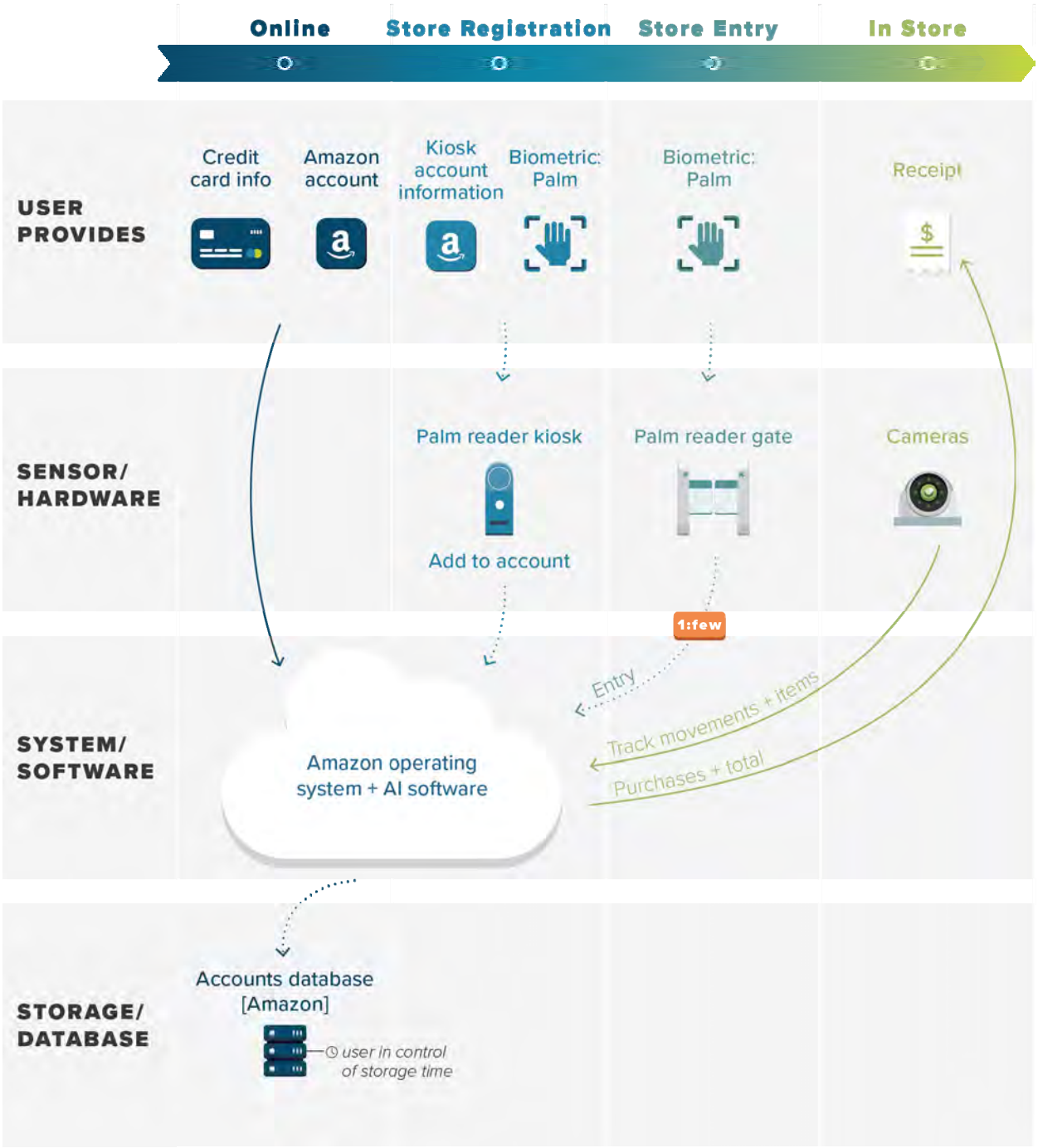
Criteria	Overview
Why	• Revolutionize the retail experience: to make it safer and more efficient
How	• Movement tracking and smart sensors in store track items customers take. Once they leave, their accounts are then charged.
Enrollment	• Sign up through a mobile app and register palm biometric (where available)
Verification of Identity	• Identity is verified through mobile app when customer signs up for an account
For	• Customers with Amazon Go accounts

Program Key Takeaways

The main benefits behind utilizing this type of technology are significant time savings for customers and financial savings for retailers, through lower operational expenditures on employees (e.g., labor wages, benefits, etc.). Some enrollment challenges that may be resolved with simple two-step palm enrollment, and interesting because some may feel this methodology is less 'invasive' as compared to facial recognition. Furthermore, this type of software presents a potential alternative to current and future models for touchless retail for both airports and airlines.

Case Study #1

Amazon Go Cashierless Retail Experience



Case Study 2: Denver-Daon Biometric Partnership

Summary

To balance the needs of passenger health and safety, Denver International Airport has partnered with public health stakeholders and biometric technology firm Daon to develop a biometric authentication system known as VeriFLY, aimed at making passenger journeys safer and more predictable. A second pilot for remote screening would involve a security checkpoint located remotely from the passenger terminal.

Program Concept

VeriFLY: With the intention of putting high-risk and health-conscious passengers first, passengers can use a reservation system on the mobile app to access a dedicated security lane. At the airport, after a temperature check the passenger can enter the security lane by scanning a QR code shown in the app at an e-gate. A health questionnaire must also be completed within 24 hours of their flight. Passengers access a reserved train car with other VeriFLY travelers, which ensures a socially distanced and contactless concourse ride to their respective gates.

With the initial implementation, this is a stand-alone system that is not tied into other databases. Future development may automate more steps of the process by including facial recognition and third-party health information.

Table 2-3: Key Points for Denver-Daon Case Study

Criteria	Overview
What	• Biometric authentication system for security lane reservations and remote security screening
Where	• Denver International Airport
Passenger Process	• Mobile app sign-up to a reservation for the security checkpoint • Health form completion • Arrive at airport for designated slot
Who	• Denver International Airport and Daon
Why	• Speed the passenger processing of passengers • Create health-conscious and more predictable journey from security checkpoint to concourse
How	• VeriFLY: Facial recognition to verify identity in the app to bring up a QR code for airport touchpoints • Remote security screening
Enrollment	• Voluntary, appointments on the app can be booked 2 weeks in advance
Verification of Identity	• Facial recognition via the mobile app
For	• Departing passengers on domestic and international flights

Future development aims to automate more steps of the process by including facial recognition and third-party health information.

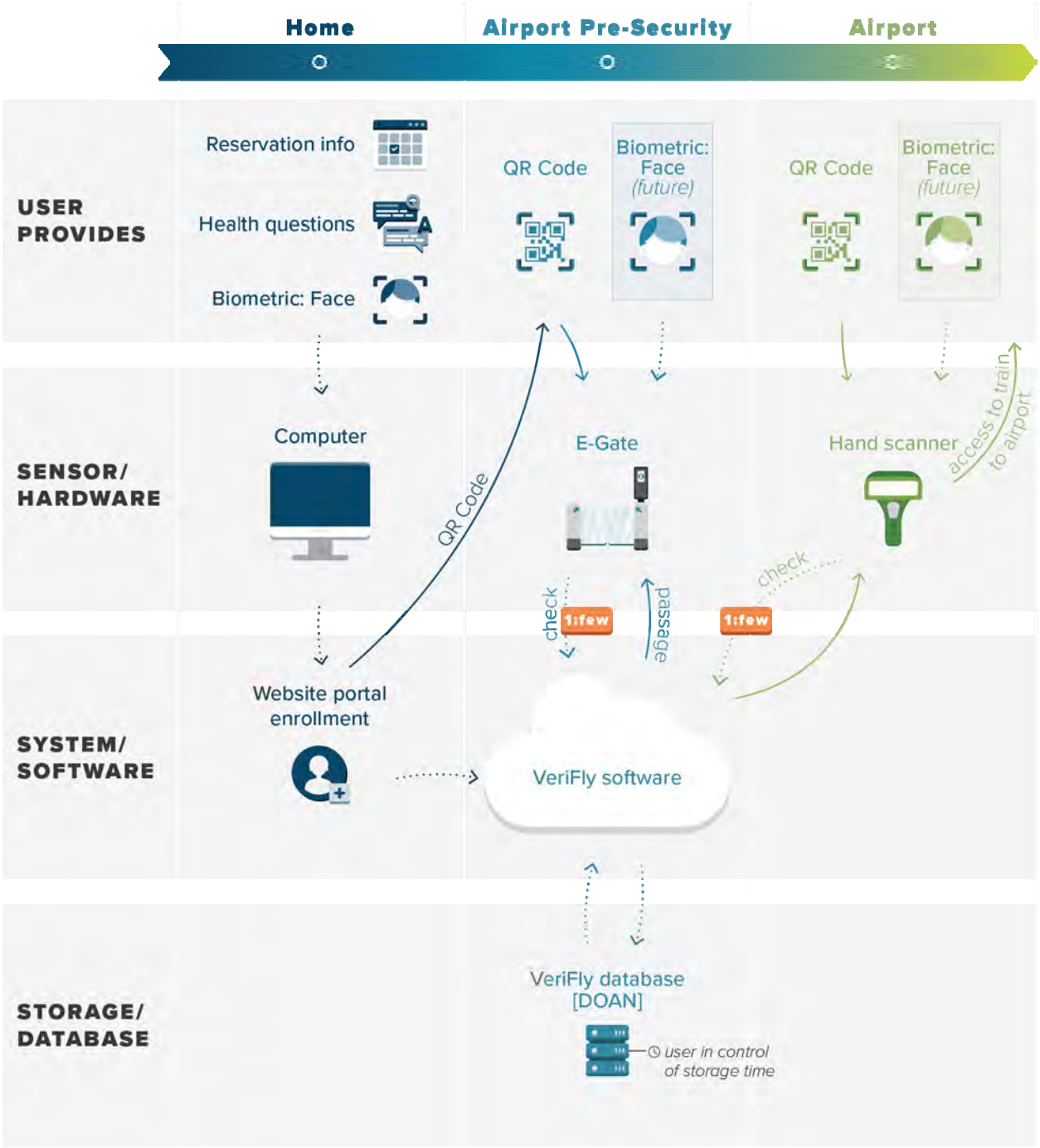
Remote screening: In the future, the airport may offer a security screening checkpoint remote from the passenger terminal, adding capacity and offering a unique experience for segments of the traveling population.

Program Key Takeaways

The VeriFLY initiative presents an opportunity to add reliability and confidence to the passenger travel journey by decreasing customer interactions and reducing potential for congestion. Furthermore, VeriFLY combines the idea of reservation systems with QR codes and can help reduce the strain on airport operations, even during reduced traffic periods as a result of the COVID-19 pandemic. It is one of several platforms that could leverage health passport information, many of which are under development. Interestingly, the remote screening pilot can also help meter the peaked nature of operations, even during a reduced traffic time period.

Case Study #2

Denver-Daon Biometric Partnership



Case Study 3: CBP Trusted Traveler Programs at U.S. Airports

Summary

Designed to provide quick, easy, and convenient processing, the Global Entry® program is a CBP program that allows for expedited clearance for pre-approved, low-risk travelers upon arrival to the United States. Global Entry® is designed to reduce the time required for travelers entering the United States through the passenger verification process. Similar programs include SENTRI and NEXUS. The roots for Global Entry® date back to INS Passenger Accelerated Service System (INSPASS) in the 1990s, before the current iteration was piloted by CBP starting in 2008.

Source: Global Entry® Program.

Figure 2-5: Overview of Global Entry® Program Procedures

Program Concept

At airports, program members proceed to Global Entry® kiosks, have their picture taken and are matched against a gallery pre-compiled from a CBP database. The kiosk then issues the traveler a transaction receipt and directs the traveler to the baggage claim and the exit.

Travelers must be pre-approved for the Global Entry® program. All applicants undergo a rigorous background check and in-person interview before they are approved for enrollment. Applications are reviewed by CBP and information is processed through various government databases. Once conditionally approved, the individual goes to one of over 100 enrollment centers to provide fingerprints and a facial photograph along with native documents (e.g., passport, proof of residency) for review by CBP. The biometrics collected at enrollment are used for facial matching.

Table 2-4: Key Points for CBP Trusted Traveler Case Study

Criteria	Overview
What	• Expedited clearance for pre-approved, low risk travelers
Where	• 75 U.S. ports of entry (POE), including preclearance airports
Passenger Process	• Individuals have their picture taken at the automated border kiosk
Who	• Customs and Border Protection • Department of Homeland Security

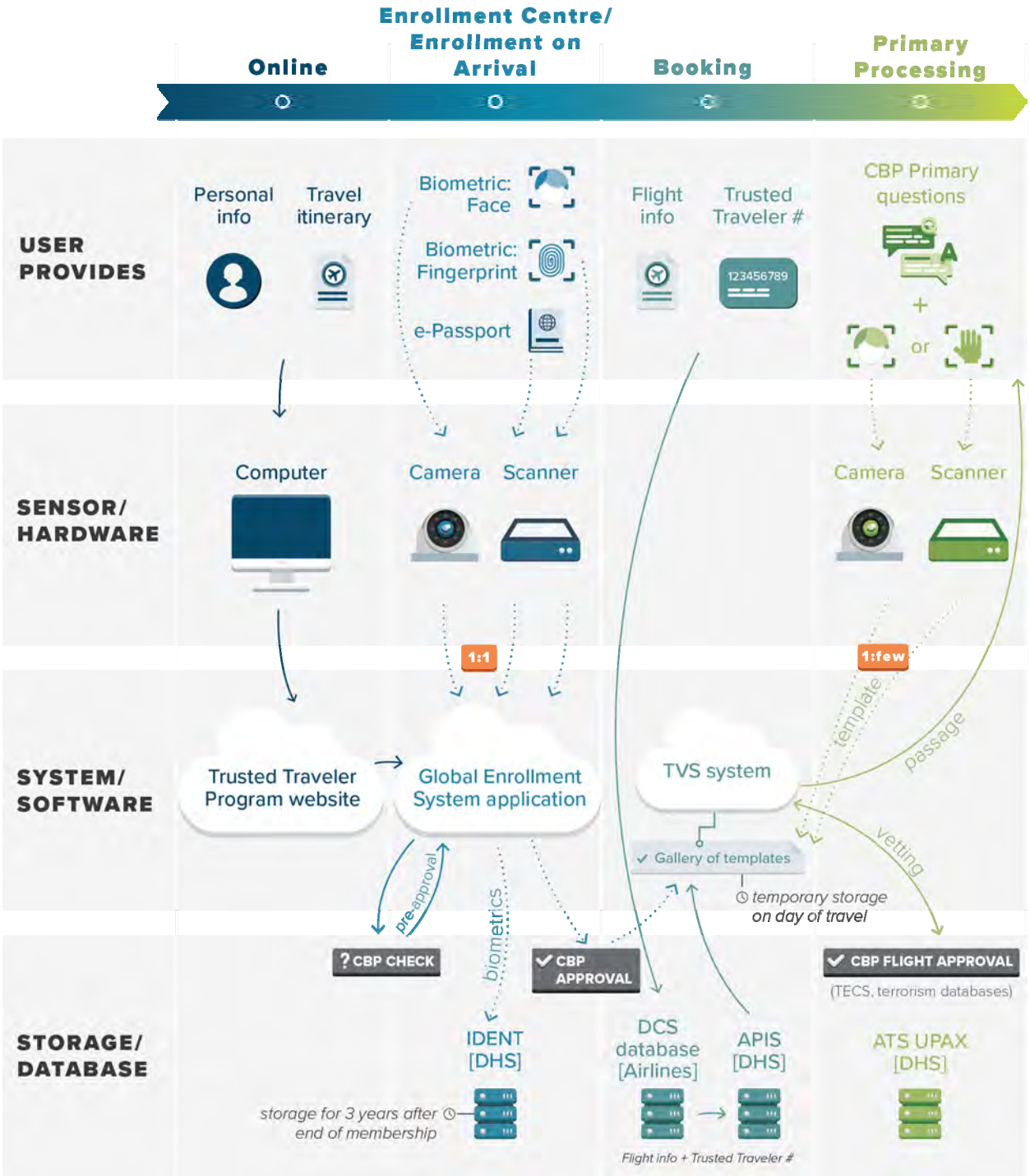
Criteria	Overview
	• Participating airports
Why	• To fast-track border crossing procedures for individual travelers who are deemed low risk
How	• Verification of identity through facial recognition
Enrollment	• Voluntary program with multi-step application process including an in-person interview
Verification of Identity	• Facial recognition • At enrollment: Passport, Photograph, Fingerprints
For	• U.S. citizens and lawful permanent residents, and citizens of certain countries

Program Key Takeaways

The Global Entry® program provides an ability for airports to safely and securely facilitate international air travel for not just U.S. citizens, but a range of country nationals (S. Korea, Canada, UK, etc.). The program presents a solution to identify low-risk passengers by vetting pre-approved travelers in advance of their trips, thereby streamlining the clearance and screening processes. An added benefit is that members are granted clearance to use TSA PreCheck™.

Case Study #3

CBP Trusted Traveler Programs at U.S. Airports



Case Study 4: Seattle-Tacoma International Airport and Designated Aviation Channeling

Summary

Pursuant to the Aviation Transportation Security Act, TSA requires all employees of airport authorities, airline carriers and other airport stakeholder employees who require unescorted access to secured areas of an airport to submit an application and be approved for a Secure Identification Display Area (SIDA) badge. The intent of doing so is to screen an applicant's information against Federal criminal and immigration databases to determine whether the applicant is a threat to transportation or national security.

Program Concept

For airports using Designated Aviation Channeling (DAC) vendor services, the process for a SIDA badge begins when the airport employee submits the application, supported by authorized signatories (or endorsers), to the DAC vendor. Specifically, the application consists of obtained employee biometric and biographic information and, in some cases, additional information may be required (e.g., I-9 document). After the application is completed, a DAC vendor ensures that the application is complete, properly formatted, and verifies the employment and education information provided.

The application is accompanied by fingerprints and a photo which is electronically submitted to TSA for a Security Threat Assessment (STA) and to the Federal Bureau of Investigation (FBI) for a Criminal History Records Check (CHCR). Upon approval of the application by TSA, the results are provided to the airport operator and a badge is issued. The badge authorizes access to secured areas of an airport, and depending on the biometric technology in use at the airport and by the employer, could be scanned for timekeeping purposes.

Table 2-5: Key Points for SeaTac DAC Case Study

Criteria	Overview
What	• Designated Aviation Channeling for aviation employee background checks
Where	• Multiple airports in the United States (e.g., Seattle-Tacoma International Airport)
Passenger Process	• Application-based process
Who	• Airports across the United States
Why	• Mandatory requirement for all airport and airline employees seeking unescorted access to secured areas, except Federal state or local government employees. • Ensure safety and security to general public and nation • Requirement by TSA
How	• Fingerprints and in some cases a photo (biometrics) • Criminal history background check • Biographical information
Enrollment	• DAC screening application.

Criteria	Overview
Verification of Identity	• Vendor representative ensures all information is correct and accurate during application
For	• Airport employees, airline carrier employees and select aviation stakeholder employees

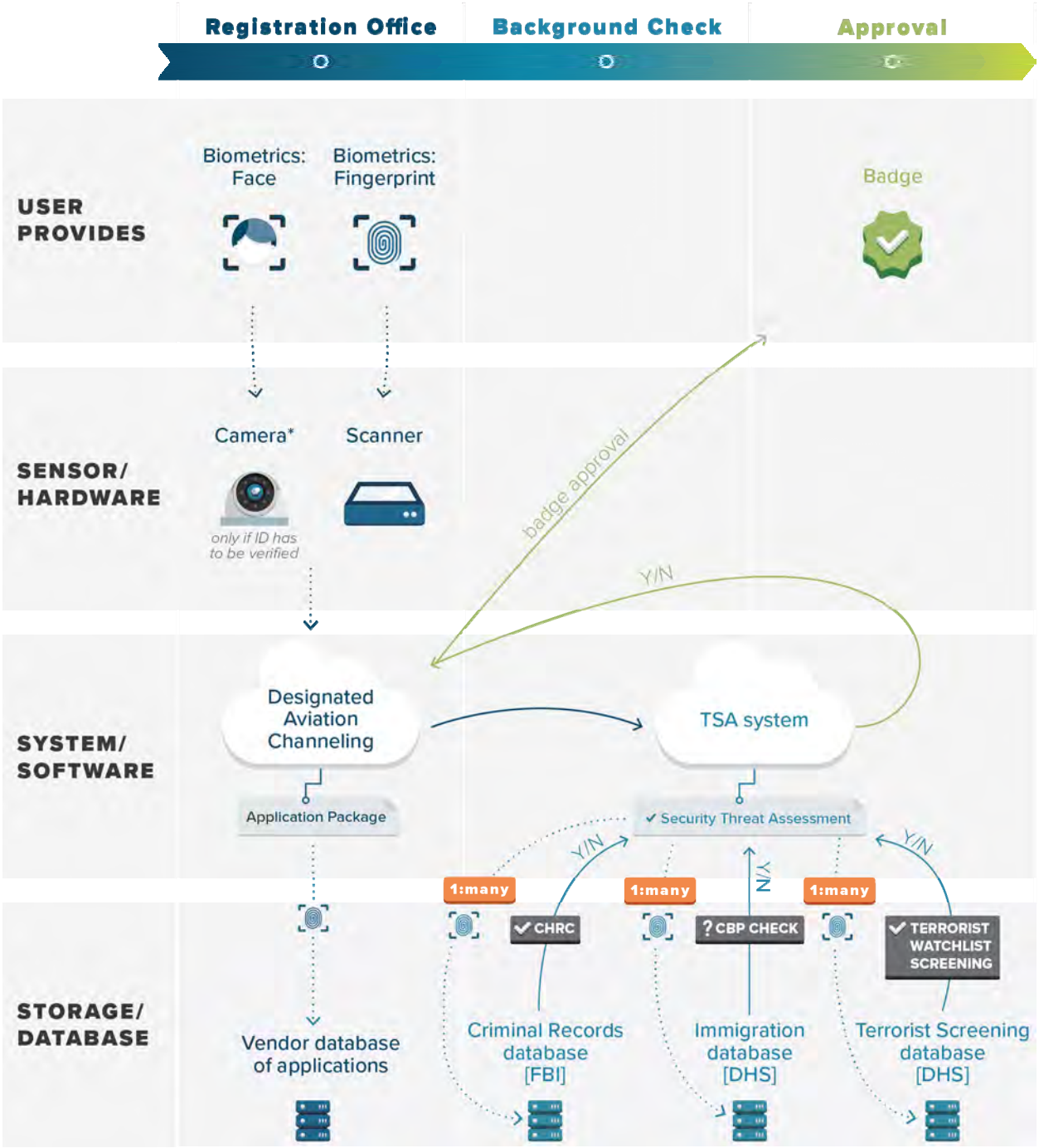
Program Key Takeaways

The DAC model is a prime example of a public private partnership in the handling of biometric and biographic data. More specifically, the use of DAC enhances current protocols and represents a set of comprehensive procedures for improved handling of personally identifiable information.

- The DAC model is an example of a public private partnership in handling biometric/biographic data.
- Evolution of protocols for handling personally identifiable information offers a good example of protocols.

Case Study #4

Seattle-Tacoma International Airport and Designated Aviation Channeling



Case Study 5: Curb-to-Gate Program by CBP and Delta Airlines at Atlanta International Airport

Summary

CBP's Curb-to-Gate Program is an application of facial recognition with the intent of reducing the number of times passengers must present their form of identification and boarding pass, as well as an increase in the reliability and efficiency of both airport CBP and security officers.

Program Concept

The Curb-to-Gate Program led by CBP and Delta Airlines allows passengers to verify their identity in a reliable and more efficient manner through leveraging CBP's Traveler Verification System (TVS):

- At check-in/bag-drop, a real-time photo is sent securely and encrypted to TVS
- The incoming photo is matched to a biometric template in a pre-compiled library, based on the airline's passenger manifest for a specific flight.
- In case of a positive match, the passenger's ID is verified and the use of facial recognition for the rest of the journey is enabled.
- At bag-drop, security and boarding, the passengers' identity and right to entry/passage is verified using facial recognition.
- For border crossings, an entry/exit record is made in the Arrival & Departure Information System (ADIS).

Table 2-6: Key Points for CBP's TVS with Delta at Atlanta Case Study

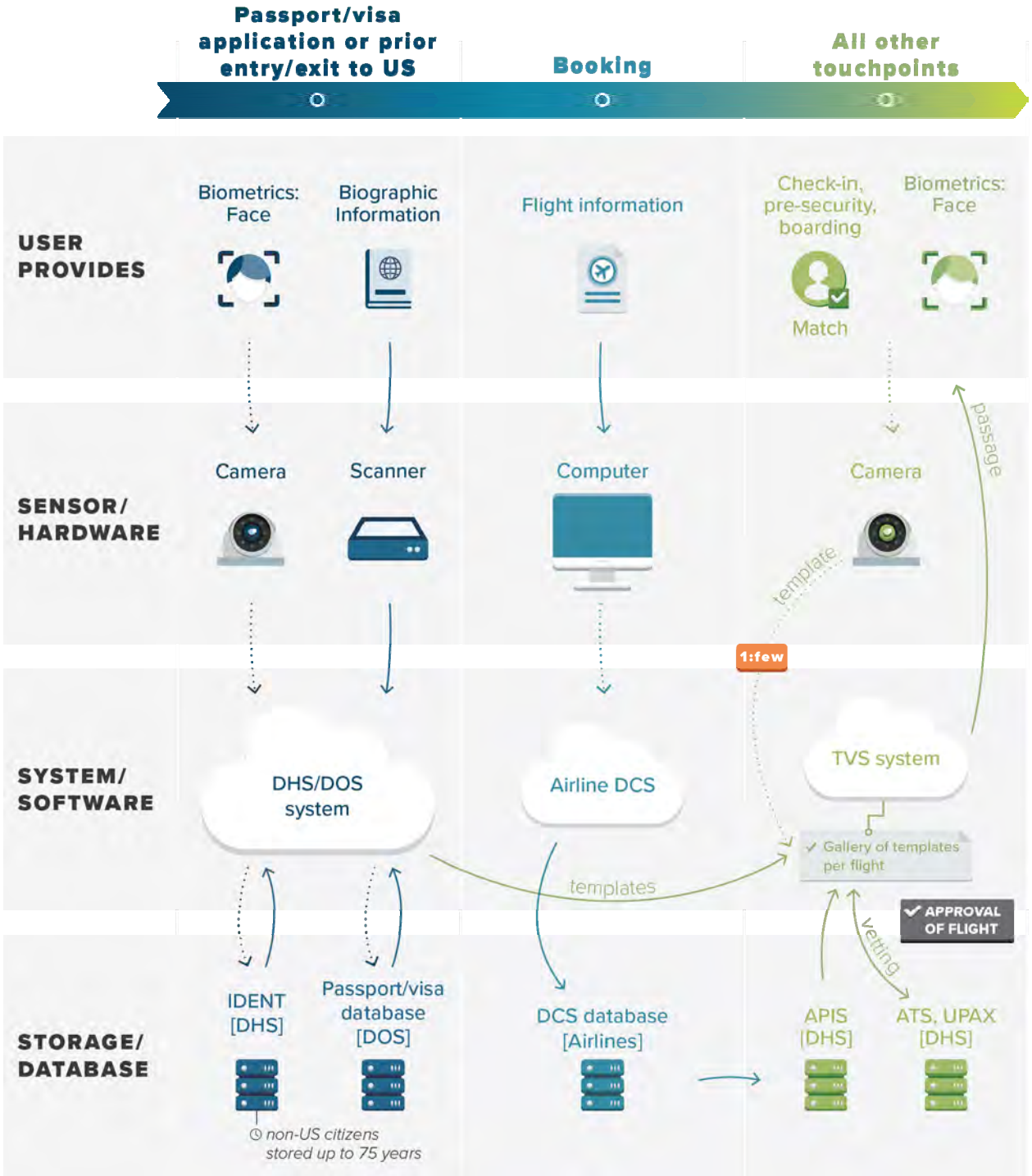
Criteria	Overview
What	• Seamless flow through facial biometric matching
Where	• Hartsfield-Jackson Atlanta International Airport (first pilot)
Passenger Process	• Opt in at check-in/bag-drop • Have photo taken at other touchpoints
Who	• Partnership among CBP, Delta Airlines, Hartsfield-Jackson Atlanta International Airport, and TSA. • NEC (technology and software). • Department of Homeland Security, Department of State
Why	• Speed passenger processing
How	• Cameras, including those in tablets. • Matching live photo taken at passenger touchpoint with pre-loaded library of biometric templates.
Enrollment	• No formal enrollment, collected when applying for a passport/VISA or at entry/exit from the United States.
Verification of Identity	• Facial recognition and 1:few matching.
For	• International flights with Delta and its partners • Expansion planned to U.S. domestic flights

Program Key Takeaways

The benefits of utilizing the Curb-to-Gate are: specific and measurable time savings for passengers and airport personnel at border processes, check-in, TSA and other processes; lower operational expenditures for airports; optimization of the use of space throughout the airport; and an opportunity for airports to revolutionize the passenger travel experience. Additionally, Curb-to-Gate significantly reduces the number of physical interactions amongst airport stakeholders, thereby lowering the probability of transmitting diseases and hazardous pathogens (e.g., COVID-19, etc.). Furthermore, this represents a significant milestone in terms of the power of end-to-end facial recognition and demonstrates the capabilities of biometric software. Lastly, this case study demonstrates the capability of leveraging biometrics without the need for re-enrolment.

Case Study #5

Curb-to-Gate Program by CBP and Delta Airlines at Atlanta International Airport



Case Study 6: Known Traveller Digital Identity at Aéroport International Montreal-Pierre Elliot Trudeau, Montreal, Canada

Summary

To respond to the increasing demand for a more efficient and streamlined passenger process, the World Economic Forum (WEF) has launched a program for the development of a trusted digital identity based on biometric technology. The goal of this initiative is to make it possible for all industry partners to use this digital identity securely and with ease of use, while protecting the passenger's privacy.

Source: KTDI.org

Figure 2-4. Known Traveller Digital Identity

Program Concept

The program is still in the early development phase and relies on the "self-sovereign" concept where passengers are the owners of their personal data and can elect to share it (or not) with different parties (e.g., airport, airlines, border authority) at different filters throughout their journey. The digital identity should be created by an identity issuing authority (3rd party or government). This authority would create a biometric template of the passenger as well as a unique security feature. With the use of distributed ledger technology, the immutability of the digital identity can be secured.

The Known Traveller Digital Identity (KTDI) concept aims to use the distributed ledger to register every successful identity claim at various authentication touchpoints in order to build up trust in the passenger. In 2018, the Governments of Canada and The Netherlands established a pilot-group to advance the KTDI efforts.

Table 2-7: Key Points for KTDI and DTC Case Study

Criteria	Overview
What	• KTDI concept, developed by World Economic Forum and partners
Where	• Amsterdam Airport Schiphol (AMS), • Montréal-Pierre Elliott Trudeau International Airport(YUL), • Toronto Pearson International Airport (YYZ)
Passenger Process	• Create digital identity at issuing authority • Passenger manages own identity and information sharing to various airport stakeholders

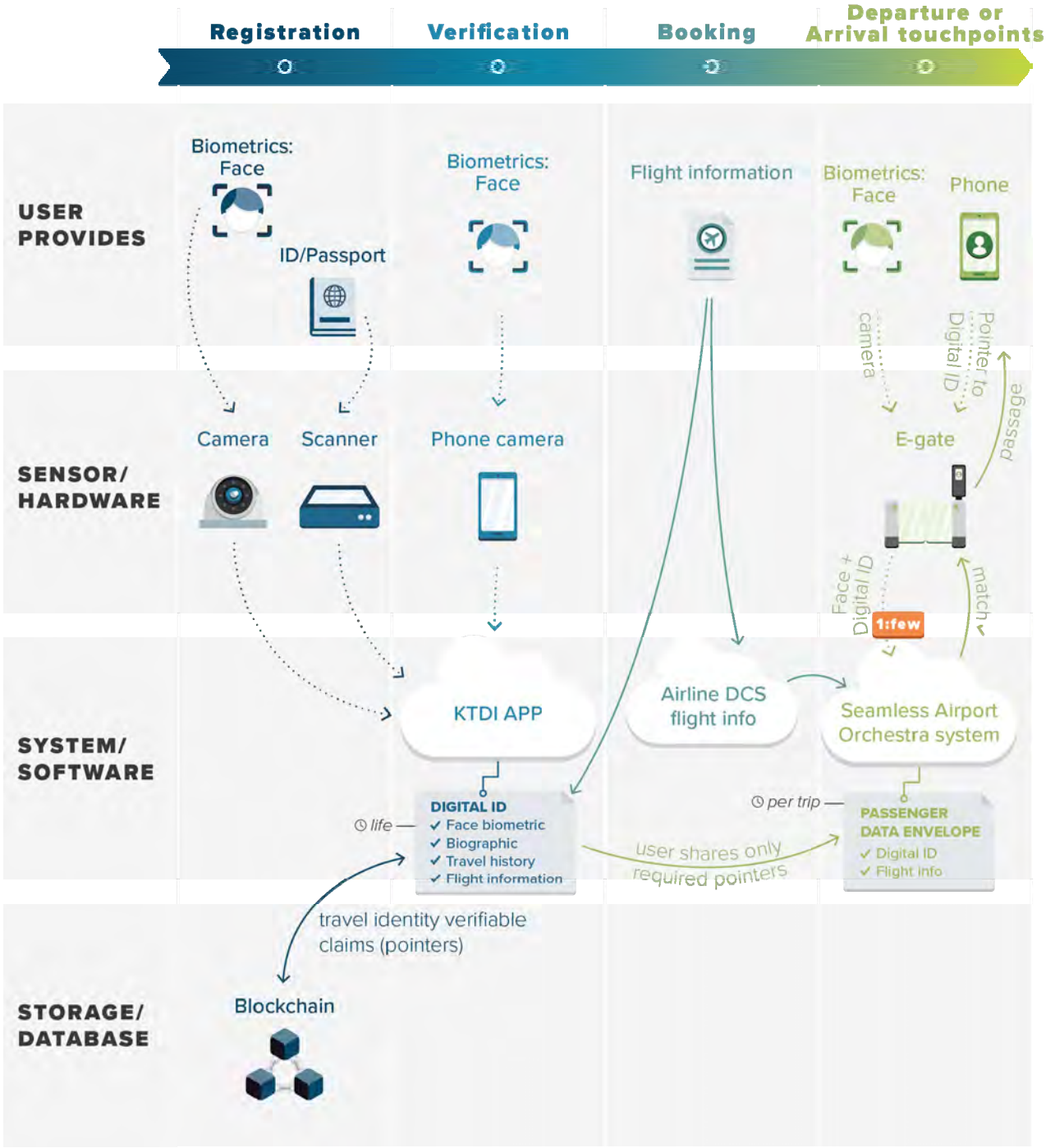
Criteria	Overview
	• Digital identity can be used for all processing steps at the airport (like seamless flow)
Who	• World Economic Forum • Airports: AMS, YUL, YYZ, • Airlines: KLM, Air Canada, • Governments of Canada and the Netherlands, • Private partners: Vision-Box, Accenture, Idemia
Why	• Create a trusted interoperable ID verification system that can be used around the globe • Avoid the creation of multiple proprietary solutions that make the passenger process more confusing • Create a solid solution for data privacy protection • Create a framework that enables self-sovereign sharing of data required for the destination of the passenger (health information, Advanced Passenger Information System (APIS))
How	• Facial recognition technology, biometric-enabled processing points (e.g., e-gates) in combination with blockchain technology
Enrollment	• Voluntary
Verification of Identity	• Upon enrollment by matching the face with the image that is stored on the e-Passport chip • At authentication touchpoint by face recognition, when required with additional credential (smartphone or e-Passport)
For	• Dutch and Canadian citizens that enrolled in the program

Program Key Takeaways

In the KTDI project, the challenge for the large group of stakeholders from two different countries, including their two respective governments, was on the agreement of sharing, transmission and storage of information and biometric data. To comply to all Canadian and EU privacy laws, mitigate cybersecurity risks and satisfy the private and public interests among the group, a lengthy process to tune the legal framework was required.

Case Study #6

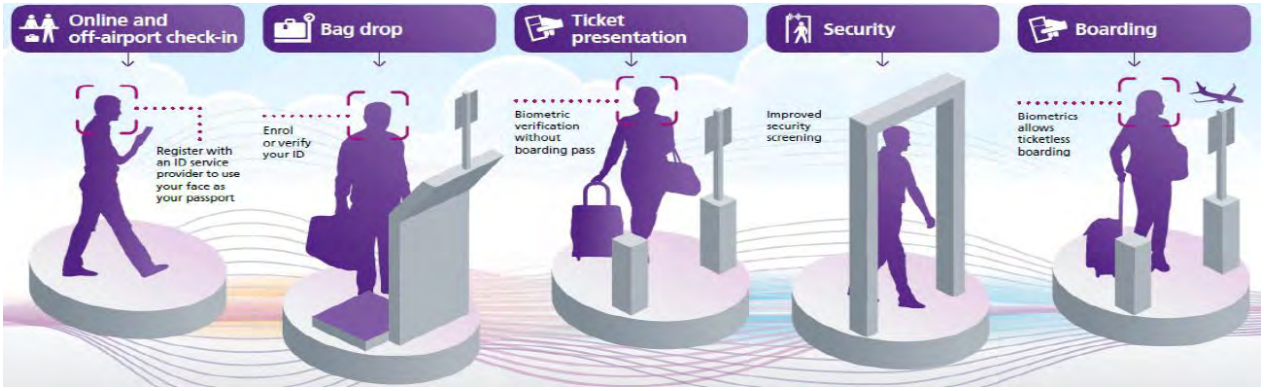
Known Traveller Digital Identity at Aéroport International Montreal-Pierre Elliot Trudeau, Montreal, Canada



Case Study 7: The Seamless Passenger Journey at London Heathrow

Summary

In the Seamless Passenger Journey, Heathrow Airport launched its first end-to-end biometrics program, which is built on the premise of utilizing facial recognition technology at the checkpoint of the departing passengers' journey. Part of the journey will involve biometric self-boarding gates, which will be installed across multiple terminals throughout the airport.



Source: London Heathrow International Airport.

Figure 2-6: Overview of Seamless Passenger Journey

Program Concept

Biographic and biometric data are captured at the first touchpoint (self-service check-in kiosk, self-service bag drop or ticket presentation gate) by reading the passenger's e-Passport chip, scanning their boarding pass and taking their photo, referred to as "image of the day". All information is then collected and stored in what is referred to as the "Passenger Data Envelope."

The biometric data stored in passengers e-Passport is compared to the image of the day and, if there is a positive match, the passenger's ID is verified and from that point onward, the image of the day is used to recognize the passenger throughout their remaining journey. This approach eliminates the need for any additional identification measures.

Table 2-8: Key Points for Seamless Passenger Journey Case Study

Criteria	Overview
What	• Seamless Passenger Journey using end-to-end biometrics
Where	• Heathrow Airport, London, UK
Passenger Process	• Processes vary by type of flight • Passengers present facial recognition at multiple airport touchpoints
Who	• Heathrow Airport, Atkins, Dormakaba, ICM, CEIA, Rockwell Collins, Arora
Why	• Streamline the passenger travel experience

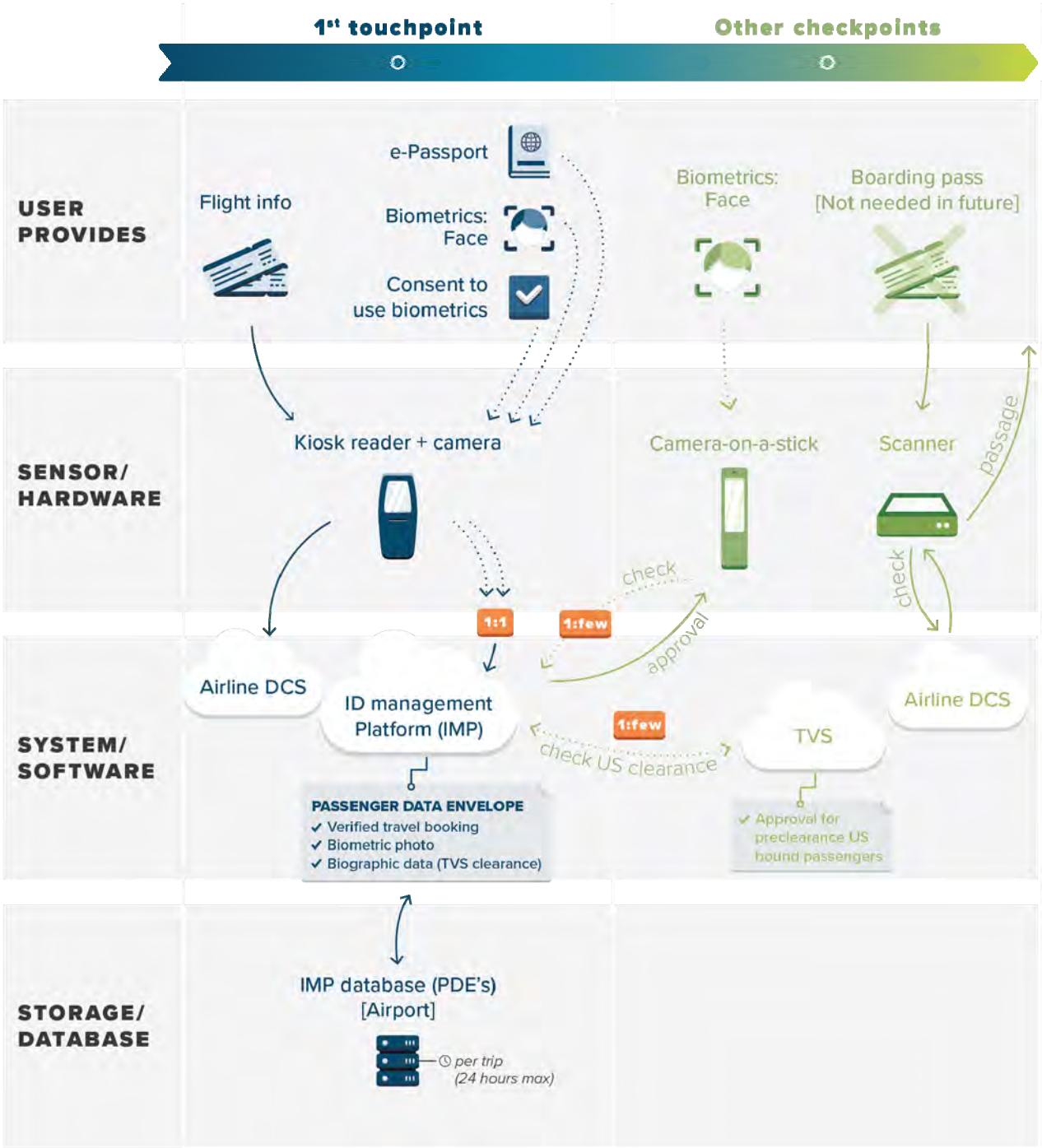
Criteria	Overview
	• Accommodate and prepare for anticipated increases in passenger demand levels
How	• Facial recognition at multiple check in points throughout the airport
Enrollment	• In person at self-service airport kiosks • Mobile enrollment to come later
Verification of Identity	• Matching an 'on the day image' taken of the passenger to that of their e-Passport
For	• Domestic and international departing flights

Program Key Takeaways

The Seamless Passenger Journey at Heathrow Airport provides a scenario where the use of biometric technology is scalable to large international airports, both in the short and long term. The quality and deployment across multiple terminals is a significant undertaking that can provide a seamless process. For passengers traveling to the United States, the Seamless Passenger Journey technology also provides ID cross-validation with CBP's Traveler Verification System.

Case Study #7

The Seamless Passenger Journey at London Heathrow



Case Study 8: Risk Management During COVID-19 Using Biometrics, Carrasco Airport, Montevideo

Summary

In 2016, Carrasco International Airport implemented a fully biometric boarding procedure as well as a biometrics border and customs checkpoint for arriving passengers. The program, referred to as Easy Airport, is the first self-service boarding system within the region based completely on facial recognition. The use of such technology has enabled border agents to initiate risk-profiling during the arrivals process, specifically related to issues stemming from the COVID-19 pandemic. Passengers arriving from low-risk countries are processed quickly, while passengers from higher risk countries are required to undergo additional screening.

Source: Carrasco International Airport.

Figure 2-7: Easy Airport e-gate at Carrasco

Program Concept

Departing passengers go through an e-gate for identity verification by facial recognition and are asked to select their flight on a touchscreen display to link the passenger information to the right flight. Boarding requires a positive facial recognition match.

Arriving passengers enter a similar e-gate for passport authentication, background checks and biometric identity verification. Significant reductions in per passenger processing times estimated down to 15 seconds, from 40-50 seconds.

Easy Airport was specifically designed for international travelers who are; Uruguayan, Argentinean, Brazilian, American or European citizens, are 18 years of age and older and have an e-Passport.

Table 2-9: Key Points for COVID-19 Risk Management Case Study

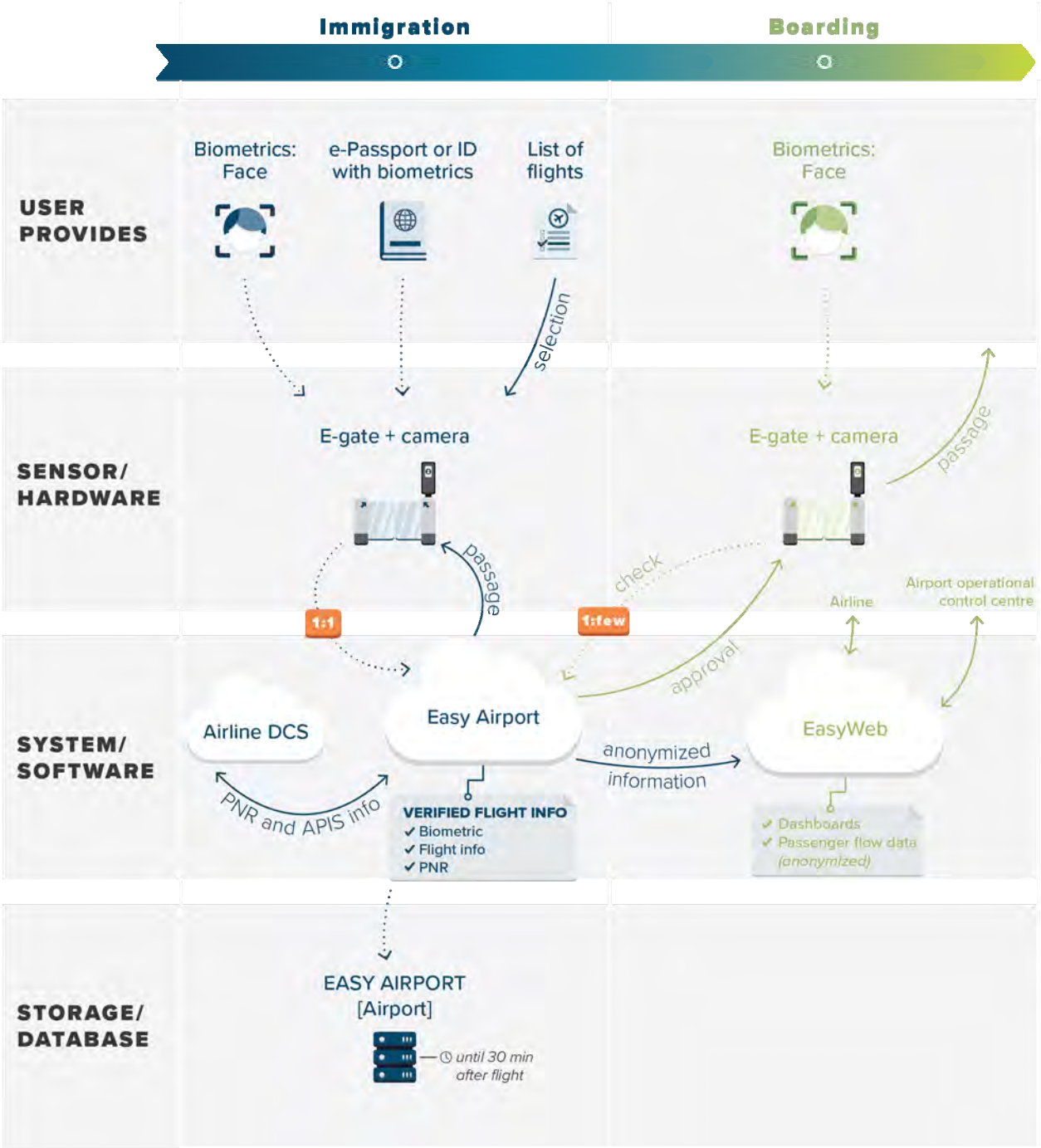
Criteria	Overview
What	• Biometric border crossing and boarding by facial recognition, and risk-profiling arriving passengers
Where	• Carrasco International Airport in Montevideo, Uruguay
Passenger Process	• Border e-gates to verify passport authenticity, passenger identity (and link to flight information) • Automated boarding e-gates via facial recognition
Who	• Corporacion America (Airport Authority), border and customs authorities and vendor: Vision-Box
Why	• Enhanced control and security • Facilitate passengers along their journeys
How	• Biometric e-gates
Enrollment	• No enrollment necessary, all is done at the e-gate
Verification of Identity	• Facial recognition matching to e-Passport
For	• Passengers from Uruguay, Argentina, Brazil, United States and Europe, with an e-Passport/biometric ID card

Program Key Takeaways

Easy Airport presented the ability to meet different airline business cases and strategic objectives, including resource and time savings. It also presents the opportunity to install state of the art technology and infrastructure to meet the airports future demand. The added data portals for airlines and other stakeholders provides additional value, which delivers anonymized data streams. More interestingly, Easy Airport, was used during the COVID-19 pandemic in risk-profiling passengers into specific categories, automatically, and notifying border agents of passengers entering the country from specific origins. Those passengers underwent a different (health) screening process.

Case Study #8

Risk Management During COVID-19 Using Biometrics, Carrasco Airport, Montevideo



Case Study 9: Digi Yatra and the Seamless Passenger Journey at Kempegowda International Airport, Bengaluru India (BLR)

Summary

Aviation in India has been growing at a considerable pace and is expected to become the world's largest domestic civil aviation market over the next 10-15 years. As a result, more emphasis has been placed on investing in innovation and digitalization to accommodate expected growth. To this effect, the Ministry of Civil Aviation has begun to implement an initiative known as Digi Yatra, which is designed with the intention of giving a seamless, hassle free and paperless experience to all air travelers in India.

Source: Ministry of Civil Aviation.

Figure 2-8: Overview of Digi Yatra

Program Concept

Under Digi Yatra, travelers in India are no longer required to show their boarding passes or proof of identity at touchpoints throughout airports within the country. Rather, the Digi Yatra biometric boarding system boarding pass will be integrated with a passenger identification document, ensuring faster and simpler processing at touchpoints such as the terminal entry gate, check-in/bag drop, security checkpoint, and boarding gates.

Table 2-10: Key Points for Digi Yatra Case Study

Criteria	Overview
What	Digi Yatra facial recognition boarding system
Where	Airports across India.

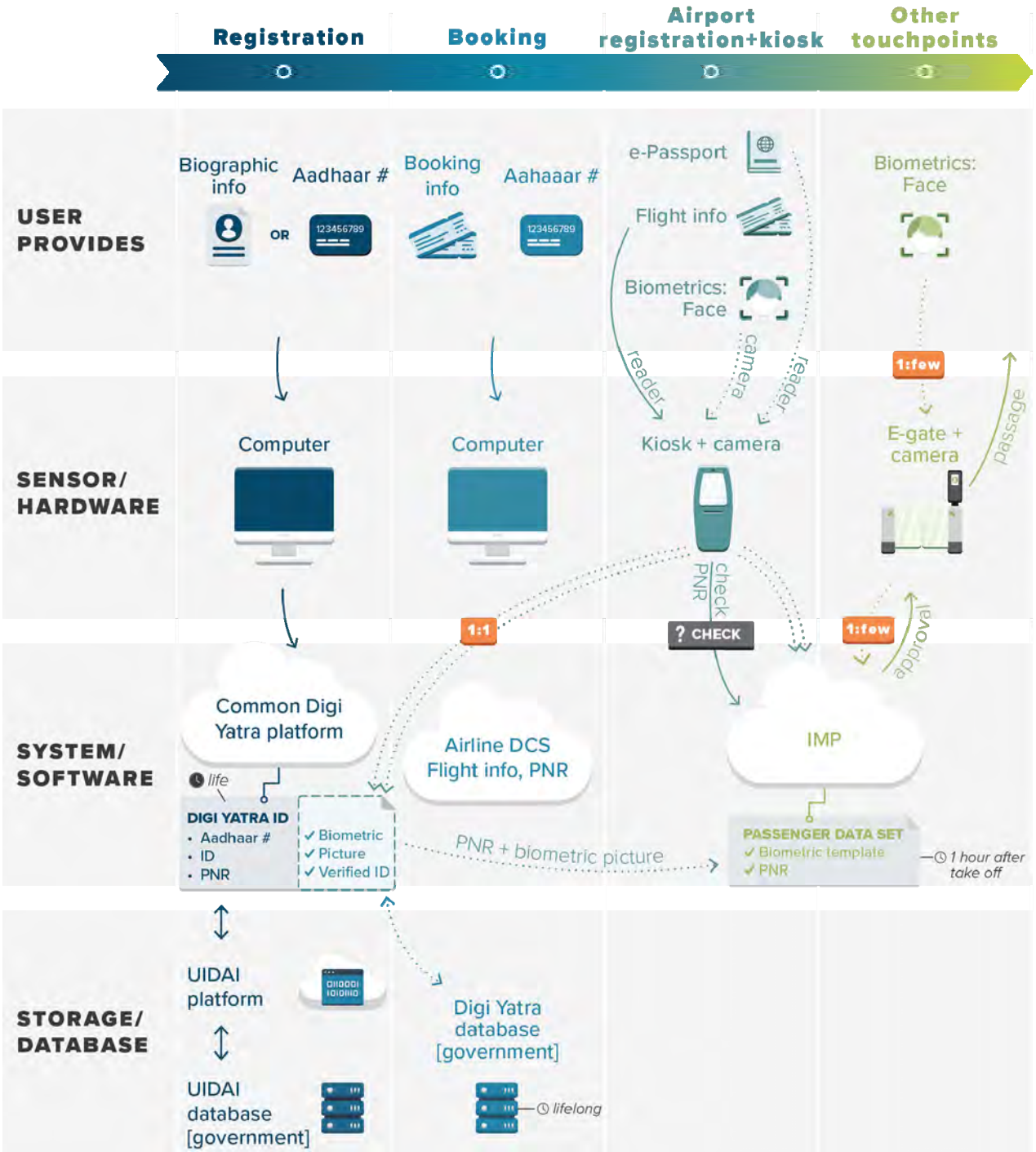
Criteria	Overview
	Kempegowda International Airport (first pilot)
Passenger Process	Register at unmanned-registration kiosks at airports across India.
Who	Airports throughout India Indian Civil Aviation Industry Airports Authority of India
Why	Remove redundancies, increase resource utilization and improve security
How	Registration kiosks at airports.
Enrollment	Voluntary Digi Yatra ID enrollment
Verification of Identity	Facial recognition matching with Government of India issued ID's (e.g., driver's license, passport, voter card, student ID, etc.).
For	Indian citizens and foreigners who travel in and out of India

Program Key Takeaways

The primary benefits of the Digi Yatra Program are that it removes redundancies at various touchpoints throughout airports by "using your face as boarding pass", enhances airport resource utilization rates and improves security and airport system performance. Likewise, the Digi Yatra Program results in lower operational costs for airports across India and allows them to achieve better throughput through existing infrastructures using a "digital framework." Moreover, the program has a relatively straight forward enrollment/ registration process, which is easy to opt-out of in case passengers prefer to manually check in.

Case Study #9

Digi Yatra and the Seamless Passenger Journey at Kempegowda International Airport, Bengaluru India (BLR)



Case Study 10: Happy Flow at Aruba International Airport

Summary

Happy Flow is aimed at improving the departure process at Aruba International Airport, by smoothing the flow, and creating a unique and seamless passenger experience. The program adopted protocols and standards that would benefit authorities, the airport and airlines.

Using facial recognition at multiple passenger touchpoints, passenger identity and right to travel are verified more securely. Plans are underway to include off-airport elements in the passenger journey (hotel check-in and car rental). In the initial launch of Happy Flow, there were also ideas to pre-clear into the European Schengen Area.

Source: Aruba Happy Flow.

Figure 2-9: Overview of Happy Flow

Program Concept

In the process, travel documents are only required at the enrollment station. There, the passenger's identity is securely checked under government set standards and the passenger's biometric is checked against the one on the travel document, and a (temporary) virtual identity is created. After enrollment, the passenger goes through self-service passenger touchpoints (bag drop, security, border control and boarding) where the passenger's face is matched to a secured database, only allowing authorized passengers to pass.

Table 2-11: Key Points for Happy Flow Case Study

Criteria	Overview
What	• Happy Flow Biometric Process for preclearance at border control crossing
Where	• Aeropuerto Internacional Reina Beatrix, Aruba International Airport
Passenger Process	• Enrollment • Baggage drop-off with biometric assistance • Biometric self-service border control checkpoint • Boarding e-gate with separate lane
Who	• Aruba Airport Authority, KLM Royal Dutch Airlines, Amsterdam Airport Schiphol and vendor Vision-Box

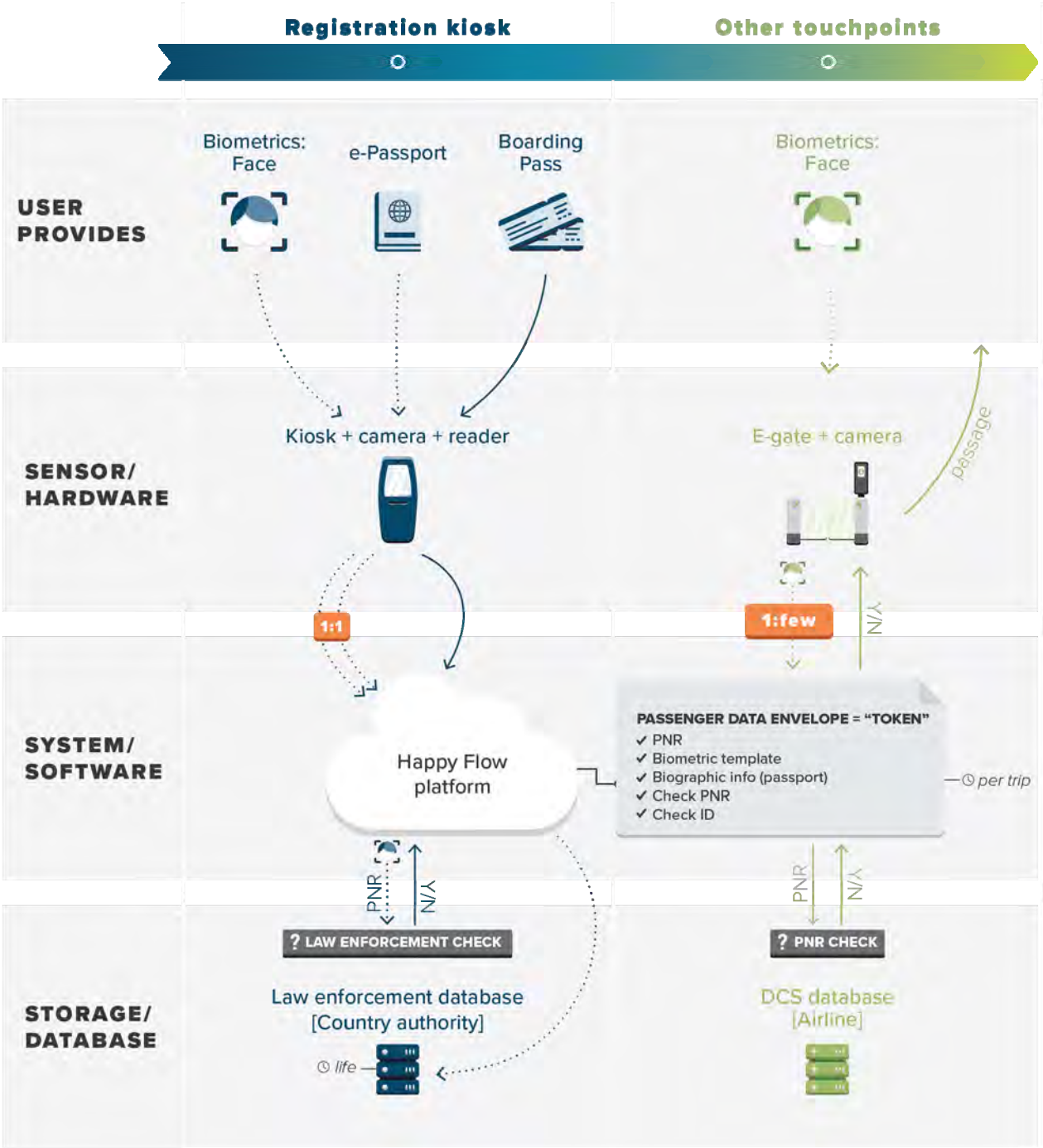
Criteria	Overview
Why	• Enhance the passenger travel experience • Streamlined, touchless airport journey for security and safety • Increase efficiency of operational processes of the stakeholders
How	• Facial biometric matching
Enrollment	• At a kiosk, passengers scan passport and boarding card, verify identity with data on passport and create a facial ID
Verification of Identity	• ID verification at kiosk • ID authorization at border control
For	• KLM departing passengers to AMS with e-Passport

Program Key Takeaways

As with other facial recognition initiatives and programs, the intent of Happy Flow was designed to promote a more streamlined departure process while improving overall security. It has been labeled a visionary model anticipating transatlantic preclearance. Enrollment is the most time-consuming step, while processing is very efficient after the biometric token is created. The system may be further optimized by introducing mobile enrollment using the ICAO Digital Travel Credential, as well as measures to counter identity fraud from off-site/mobile enrollment. Nonetheless, a broader vision for enrollments “on the beach” which would be possible within the program, may not be supportable by all stakeholders.

Case Study #10

Happy Flow at Aruba International Airport



Key Trends in Airport Biometrics

Based on the 10 case studies of recent deployments, there are five trends that are important to consider for the future of biometrics at U.S. airports. These five trends are:

- Trend 1: The deployment of integrated and multi-stakeholder biometric solutions is increasing, given its greater potential benefits
- Trend 2: Digital transparency and privacy concerns are adding to the complexity of implementation, particularly as the legal landscape changes
- Trend 3: A focus on identity verification solutions is evident, in part, to distinguish from mass surveillance programs that also leverage biometrics.
- Trend 4: Global biometrics and standards are emerging from a variety of governmental and non-governmental entities which are addressing privacy, security, ethical, and technological concerns.
- Trend 5: Smartphones are expected to enable greater use of biometrics through the on-device storage capability for biometrics, as well as the promise for the transmission of digital travel credentials.

KEY TAKEAWAY

These trends portend the future development of solutions that may be more integrated, transparent, and privacy conscious. Solutions may offer more secure identification, within globally accepted practices, with the enabling technologies leveraging smart devices, linked to our biometrics.

Figure 2-9. Overview of five key trends on airport biometrics

Trend 1: Deployment of Integrated and Multi-Stakeholder Biometrics is Increasing

Where We Were:

Airport biometrics were previously constructed around single-purpose ideas. Access control, for example, created an environment where a biometric clearinghouse was compiled to create a relationship with credentialing systems.

Where We Are Going Now:

We are now moving into a world where a single enrollment could have multiple stakeholders using the system. The premise is that the overall cost of having five separate enrollment centers for five different stakeholders could be combined together. Known as interoperability, there are multiple ways to enable a single biometric to be used across airlines, government(s) and airports.

Typically, stakeholders have depended on a face-to-face customer service model. Physical interaction with customer service representatives may increasingly be the exception and possibly available as a premium service, especially during the COVID-19 recovery period. One cannot efficiently accommodate the multiple groups, from ride share, car rental, airlines, government agencies and other parties each having their own enrollment stations and different biometric technologies.

As a result, a multi-stakeholder model is the preferred direction to reduce the number of in-person contact points and provide the greatest overall system benefit.

Key Examples

- CLEAR®: can be used at the TSA checkpoint, airline lounges, flight boarding, as well as for access to some professional sporting events (e.g., National Football League, Major League Baseball)
- DHS Office of Biometric Identification Management: since 2003, the image collected with a visa application used to confirm identity at POE, as well as for applications involving TVS.

Trend 2: Digital Transparency and Privacy Concerns Increase Complexity

Where We Were:

There are privacy laws and policies used for public and private sector deployment of biometric solutions. Many of these have strict requirements governing the use, retention and disposal of personal information. On occasion, lapses of data ownership have occurred, such as the disposal of assets of Verified Identity Pass in 2009.

Where We Are Going Now:

A heightened attention is advancing regarding the threat of cybersecurity attacks, theft of personal information as well as vulnerabilities associated with privacy. Confusion and in some cases a lack of awareness of risks exist within the traveling public.

It is not good enough to simply tell the public “we will keep your information private” or provide an opportunity for an “opt-out” solution. Privacy advocates are calling for more sophisticated solutions to ensure that easy-to-use tools are available especially when accountability is spread among airline, governmental and other third-parties.

Key Examples:

- Perceptics data breach: major lessons learned from 2019 when information on facial recognition was improperly stored, resulting in access from unauthorized parties.
- Self-sovereign biometrics: different models to reframe the control of the individual on identity and usable across governments, airports and airlines.
- Digital Trust in Places and Routines: a project that creates standard communications methods, signage symbols and accountability notices to make it easier to communicate to passengers.

Trend 3: Identification Verification Solutions (Not Mass Surveillance)

Where We Were:

We have equated the word "biometrics" to equally represent all forms of algorithms and techniques to manage identity. An analogy can be made between the word "password" and biometrics to the general public – there are strong secure passwords and there are poor, ineffective passwords.

There are a number of emerging mass surveillance solutions that are comprised of public and private databases. Clearview AI, for example, leverages 3 billion images taken from Facebook, Instagram, and other social networking platforms to supply clients with identity information. Although many governments have invested heavily on national biometric registration and identity systems, only a few have some features constructed with mass surveillance in mind.

Where We Are Going Now:

Current and proposed uses of biometrics at U.S. airports are significantly narrower in purpose. They are related to an express purpose (facilitate process, manage identity) and are formulated to verify identity, not conduct mass surveillance.

However, due to the high-profile nature of Clearview AI and the rapid advancement of alternate biometric models, there can easily be confusion and a lack of consumer confidence about proposed solutions. A key trend emerging involves airlines, airports and governments adopting "identity verification" as the description of the program being deployed. In so doing, the roll-out of biometric solutions can be distinguished from mass surveillance applications that tend to inflame the user base.

In other words, instead of referring to solutions as "facial recognition" or "biometrics" – which imprecisely implies a set of unfettered processes – airport operators may more precisely refer to processes as "identity verification solutions." In addition to appropriate terminology, it is imperative that airport operators and others wishing to deploy biometrics-enabled initiatives do so within a framework consistent with best practices with respect to data security and privacy considerations.

Key Examples:

- TVS may be powered by biometrics, but is accurately described as an identity verification solution, which differs from mass surveillance.
- "My face is my boarding pass": Plain speaking solutions are being used within the Digi Yatra program in Bangalore, India which clearly communicates the focused nature of the solution.

Trend 4: Global Biometrics and Standards Taking Hold

Where We Were:

It was only in the 1980s when passports became standardized by the International Civil Aviation Organization. Over the past 20 years, the ICAO standard included a chip within a passport for the current e-Passports. Yet the work is not complete for the original vision of e-Passport rollouts. Visas were originally meant to be stored in a larger capacity chip. Other data including more advanced encryption mechanisms using public key infrastructure were also meant to be augmented to reduce the potential for document fraud.

Where We Are Going Now:

The Digital Travel Credential (DTC) represents the first major change in document standards since ICAO's Document 9303 was modified to include e-Passports. There are a number of options relevant to biometrics, including the mechanism to store information (blockchain, mobile phone, e-Passport) and also grow capabilities to better manage digital identities.

The key aspect of the DTC platform is to enable interoperability in a standard fashion. In other words, there is the ability to ensure that incompatibilities (e.g., Video Home System (VHS) vs Betamax video tapes) have a pathway established for exchanging digital identity information.

Key Examples:

- Passport-free travel: a number of countries including Canada and multi-lateral regions such as Mercosur, are evaluating DTC as a mechanism to contain traveler information.
- Health information: while there are a number of advancements contemplated associated with COVID-19 recovery, there are applications to include certain health information rooted on the ICAO Digital Travel Credential platform. The so-called "health passport" containing personal health information and immunization records may be an augmentation that different countries adopt in the future.

Trend 5: Leveraging Smartphones

Where We Were:

When biometrics first started being used broadly at airports in the 1990s, it was exclusively for voluntary products such as INSPASS trusted traveler models. There is still a strong value for the face-to-face interaction between an officer and an individual when going through certain regulated processes, such as clearing through a POE into the United States.

Where We Are Going Now:

Many applications for biometrics exist on mobile smartphones, but these mostly relate to device unlocking, mobile payments and some identity information to be transferred across the internet, such as a passport photo page.

Increasingly, there are mobile applications that leverage still photos or live video interviews in order to integrate voice/video/data. Such applications can include biometric identity verification, allowing it to be done remotely and seamlessly.

Where there are doubts about the identity of the individual, there may be a triaged process to help with increased confidence of identity verification during a trip. In so doing, there is a home, hotel or office-based interaction that can create a provisional biometric record, that is then fully vetted on-site at an airport on the next journey.

Key Examples:

- The proliferation of health information passes, such as Commons Project CommonPass, IATA TravelPass, that are built around a smartphone app to house personal information such as a COVID-19 test result, vaccination status or other information such as photographs
- Mobile passport control, offered by a third party or in 2021 by CBP directly, that includes the ability to scan the machine-readable zone of a passport picture page through a smartphone camera

Chapter 3

Legal, Policy, and Privacy Review

Summary

To pursue biometrics as potential solutions to challenges in aviation, industry stakeholders need to understand the legal, policy, and privacy issues associated with the use of biometric data. The two predominant policy and legal issues associated with the use of biometric data, including facial recognition, are protection of privacy rights and the inconsistent treatment under a myriad of international, federal and state laws.

The chapter explains basic constitutional principles associated with the collection of biometric data; the few federal laws applicable to the use of biometric technology and the proliferation of inconsistent state laws; on-going federal government activities and the role of airport operators, carriers, and tenants, including any litigation risks; privacy principles applicable to the aviation industry; significant court decisions, particularly those eroding traditional precedents because of the use of heightened or pervasive biometric technology; penalties and costs of litigation for violations of law; increasing collaboration of international organizations initiatives; and best practices, applicable standards and Privacy by Design principles; and international regulations that offer airport operators and stakeholders the safest course of action in their roles as airport operators, transportation industry providers, and retailers.

While the predominant concern under the Constitution is the right to privacy, of equal concern is the fact that in the absence of a comprehensive national law, individual states have passed laws, a handful of which limit/prohibit the use of biometric data specifically, some of which address sensitive personal data, and all of which require action and notices upon breach of the systems. Many of these laws impose sanctions for failing to meet requirements pertaining to collecting and protecting biometric data.

Another emerging trend is the development of laws and restrictions by other countries, the EU, and international organizations, some with a broad reach that may impact airport operators and airlines in the United States, to include the assessment of penalties for non-compliance.

There are many sources of best practices for the protection of personal privacy. These include Privacy by Design, 2019 EU Data Protection Guidelines, and Fair Information Practice Principles which offer guidance on transparency, adoption of policies and practices that incorporate privacy protections, communication tips, and other similar practices.

Introduction

To pursue biometrics as potential solutions to challenges in the aviation industry, it is first necessary to understand the legal, policy and privacy issues associated with the use of biometric data. The two predominant policy and legal issues associated with the use of biometric data, including facial recognition, are protection of privacy rights and the inconsistent treatment under a myriad of international, federal and state laws.

Protection of privacy rights is the most prevalent concern surrounding the use of facial recognition. Some contend that the use of facial recognition is a violation of privacy rights, that such use may infringe on constitutional rights, and that systems where biometric data are stored provide inadequate legal and

security protections from breaches, abuses, and criminal activities.[1] As discussed in the subsection on state laws, the majority of recent lawsuits assert violations of state law by private sector businesses.[2]

Additionally, notwithstanding the increased efficiencies and security benefits associated with facial recognition technology, media reports highlight concerns over the effectiveness of the technology, with claims that facial recognition has a high rate of misidentification and bias.[3] Further, federal studies report that differing algorithms resulted in differing degrees of misidentification and bias.[4] In a recent wave of criticism associated with allegations of racially-based policing and the potential abuse by law enforcement engaged in surveillance activities of crowd demonstrations, giants in the industry, Amazon, Microsoft, and IBM have either suspended or terminated production and/sale of the technology.[5]

A recent legal and policy trend in the area of biometrics has been a proliferation of state laws that address a wide range of biometric technology issues such as data breaches, use restrictions, bans on police use, etc. The legal landscape with respect to state laws is non-uniform and in flux.

Another area of legal divide reflected in both federal and state laws is whether the entity collecting and using the biometric data is a federal or state agency or a private sector or commercial entity. There are no uniform legal requirements for: the protection of biometric data; which parties are responsible for protecting data; and, what types of data are entitled to protection and under what circumstances. Thus, the state of the law, more specifically with respect to the collection, use, protection, retention and disclosure of biometric data, is unsettled and evolving.

Notwithstanding the state of the law, changes and advancements in the technology itself arguably serve to mitigate litigation risks. For example, in the past facial images were retained in mass storage as photographs, whereas now facial "templates" are stored as numbers using sophisticated algorithms, and in most cases encrypted. With the use of facial templates and encryption, some concerns about data breaches have been addressed. Additionally, the courts have begun to debate/distinguish between capturing a photograph versus application of a biometric template to a facial image, bringing it within the scope of a state biometrics law. [6]

In recent years, state legislatures, privacy advocates, and free internet proponents have focused on cybercrime, i.e., hacking and misuse of data, and debated the need for (or opposition to) the application of additional security measures such as encrypting personal data to lessen the risk of access to and ease of illegal use of the data in the mass storage of data or jpeg files.[7] As a general rule, use of biometric data for the management of employees and for commercial operations is principally governed by state law.[86]

There is no comprehensive *federal* law governing the collection and use of biometric data, including industry employees' and/or consumers' privacy.[9] Under a "patchwork"[10] of federal laws, there are provisions aimed at providing privacy protections for individuals' data in specific industry sectors, such as: limitations on federal agencies' collection of personal information (if relevant and necessary to comply with a legal mandate);[11] protections for medical and financial data;[12] and limited enforcement action for unfair and deceptive practices.[13] In the absence of any overarching federal framework, states have been enacting and/or amending laws to protect its residents' privacy regarding biometric data, particularly facial recognition data.[14]

Airport operators and stakeholders, such as airlines and vendors, not only must comply with applicable federal and state laws that apply to biometric collection and use for employees and consumers, but in certain circumstances must confront conflicting laws from multiple states, and other countries and/or international organizations. Airport operators face differing risks and requirements depending on whether they are using biometric data collection for employee timekeeping, access to restricted areas or other airport operational purposes or dealing with passengers to facilitate travelers' experience or retail purchases.

What follows in this chapter is a summary of key legal and policy issues and trends associated with the use of biometrics in the aviation environment. (Additional detailed discussion is set forth in Appendices 10-12). In particular, the chapter highlights:

- basic constitutional principles associated with the collection of biometric data;

- the few federal laws applicable to the use of biometric technology and the proliferation of inconsistent state laws;
- on-going federal government activities and the role of airport operators, carriers, and tenants, including any litigation risks;
- privacy principles applicable to the aviation industry;
- significant court decisions, particularly those eroding traditional precedents because of the use of heightened or pervasive biometric technology;
- penalties and costs of litigation for violations of law;
- increasing collaboration of international organizations initiatives;
- best practices, applicable standards and Privacy by Design principles, and international regulations that offer airport operators and stakeholders the safest course of action in their roles as airport operators, transportation industry providers, and retailers; and
- Guidance on mitigation of risk of litigation and findings that support a responsible framework for use of biometrics in the air environment.

Interplay of U.S. Constitution, Federal Laws, and State Laws

The legal concern most frequently raised in connection with the use of biometrics, and in particular facial recognition, is the right to privacy. The body of law defining the right to privacy is an amalgam of concepts evolving from multiple sources: common law, the Fourth, First, and Fifth Amendments to the U.S. Constitution, and applicable federal and state laws.[15] In other words, there are many sources (and types) of privacy rights that may be implicated depending on the particular use of facial recognition, who is using it, and the nature of the violation asserted.[7] What follows is a discussion of those legal considerations mostly associated with the use of biometrics, especially facial recognition, in an airport environment.

KEY TAKEAWAY

This section provides a basic outline about the "patchwork" set of privacy laws under federal and state law, touching on areas relevant to aviation stakeholders.

The Right to Privacy under the U.S. Constitution

The U.S. Constitution protects privacy from *governmental*[8] invasion, and this includes state and local authorities operating in the airport environment. Protection of a person's right to be let alone by private parties is left largely to the law of the individual states.[9]

While the Constitution does not explicitly mention any right of privacy, the Supreme Court has declared that the right of privacy is a fundamental right guaranteed by the Constitution.[10]

Privacy advocates have challenged the collection and disclosure of biometric data under the provisions of the Fourth and Fifth Amendments of the Constitution.[11] The Fourth Amendment to the U.S. Constitution provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause..." and the Fifth Amendment provides: "No person . . . shall be compelled in any criminal case to be a witness against himself…"

The question of whether the collection of facial biometrics constitutes a search for purposes of the Fourth Amendment would have been answered, until recently, by the application of historical precedent that no person has a reasonable expectation of privacy in his or her face.[12] However, recent lower court decisions suggest this may not be true for the pervasive or intrusive use of facial biometrics technology for identification and/or authentication purposes.[13]

The use of facial recognition technology by government actors can be analyzed in three distinct aspects:

- the initial collection of biometric data;
- the request for identification; and
- the comparison between the stored data[14] and data presented by an individual on a particular occasion.

The first is likely consistent with the Fourth Amendment. The second and third aspects are settled areas of law: A request for identification does not, by itself, constitute a Fourth Amendment seizure,[15] and "the process of matching one piece of personal information against government records does not implicate the Fourth Amendment."[16]

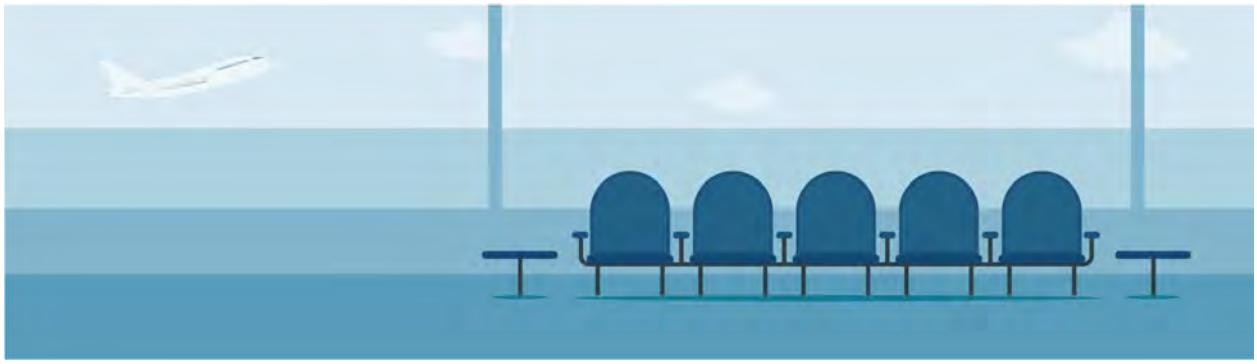
"The ultimate touchstone of the Fourth Amendment is reasonableness."[17] Generally, reasonableness requires that, whenever a government actor conducts a search or seizure of a person or his or her property, that official must have a warrant based on probable cause and issued by a judge or magistrate.[18]

To determine whether a Fourth Amendment search occurred, a court initially will examine the search under tests formulated by the Supreme Court.[19] One test looks at whether the government physically intrudes[20] (i.e., trespasses) and the other whether the intrusion violates a person's reasonable expectation of privacy.[21,22] If a court determines that the intrusion falls within the scope of Fourth Amendment protection, it examines whether the search complied with the scope of the terms of the warrant, if one was obtained, or

whether a recognized exception to the warrant requirement applies (e.g., administrative search, border search, exigent circumstances, etc.).[23]

Public Spaces and the Fourth Amendment

Historically, the Supreme Court has determined that certain activities are not searches or protected by a constitutional right to privacy: persons on public streets and beaches[24], conveyances on public roads[25], prisoners in jail[26], and information on the exterior of mails.[27] Further, the Supreme Court has recognized that a temporary detention of a person for police questioning in connection with an airport search was reviewable under a lower standard than the rule announced in Terry v. Ohio[28] (requiring reasonable suspicion that the person is involved in criminal activity for a temporary detention by a law enforcement officer).[29] The Court found the temporary detention although constituting a seizure under the Fourth Amendment, was constitutional because of the officer's articulable suspicion and the public interest involved in the suppression of serious crime.[30]



In recent years, however, the courts, and in some cases, the Supreme Court, have wrestled with the traditional framework about public spaces when faced with advances in technology that pose a potential for unreasonable intrusion into a person's privacy.[31] The Supreme Court noted that technological advances provide "access to a category of information otherwise unknowable,"[32] and "implicate privacy concerns" in a manner as different from traditional intrusions as "a ride on horseback" is different from "a flight to the moon."[33]

The trend from recent Supreme Court cases focused on GPS and cell phone tracking appears to signal that where the use of heightened technology is more intrusive than traditional forms of observation, courts may find the tracking and identification of persons to be unreasonable under the Fourth Amendment.[34]

Exceptions to the Fourth Amendment Warrant Requirement

Even where the Fourth Amendment text would otherwise suggest its application, the Supreme Court has recognized certain governmental activities as reasonable *per se* under Fourth Amendment. Because these activities are deemed reasonable *per se*, they are regarded as exceptions to the warrant requirement of the Fourth Amendment. For example, routine searches of persons and items at the border by duly authorized officers (e.g., CBP and Immigration and Customs Enforcement (ICE)) are deemed reasonable and may be conducted without suspicion.[35] The border search exception is not limited to searches that occur at the border itself but includes searches that occur at the "functional equivalent" of the border (e.g., at an airport inspecting and clearing arriving international passengers).[36]

Courts have noted that there is a diminished expectation of privacy at airports.[37] In that context the courts have held that routine airport screening searches are reasonable under the special needs exception and do not require a warrant, individualized suspicion, or consent,[38] provided that they are properly calibrated to

their purpose and not in furtherance of traditional law enforcement goals.[39] Under the special needs doctrine, courts assess the constitutionality of the challenged conduct by weighing the government conduct—in light of the special need and against the privacy interest advanced—through an examination of three factors: (1) the nature of the privacy interest involved; (2) the character and degree of the governmental intrusion; and (3) the nature and immediacy of the government's needs, and the efficacy of its policy in addressing those needs.[40]

Liability

For alleged violations of the Fourth Amendment, persons can sue state and local government actors under 42 U.S.C. §1983 which provides a private cause of action against state officers for violations of federal civil rights.[41] With respect to alleged unlawful searches or seizures by federal officers, the Supreme Court in Bivens v. Six Unknown Agents held that an individual could sue for monetary damages for a violation of the Fourth Amendment.[42]

Private Party Acting as an Agent of the Government

Traditionally, searches by private parties do not trigger the Fourth Amendment unless the party is acting at the direction of a government actor.[43] In other words, a search conducted by private individuals at the instigation of a government officer or authority constitutes a governmental search for purposes of the Fourth Amendment. Where a private party assists or acts at the direction of a federal agency in performing an activity lawful under an exception to the Fourth Amendment warrant requirement, such as the border search exception (i.e., CBP or ICE) or special needs exception (i.e., TSA), the private party's assistance would fall within the protected scope of the exception.[44] For example, courts have indicated that there is a diminished expectation of privacy at airports,[45] and thus, searches conducted by airport personnel in accordance with a federally approved security plan are deemed to fall within the special needs exception to the Fourth Amendment.[46]

Recently, there has been increased attention and scrutiny where private parties are engaged in voluntary data-sharing with law enforcement. Most cases decided in this area focus on the degree of governmental influence over the initial collection.[47]

At least one commentator has suggested that the analysis for determining whether a private party engaged in voluntary data sharing with law enforcement sufficient to make it an agent of the government should include consideration of the following four factors:

- first, whether data-sharing is repeated or, instead, spontaneous;
- second, whether the data-transfer was aimed to assist law enforcement;
- third, how powerfully-equipped the private actor is to perform data surveillance; and
- fourth, whether law enforcement practice has evolved to reflect the availability of privately collected data.[48]

DNA Identification as a Case Study

Although courts have not yet had the opportunity to examine the *governmental* use of facial recognition technology,[49] recent case law on the collection of DNA and creation of DNA profiles provide a useful framework for understanding how courts will likely address such conduct in the future. Ultimately, the similarities and differences between DNA profiling and the use of facial recognition technology arguably demonstrate the latter's legality. (See Appendix K for a case study analyzing courts' treatment of DNA).

Federal Privacy Laws Relevant to Airport Operators and Stakeholders

Generally, federal privacy laws: (1) govern a federal agency's collection and use of biometric data; and/or, (2) protect consumers' privacy with respect to the collection and use of their biometric data and provide them a cause of action. There are a number of federal privacy laws applicable to the collection and use of biometric data *by federal agencies* as well as specific activities by various industries in distinct business sectors, some of which are relevant to airport operators and stakeholders. Interestingly, a 2015 U.S. Government Accountability Office (GAO) report observes that there are no federal laws restricting the *capture* of facial images except with respect to matters associated with minors.[50]

KEY TAKEAWAY

As discussed in this section on state laws, aviation stakeholders should note that if you are doing business in a state that does not have a law expressly limiting the collection and use of biometric data, such as facial recognition, but you collect and use biometric data on a resident from one of those states you may be required to implement changes and follow the requirements of the resident's state or potentially face stiff penalties.

With respect to legal protections pertaining to *commercial uses* of biometric data, including facial recognition technology, federal laws can be divided into three broad categories: those that address privacy and consumer protection for: "(1) the capture of facial images; (2) the collection, use, and sharing of personal data; and (3) unfair or deceptive acts or practices, such as failure to comply with a company's stated privacy policies."[51]

The overarching federal law governing federal agencies' collection, use and disclosure of personal identifying information (PII), such as biometric data, is the Privacy Act of 1974.[52] Other federal laws pertinent to or regulating the collection and sue of biometric data include the Federal Trade Commission Act (addressing unfair or deceptive acts); and the Public Health Service Act (setting forth authorities to control public health emergencies such as COVID-19). (See Appendix K for a detailed discussion of federal laws governing privacy in specific sectors).

U.S. Congress Legislative Activity

On January 1, 2019, the 116th Congress commenced and ended on January 3, 2021. During the two-year period that Congress is in session, a bill may be introduced at any point and it remains eligible for consideration until the Congress ends or adjourns *sine die* (i.e., adjourning without specifying a return date).[53] Since January 2019, there have been approximately 70 bills introduced which propose to protect consumers' privacy or impose limits on private sector or government agencies' collection and use.[54] Critics of the collection and use of biometric data and privacy advocates have voiced the need for national legislation to establish a comprehensive framework for government and commercial use and collection of biometric data.[55] By the end of the session, except for a handful, most of the bills were not voted out of committee and only a handful of generic provisions applicable to DoD activities within defense authorization acts (FY21) were enacted.[56] It is worth monitoring activity in the 177th Congress, which commenced in January 2021.

Survey of State Laws

In the absence of a comprehensive federal law regulating the collection and use of biometric data, states have enacted basic laws protecting citizens' and consumers' privacy, most of which do not expressly specify coverage for biometric data. Distinct from specific provisions governing biometric data, there are many state laws protecting *personal* data. In some cases, where there is no express mention of biometrics, biometric data is regarded as a subset of personal data.[57] In other cases, however, the law distinguishes

between personal identifying information and biometric data by considering the latter as a unique category of sensitive personal information.[58] Even among the handful of states that have enacted laws expressly governing the use of biometric data, the definitions of biometric data are not uniform, and requirements imposed on companies' use of biometric data are inconsistent, adding to the uncertainty for private companies seeking to ensure compliance with applicable laws.[59] A discussion of state laws (Texas, Washington, California, New York, and Nevada) that expressly govern biometric data is set forth in Appendix K.

State laws are particularly relevant under circumstances where airport operators and stakeholders are collecting personal data and using biometrics, such as facial recognition, to manage their workforces and for commercial or transportation services for travelers. State laws can be grouped into four broad categories:

- Some 19 states regulate the collection and use of facial recognition data (and an even larger number protect such data under a broad definition of personal information);[60]
- All 50 states, plus the District of Columbia, Puerto Rico, Guam and the U.S. Virgin Islands require private companies or governmental entities to notify residents of a data breach;[61]
- Approximately 35 states, plus the District of Columbia and Puerto Rico, mandate entities destroy, or otherwise make inaccessible, personal information that is no longer of use or after a specified period of time;[62] and
- A handful of states prohibit state and local agencies from collecting, using, sharing, and retaining biometric data, particularly facial recognition data, except in limited circumstances.[63]

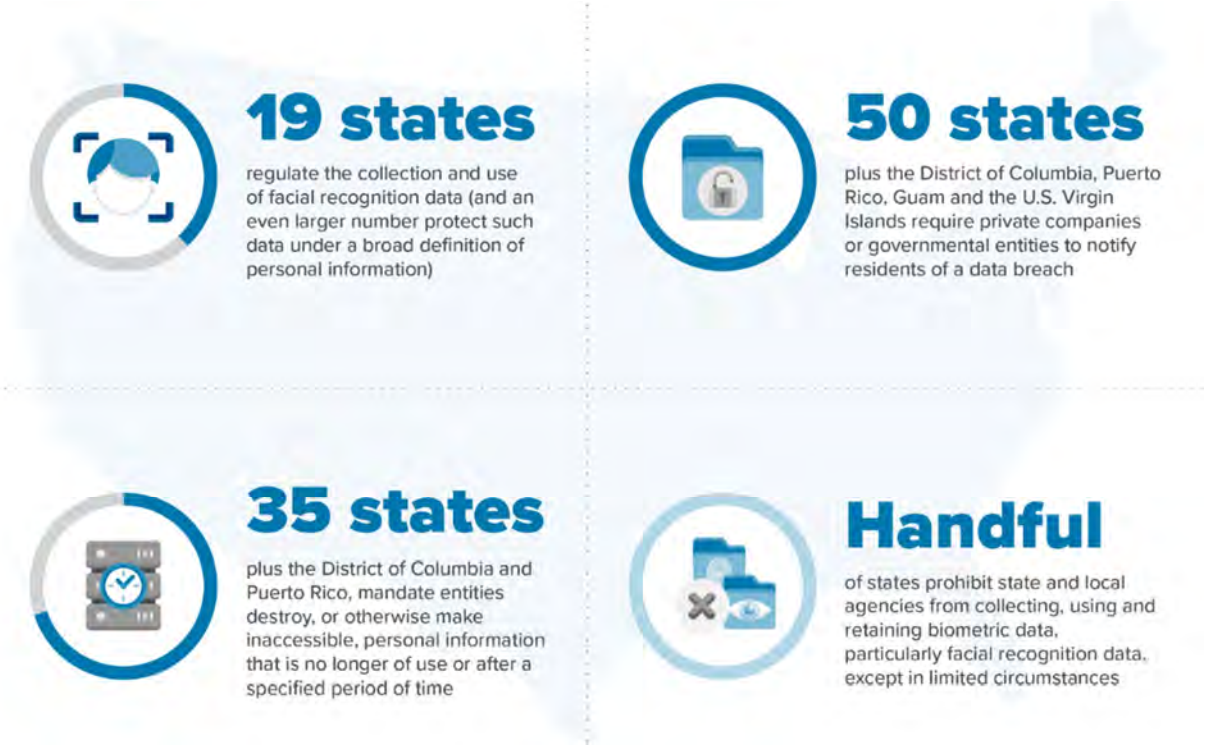


Figure 3-10: Summary of state laws related to the collection and use of biometric data

The state laws widely vary in their protections, penalties for violations, and requirements for businesses.[64] According to at least one article, as of May 2020, it is legal in 45 states to identify an individual using images taken without consent while they are in public while New York, California, Washington, Illinois, and Texas do not allow it for commercial use.[65] Several states, however, either expressly define personal

information to include biometric data or have been interpreted to provide such protection.[66] Several states have determined that the definition of personal information excludes biometric data.[67] In 2019 alone, legislatures in 25 states considered biometric privacy bills.[68]

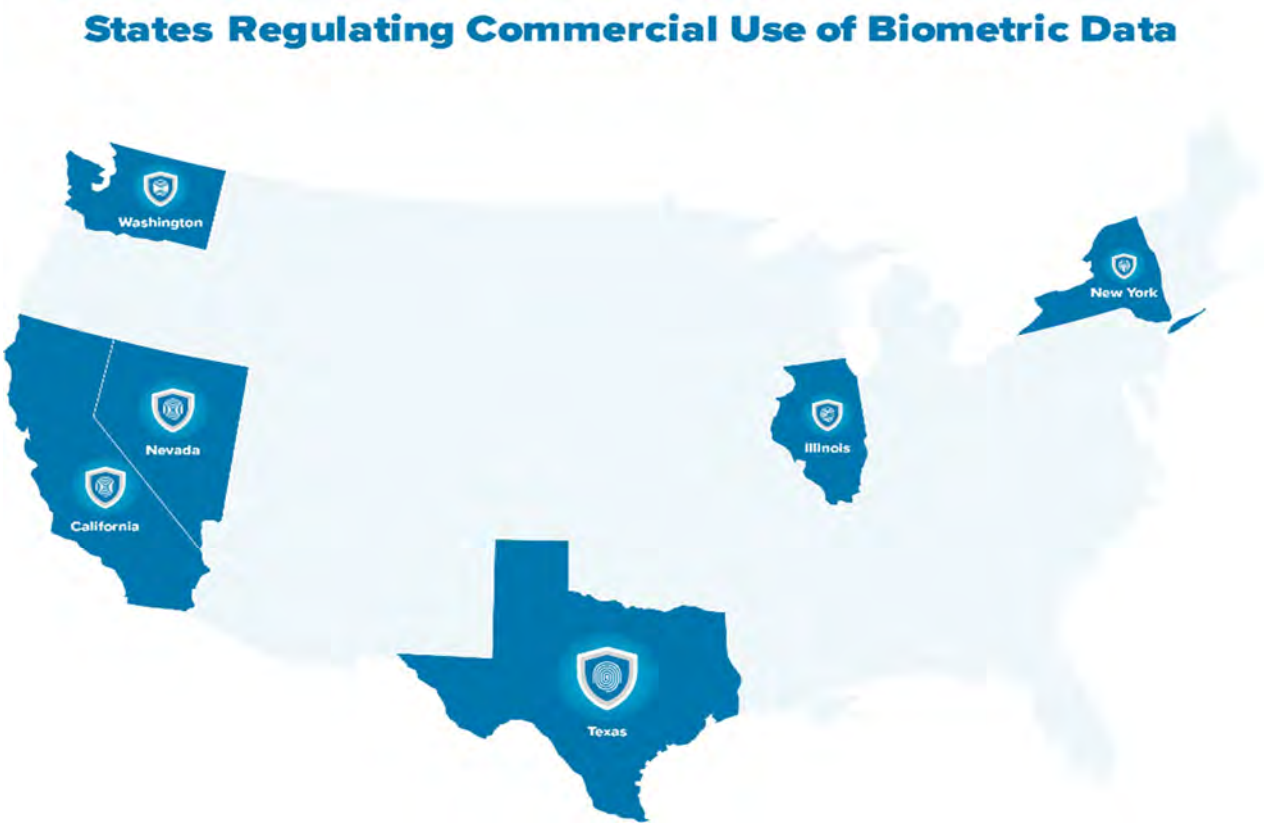


Figure 3-11: Six states in the U.S. regulate commercial use of biometric data

Illinois

Enacted in 2008, the Illinois Biometric Information Privacy Act (BIPA) is the first law to expressly address biometric data.[69] BIPA imposes requirements on employers and private entities to make written privacy policies publicly available and provide written notice to, and obtain written consent from, employees on whom the biometric information is being collected and retained, the purpose of the collection, and the period of storage. It also prohibits profiting off biometric data, allows only a limited right to disclose collected data, sets forth data protection obligations for business.[70]

Significantly, BIPA requires companies to adhere to reasonable standards while possessing the data and creates both a private cause of action and authorizes enforcement by the state's attorney general.[71] Of note, BIPA carries strong penalties: $1000 for each negligent violation and $5000 for each willful or reckless violation.[72] Pursuant to a private cause of action, plaintiffs can recover injunctive relief and any actual damages (that exceed the prescribed penalties).

Over a two-year period, 2018-2019, over 200 lawsuits were filed for alleged violations of BIPA and reportedly this is on the rise.[73] Illinois state courts rendered decisions on whether a technical violation of BIPAS was sufficient to pursue a case, as federal courts and state courts define injury differently for purposes of determining standing to bring a suit in the respective courts.[74]

To date, most of the cases under BIPA have been class actions targeting employers' use of biometric technology at work. These lawsuits are not only on the rise, but expensive and difficult to defend against.

For example, in 2020, Facebook offered to settle a class action lawsuit (in California) for alleged violations of BIPA for $650 million (after the trial judge initially rejected the proposed $550 million settlement).[75] In May, plaintiffs filed lawsuits against Facebook in Texas and Arizona, adding to the many other suits pending nationwide and the company is reportedly facing billions in damages.[76]

There is also uncertainty with respect to application of BIPA (and other states' biometric privacy laws) under circumstances where airport stakeholders are partnering with government agencies, such as CBP under the TVS program. Factors bearing on applicability, compliance, and potential liability include whether the state law addresses only commercial uses of biometric data and excludes government agencies from its scope, as do all of the biometric state laws discussed in this section (with the exception of the recent Washington law); whether the airport stakeholder's partnership can be viewed as acting as an agent of the government by collecting facial images and transmitting them to CBP (and not retaining them), but this becomes complicated if the stakeholder collects the data for a dual business purpose as well, such as facilitating the boarding process (See Appendix K for a discussion of other state laws).

Most recently similar legislation has been introduced in several other states (e.g., Arizona, Florida, and Massachusetts).[77] Also states have enacted laws to protect the privacy of minors and students.[78] In addition to the proliferation of state laws enacted or under consideration, local jurisdictions have approved ordinances banning the use of facial recognition technology by city government agencies, and in particular, police forces.[79] It is anticipated that this trend will continue as privacy concerns increase.

Supremacy Clause and Conflict of Laws

The Supremacy Clause in the U.S. Constitution provides that even if a state statute is enacted in the execution of acknowledged state powers, state laws that "interfere with, or are contrary to the laws of Congress" must yield to federal law.[80] In the event of a conflict between existing/future federal law governing the use of facial recognition technology, federal law is deemed to preempt state law in three situations:[81] (1) when the federal law specifically states that it preempts conflicting state laws[82]; (2) when the federal law purports to "regulate conduct in a field that Congress intended the Federal Government to occupy exclusively" [83]; and, (3) when a state law "actually conflicts with federal law … the [Supreme] Court has found pre-emption where it is impossible for a private party to comply with both state and federal requirements[.]" [84,85]

By way of example, this issue has been at the heart of lawsuits and commentaries challenging the Government's Secure Communities program seeking to mandate the sharing of fingerprints collected by state and local authorities as a means of checking immigration status and enforcing federal immigration laws. State and local authorities enacted policies and laws seeking to defy the mandate. While Congress has the power to preempt state law, it is not always clear where to draw the line between immigration enforcement and the exercise of general police powers. [86]

With respect to a conflict between state laws, federal courts analyzing the issue "ordinarily must follow the choice-of-law rules of the State in which it sits." [87] Where a commercial entity includes within its Terms of Service that any litigation will be conducted in a chosen state, the court will uphold that term if the chosen state has a "substantial relationship" to the parties and transaction unless the decision would be contrary to a fundamental policy of the alternate state.[88]

[89]Numerous commentaries have recommended enactment of comprehensive national legislation regulating privacy protections in connection with the collection and use of biometric data, particularly in the face of conflicting state laws on data privacy.[90] Several challenges render this a difficult task. Should national legislation preempt all the state laws in effect and set the bar for minimal requirements? How would the law make it clear to all stakeholders what the specific requirements and obligations are and would it distinguish between personal information and sensitive personal data? Should national legislation incorporate state law provisions pertaining to consent, opting out, correction of data, enforcement, etc.? Thus, while there has been a call for passage of a federal law governing privacy and personal information,

the drafting, scope and construction of a comprehensive framework, addressing these and many other related issues pose a daunting task.

Additional Legal and Policy Considerations

Surveillance v. Identification

> **KEY TAKEAWAY**
>
> As set forth in this section, one of the key takeaways is that states are considering and enacting laws limiting/governing the collection and use of biometric data at a rapid pace, so air industry stakeholders need to stay current with emerging privacy law trends and comply with the enactment of state laws and other nations' requirements if you collect and use or propose to collect and use biometric data about your customers.

As noted earlier, there is a long-standing history of the use of stationary security cameras at airports, retail establishments, subways, and public streets.[91] The courts generally found that individuals did not have a reasonable expectation of privacy in public places and tended not to view public surveillance as a search, governed by the Fourth Amendment. In a recent decision, regarding the use of four fixed automatic license plate readers to surveil the ends of a bridge, a state court concluded that while the limited use of the technology did not constitute an unreasonable search, it struggled with where to draw the line.[92] Part of the challenge the courts face is assessing society's reasonable expectation of privacy where heightened technology influences or shapes those expectations, particularly with concerns centered around pervasive police presence.[93] Legal and policy challenges associated with private sector use is on the rise where the security camera is linked to some form of facial recognition technology.[94]

Bias

While the intersection of facial recognition technology and discrimination, misidentification and bias have occasionally cropped up in criminal prosecutions, policing, or cases involving false arrest,[95] there has been little litigation against private employers applying the technology where the claim is one of bias or discrimination. The litigation risk would most likely arise in the context of contract constraints or violation of state laws.[96]

The issue, however, is front and center in assessments of the technology. Under a number of studies by the National Institute of Standards and Technology (NIST), the agency found that the accuracy of the facial technology depends on factors such as: the specific vendor; whether the purpose is for verification or identification; and, whether the algorithm is one-to-one or one-to-many.[97] Further, the latest NIST report acknowledged that the type of recognition algorithm used, i.e., one-to-many identification or one-to-one verification, in various facial technologies, resulted in a higher incidence of false positives and false negatives for certain ethnic, gender, and age groups.[98] The latest NIST study also reported that the impacts of false positives and false negatives varied greatly depending on the use or purpose (e.g., some capable of mitigation by a second attempt, some presenting a security concern and requiring additional follow-up, some leading to false accusation, and some inconveniencing commercial applications such as access to phone use).[99] That same study concluded that advances in the vendor technologies available have consistently improved upon mitigating bias and misidentification,[100] and reinforced the finding in the NIST Report that that "massive gains in accuracy have been achieved in the last five years (2013-2018)."[101] In February 2020, NIST indicated it is in the process of assessing CBP's facial recognition algorithm.[102]

Title VII Discrimination

Included here is a brief mention of potential litigation based on allegations that an employment practice, such as the collection and use of an employee's biometric data may implicate and violate religious beliefs.[103] Courts may require employers to provide a reasonable religious accommodation, such as an alternative method of clocking in.[104] Other employment considerations may apply such as the necessity of reasonable accommodations under the Americans with Disabilities Act.[105]

Foreign Laws & Regulations

A short discussion of key foreign laws and regulations are included because they may involve challenging restrictions and legal risks to the use of biometrics by parties arguably subject to both U.S. and foreign laws and regulations. Many countries have turned to the use of biometrics, particularly facial recognition technology, to perform verification functions associated with traveler facilitation programs, criminal investigations and passport administration.[106]

KEY TAKEAWAY

Although the focus of much of this paper is on the current U.S. legal and policy landscape, this short section describes the EU privacy rules and their potential impacts for U.S. businesses.

The European Union (EU) General Data Protection Regulation (GDPR),[107] adopted officially on April 27, 2016, entered into force on May 24, 2016, and requiring EU members to incorporate it into their national law by May 25, 2018, offers insights into foreign trends and highlights potential conflicts with entities such as carriers subject to two sets of laws. The GDPR superseded the 1995 Data Protection Directive in the EU, but like the Directive, the GDPR carries extra-jurisdictional ramifications by requiring countries

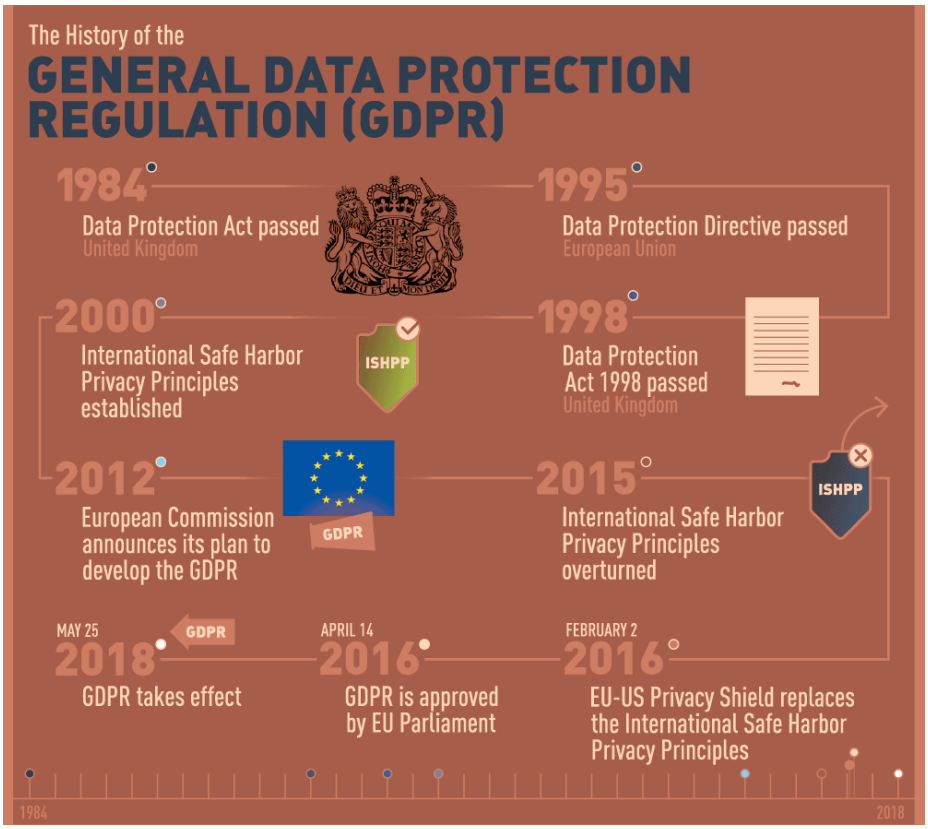


Figure 3-12: A history of EU data protection regulations leading up to the GDPR.[108][109]

or entities to prove compliance with the GDPR before allowing the transfer of EU-held personal data.[110]

The GDPR restrictions and requirements apply to an entity processing personal data in three circumstances: 1) where the company processing the data is established in the EU; 2) where, regardless of where the company is located, or where the processing occurs, the processing relates to an offer of goods or services to EU residents or monitoring their behavior that occurs within the EU; or 3) where the processing occurs and the GDPR applies as a matter of public international law (e.g., within an EU mission or consular post).[111] Article 2 provides four exceptions to the GDPR's applicability, including when government agencies and law enforcement collect and process data for the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties or for preventing threats to public safety.[112] Arguably, however, the GDPR may apply to companies that provide EU residents' data to national security or law enforcement agencies. Further, it should be noted that the GDPR applies to personal data obtained from public sources.[113]

The GDPR is intended to provide safeguards for consumer data security rights. It regulates the private sector with respect to the collection, use, retention, storage, and sharing of automatically processed personal data, including biometric data, defined as "special categories of personal data."[114] Pursuant to Article 4 (14), biometric data is classified as a special category and defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." The processing of sensitive personal data is otherwise prohibited except if one of any of a number of enumerated exceptions apply, including, but not limited to, explicit consent, specified public interest considerations, and certain exemptions in the fields of employment and social protection law.[115]

In essence, there are seven key requirements for organizations that process[116] biometric data pertaining to EU residents, as shown in Figure 3.5.

Significantly, the GDPR limits the ability for cross-border transfers of personal data and generally requires a finding that the receiving country has adequate data protections in place (the so-called "adequacy decision").[117] The EU had issued the United States "only a limited adequacy decision with respect to companies that registered voluntarily under the EU-U.S. Privacy Shield program that the U.S. Department of Commerce administered and whose principles the Federal Trade Commission enforced"[118] This status recently changed.

On July 16, 2020, the European Court of Justice handed down a ruling that could have significant impacts for U.S. companies that collect personal data, including biometric data. "The Court of Justice invalidated Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield."[119] The Court found that information on EU citizens when transferred to U.S. servers was not adequately protected from "government surveillance."[120]

Essentially, the Court found that the data was not adequately protected from U.S. government authorities and failed to provide EU citizens with certain rights guaranteed under the GDPR.[121] At a minimum, U.S. businesses that collect data on EU customers may need to assess their data protection policies and systems or risk severe sanctions.

As of February 26, 2020, Google has been fined approximately $55 million for GDPR violations relating to unclear terms and for failing to provide valid consent.[122] It should be noted that U.S. courts do not recognize nor are they required to enforce judgments for "the collection of taxes, fines, or penalties rendered by the courts of other [nation] states."[123]

On February 17, 2020, the EU's digital and competition chief told reporters that automated facial recognition breaches the GDPR, as the technology fails to meet the regulation's requirement for consent.[124] Moreover, it was reported that the EU plans to regulate certain applications of facial recognition technology in the future because it can violate EU subjects' privacy rights.[125]

Figure 3-1: Seven GDPR Requirements

As seen in the case of Washington State recently, the EU released the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 for the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.[126] In other words, as a counterpart to the GDPR, the EU implemented rules to protect the privacy rights of its residents when dealing with *public* European Union Institutions.

In addition to the EU, approximately 28 countries have enacted legislation or promulgated regulations governing biometric data.[127]

International Organization Activities

There are a number of international organizations working on, coordinating, and collaborating with others to support initiatives to achieve a more seamless travel experience in the commercial aviation industry. Significantly, most advocate for global standards in an obvious effort to incorporate uniformity in international aviation.[128] (See Appendix K for a discussion tracing the history of several international initiatives relying on the collection and use of biometrics, including among others the ICAO Digital Travel Credential, the UN High Commissioner for Refugees Population Registration and Identity Management and EcoSystem, IATA and ACI Smart Security and New Experience Travel Technologies, and WEF Known Traveller Digital Identity).

Although used in a majority of airports worldwide, biometric data systems such as fingerprint image and facial recognition technologies, are subject to very strict conditions under the European 2016 General Data Protection Regulation (GDPR). Due to its sensitivity, prohibition of biometric data processing is the rule, except if strong safeguards are provided to protect personal data (express consent, proportionality, necessity, limited storage time are some of the key principles). Thus, while automatization of border control (i.e PARAFE E-Gates or a CLEAR® security check point) is legitimate, and even, to a certain extent, improvement of passenger journey experience (facilitation), mass surveillance to monitor passenger behavior along his airport journey is usually banned. In addition, given the high financial penalties at stake, the GDPR extra-territorial scope is another crucial issue a non-EU stakeholder shall consider, in particular if it has an establishment based in the EU or if it provides services to individuals based in the EU (no matter the individual nationality).

Isabelle Lelieur
Partner and Avocat à la Cour
at Chevrier Avocats. Paris. France

Best Practices/Privacy by Design

There are many publications and organizations offering advice and recommendations on protecting the privacy of consumers' and employees' biometric data.[129] Many sources agree that in the early 1970's a set of principles, known as the Fair Information Practice Principles (FIPPs),[130] were developed and evolved over the next several decades to provide a framework for the protection of personally identifiable information. (see the Appendix L for the description of the FIPPs core principles).

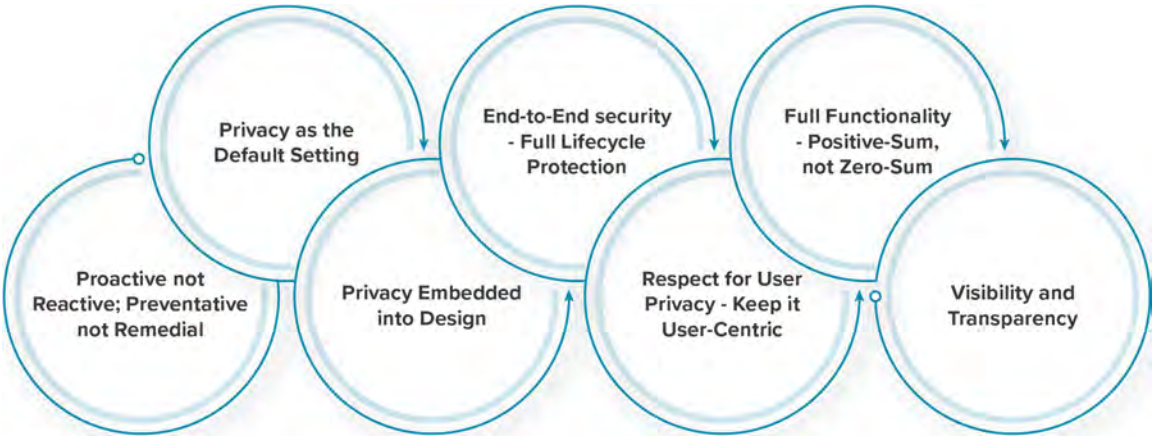
KEY TAKEAWAY

With the expected increase in use of biometric data, including facial recognition, and the anticipated benefits and efficiencies from its use in the aviation industry, as discussed below, stakeholders need to find the right balance of privacy protections and technological applications.

During the mid-1990's Ann Cavoukian introduced another widely accepted approach, Privacy by Design.[131] Privacy by Design garnered international acceptance upon the unanimous passage of a resolution in 2010 by the International Assembly of Privacy Commissioners and Data Protection Authorities.[132] The concept advocates the integration of privacy into data systems and technologies at every stage or step to reflect a "design thinking" perspective.[133]

In essence, the seven principles of Privacy by Design promote incorporation of privacy protections into the design and build of technology and Information Technology (IT) systems, applicable policies and practices, including those governing retention and destruction. The principles stress that inclusion of these protections can be made without sacrificing functionality or security. Further, they advocate business accountability to the public for privacy protections and providing data subjects with avenues of redress and an "active role" in the collection, use, and protection of their data.

The seven foundational principles for Privacy by Design are:



The seven principles explained are:

1. Proactive not Reactive - builds privacy considerations into technologies, policies, practices, etc. to prevent invasive events before they can occur.
2. Privacy as the Default Setting - incorporates privacy protections automatically into IT systems or business practices to provide maximum safeguards by default.
3. Privacy Embedded into Design - promotes the integration of privacy into IT systems and operations in a "holistic" way to ensure it is key foundational element without sacrificing functionality.
4. Full Functionality - Positive-Sum, not Zero-Sum-accommodates non-privacy objectives without trade-offs to achieve full functionality while protecting privacy: in other words, this principle advocates the accommodation of all legitimate interests and objectives in a "win-win" manner, not through the dated, either/or approach, where unnecessary trade-offs are made and supporting the position that it is possible to have both privacy and security.
5. End-to-End Security - Full Lifecycle Protection-extends privacy and security protections for the entire retention period through destruction.
6. Visibility and Transparency - Keep it Open-assures users and providers that the collection and use of personal data complies with representations and objectives while providing for accountability through independent verification as well as avenues of redress.
7. Respect for User Privacy - Keep it User-Centric-aims at providing data subjects with an "active role" in the collection, use, and protection of their data[134]

In 2012, the Federal Trade Commission (FTC) issued a report on consumer data privacy,[135] that recommends a number of best practices, that addressed both substantive and procedural protections. Building on its 2010 preliminary report that had recommended that businesses build privacy protections into their operations as described by Privacy by Design, the 2012 FTC report proposes best practices that offer simplified choices that give consumers more meaningful control, and would increase the transparency of their data collection and use practices.[136] (For a list of the 2012 FTC Report recommended practices see Appendix L).[137]From a global perspective, it is worth noting recent EU developments which include the 2019 EU Data Protection

KEY TAKEAWAY

Many of the principles of privacy protection, such as Privacy by Design, and best practices, as discussed in this section, have been incorporated into U.S. law and internationally so that compliance with these principles may place you on surer footing with the law.

Guidelines (4/2019) on the GDPR requirements for Data Protection by Design and by Default.[138] The draft Guidelines (which were open for comment until January 2020) proposed measures and guidance addressing: data protection by design; data protection by default; data subjects' rights; safeguard requirements; practical guidance on the application of the principles; and certification. Thus, the guidelines propose direction regarding what data protection obligations mean in practice and how to implement the data protection principles effectively. Similarly, the EU published guidelines on consent describing the elements of valid consent (i.e., under GDPR article 4(11)).[139]

The EU also published Guidelines (2/2020) on GDPR provisions on transfers of personal data between EU and non-EU public authorities and bodies.[140]

Commercial Developments

A recent initiative focuses on transparency, consumer education, and the mitigation of privacy concerns is the Digital Transparency in the Public Realm (DTPR)[150] DTPR is a collaborative project initiated by Sidewalk Labs, currently stewarded by Helpful Places, and joined by more than 100 participants to develop a standard that informs and advises individuals in simple language about complex forms of technology and data collection activities. In particular, DTPR seeks to design transparent patterns and prototypes that entities can use to develop signage that conveys to members of the public information about the use and collection of digital technology.[141]

There are four components to DTPR: icons, a signage system (based on the icons), a "digital channel" (which when you scan a QR code) connects you with a website for additional information, and when considered collectively conveys a set of definitions of key concepts or taxonomy.[142] Different icons convey different information such as "the purpose of the technology; another, the logo of the entity responsible for the technology; and a third contains a QR code that takes the individual to a digital channel where they can learn more. In situations where identifying information is collected, a privacy-related colored hexagon would also be displayed."[143]

The icons in Source: Helpful Places

Figure 3- are initial prototypes of a visual language for signage in the public realm that alerts the public to the presence of a digital technology. The black hexagons express the purpose of the technology; the blue and yellow hexagons show how identifiable information is used; and the white hexagons display the entity responsible for the technology. Another white hexagon with a QR code and URL enables people to learn

more.

Source: Helpful Places

Figure 3-5: Open-source icons aimed to facilitate digital transparency goals

Findings

Significantly, the World Economic Forum published two reports in February 2020 and more recently in December 2020 in furtherance of an initiative launched in 2019 to design a governance framework for the responsible use of facial recognition technology.[144] The project applied a use case approach focused on improving the air passenger boarding experience. The WEF reports suggest a comprehensive approach to using not only facial recognition technology but also other forms of biometric technology in the air environment.[145] Components of the WEF framework include: 10 principles for action[146], best practices, an assessment questionnaire, and an audit framework.[147] The two reports set forth a four-step approach to building the framework. Each step is intended to represent an additional level of commitment for ultimately achieving transparency and public trust. The December 2020 report focuses on auditing and certification not only to validate compliance with the principles for action, but to build in accountability, monitoring, and opportunities for improving the flow management process.

WEF while noting that the framework may serve as a "blueprint" for other applications, concludes that the next steps of the pilot or "journey" are:

> Test the audit framework and certification scheme with industry actors, assess their relevance and the amount of work they create for actors seeking certification, and review them based on the observed results. If successful, this policy pilot will pave the way for the design of a standard for the responsible application of facial recognition systems. Once the pilot project is completed, a multi-stakeholder coalition of actors committed to respecting and promoting this certification model will be formed.[148]

Drawing on sources discussed earlier, below are findings drawn from legal research and best practices, designed in part to mitigate litigation risks as well as promote sound privacy practices. The list below is intended to identify considerations that may be factored into decisions to use or support the use of biometric data technology:

- Determining and assessing whether the application of a type of biometric technology is as a matter of policy and operations, key to your business, either as an employer supervising your workforce (e.g., timekeeping, access to restricted areas, etc.) or a member of the aviation transport industry providing a service to customers;
- Consulting with legal advisers and understanding legal (both federal and state) requirements and restrictions (particularly those with broad reach and severe penalties) that govern the collection and use of personal data, especially biometric data, and appreciating that laws may impose different requirements depending on the type of collection and use of specific biometric data;
- Reviewing existing company policies, establishing a compliance plan, and designating a compliance officer responsible for ensuring that applicable policies, practices, and systems meet privacy principles and legal requirements;
- Making sure policies address obligations and issues of (advance) notice, (affirmative/written) consent (and the ability to opt out), sharing with third parties, the ability to access and amend personal data, and why your company collects specific data and the purposes for which it uses it;
- Focusing on and including policies and practices that allow for reasonable accommodation as the law may require (e.g., religious reasons, Americans with Disabilities Act, etc.);
- Identifying and addressing any applicable union issues;
- Informing employees and/or the public in clear and plain terms about your company's privacy policies and practices, including measures to protect the data, as communication is critically important;
- Meeting with privacy and civil liberties groups, as warranted, and legislative representatives to inform them of specific programs and protections, to appreciate any privacy concerns, and to avoid misunderstandings and/or unwarranted criticism;
- Ensuring that IT systems safeguard personal data, limit others' access, and are governed by practices limiting the collection of data to that which is authorized and necessary, retaining for only as long as necessary, and providing for appropriate means of storage and disposal;

- Prohibiting the sale or transfer of personal data to third parties without the express consent of the data subject;
- Ensuring a data breach notice mechanism is in place as a precaution; and
- Importantly, staying current on changing laws, both domestic and international, anticipating foreseeable changes if possible, and seeking advice from counsel to appreciate and address any impacts on your company's use of biometric data.[149]

Chapter 4

Planning and Process Considerations

Summary

This chapter highlights the role of technology, such as the use of biometrics, in passenger terminal area operations and planning. More specifically, in considering the use of biometrics in process improvements, airport stakeholders are advised to ultimately balance the demand and capacity of a facility to achieve certain operational requirements and the desired level of customer service.

The chapter provides a discussion of numerous factors for determining the applicability of biometrics in the airport setting, such as passenger demographics, airport size and geography, and the operational profile (e.g., primarily serving international or domestic traffic). Airports that are capacity constrained in some manner will likely be the early adopters with regard to the use of biometrics given the imperative that any incremental benefit, regardless of magnitude, may offer a meaningful overall improvement. While discussed in more detail within the chapter, critical factors to be considered are:

- Would passenger or facility security (e.g., identity assurance and accuracy) be enhanced?
- Would a small increase in capacity or level of service be meaningful to the overall experience of the population affected?
- Are there reasons besides capacity enhancement and security to implement biometrics, such as the desire to reduce staffing costs or improve the reliability of certain processes?
- Are the stakeholders required to implement the changes supportive of the end goals?
- Other questions that airport decisionmakers may address include:
    - In what parts of the passenger or employee journey should the use of biometrics be considered?
    - What are the potential benefits to the airport and associated stakeholders to implementing biometrics?
    - Given the potential costs associated with making enhancements with the use of biometrics, where is it most impactful for the least amount of investment?
    - How are biometrics successfully implemented in an airport environment?
    - Do the passengers using your airport have a high rate of passport ownership or Trusted Traveler program membership?
    - Do the airlines wish to implement biometrics at your airport and who is paying for the up-front capital investment and the ongoing operations and maintenance of the equipment?

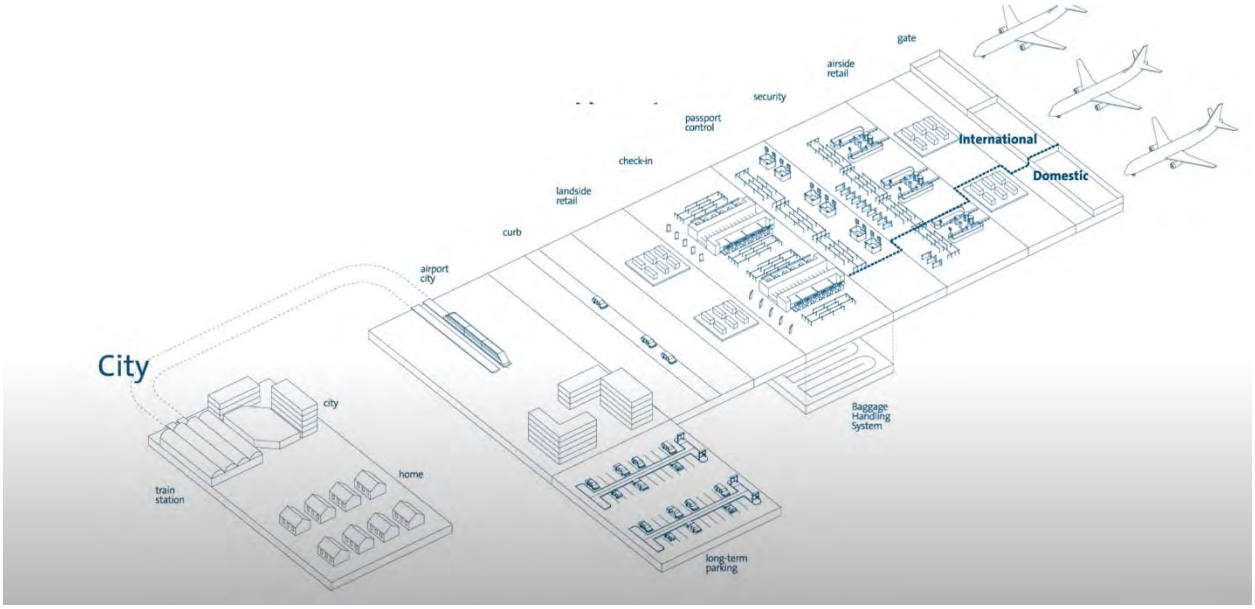
Airport operators are advised to review the pros and cons of specific biometric implementations to decide whether an implementation is warranted. In most cases, the return on investment (ROI) for the airport operator goes beyond strictly financial considerations for the implementation of biometric solutions. Instead of making decisions based solely on the financial ROI, airports are evaluating several additional considerations such as customer service, airport technology goals, passenger safety, operational efficiency, and competitive concerns.

Introduction: Biometrics Will Disrupt Traditional Airport Planning

> **KEY TAKEAWAY**
>
> Technologies, such as biometrics, are changing how terminals function, requiring that future terminal design delivers flexibility instead of simply physical purpose-built expansion.

Terminal planning in the airport environment is ultimately an exercise in balancing between the demand and capacity of a facility to achieve certain operational requirements and the desired level of customer service. Traditionally, capacity could be gained by adding new processing capability, which often involved physically expanding the size of facilities. While these static planning decisions were sometimes easier to make, building expansion requires a significant time and financial investment to implement. These expansions were also often purpose-built, to serve a specific need in the terminal, such as airline check-in or security screening and could not be repurposed as demand changed. More recently, technology has been integrated into facility planning to increase capacity and improve processes, while lessening the need for more expensive and time-consuming expansions.

This shift toward technological solutions requires that future terminal design delivers flexibility instead of simply physical purpose-built expansion. Technology and innovation have changed and will continue to change how terminals function. Increased throughput at various passenger processing functions, for example, lead to less processing space required. This provides new opportunities to transform unused processing space into more valuable passenger dwell space, preferably airside rather than landside, as was formerly the case with many pre-September 11th terminal designs.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-14: Airport overview of several passenger touchpoints in the departure process

Biometrics is one of those recently deployed technological innovations that is influencing the way airport terminals are designed and operated. Biometric use has been a part of everyday life for many years including in personal banking, building access, smart home devices, hands-free cars, and access control and single sign on. It is not uncommon to use a fingerprint scan to access a secure building or to use your voice to unlock your car or make a Bluetooth phone call. These concepts are now being expanded in application to airport facilities.

Source: JetBlue

Figure 4-15: JetBlue Self-Boarding Process

As outlined in Chapter 2, there are a number of use cases worldwide and within the United States. Of particular note for the planning of terminal facilities:

- Recent biometric implementations at airports, which have been driven primarily by airlines, include: JetBlue's first fully integrated biometric self-boarding gate for use by international flights – developed in partnership with CBP, JetBlue started trials on select international flights at Boston-Logan International Airport (BOS) and Fort Lauderdale-Hollywood International Airport (FLL) in 2017, before permanent installation began at John F. Kennedy International (JFK) in late 2018.
- Delta Air Lines' biometric Terminal F at Hartsfield-Jackson Atlanta International Airport (ATL) – In partnership with CBP, this Curb-to-Gate program utilizes facial recognition for all stages of the departure

process from check-in, to security access, to flight boarding, eliminating the need for passport or boarding pass verification.
- Alaska Airlines and Delta Air Lines fingerprint access to airline lounges – for those members who opt-in, both airlines partner with CLEAR®use fingerprints as a biometric token to grant access to their full network of domestic U.S. airline lounges.

These individual implementations of biometrics have proven beneficial to passengers, airlines, and airports, including reductions in queueing, space required, staffing, and human error. To achieve maximum impact, however, it is important to think about the end-to-end journey. This may provide for the opportunity to reduce disparate terminal processes as well as improve the integrity of operations, and the passenger experience. To facilitate this biometric journey, it is ideal that solutions be developed that are cognizant of the trends and standards addressed in Chapter 2 of this Primer.

As with most technological advances which change the functionality of a process or task, biometrics introduce new considerations for the airport facility. Some examples include the need to understand how to accommodate opt-out passengers, those that might require additional support or screening, and the premium passenger experience. Accommodating and troubleshooting passenger match errors, system errors, equipment failure, or other technology down-time scenarios are other new challenges that must be considered as part of the implementation. Privacy concerns also need to be addressed early and incorporated into every aspect of the design and implementation of biometric solutions.

It is important to note that all airports are different in terms of size, airline market shares, passenger demographics, and the role each plays in the broader aviation system. For example, while the U.S. Department of State reports that over 44% of Americans hold a passport, which is a key document for enabling biometrics without additional enrollment requirements, the rates of passport ownership are not consistent from state to state. High population density states like California and New Jersey have high rates of passport ownership while states like Alabama and West Virginia have much lower rates. There is not a one-size fits all solution for biometric implementation in every airport, but this Primer is intended to inform airport decisionmakers on how the use of biometrics is evolving inside and outside the airport landscape and the associated impacts and benefits of doing so at each stage in the passenger and employee journey. Important considerations for evaluating biometrics will be reviewed and used to evaluate potential biometric solutions in individual terminal processes along the passenger journey.

Considerations for Evaluating Biometrics in the Airport Environment

As with most emerging technologies, implementing biometrics is a moving target that is constantly evolving and changing. In some airports, biometrics have been deployed or trialed in piecemeal implementations by a diverse set of stakeholders, including CBP, airlines, and ground transportation providers. This reality can make it challenging to consider biometrics in a terminal operational solution as it effects critical design decisions and may quickly be rendered obsolete if not planned properly. To better understand whether biometrics should be considered, airport decisionmakers may have the following questions:

KEY TAKEAWAY

As an evolving and changing technology, it is important to think about biometric implementations at each terminal process from varying perspectives including space, security, staffing, and capacity to evaluate the appropriate use case.

- In what parts of the passenger or employee journey should the use of biometrics be considered?
- What are the potential benefits to the airport and associated stakeholders to implementing biometric technology?

- Given the potential costs associated with making enhancements with the use of biometrics, where is it most impactful for the least amount of investment?
- How are biometrics successfully implemented in an airport environment?

Since every airport is physically, geographically, and demographically different, it is important to think about biometric implementation at each terminal process in the passenger journey from several perspectives to evaluate the appropriate business case. The following questions have been developed to serve as a checklist when evaluating the business case for a biometric solution.

- Who are the stakeholders that are involved with this terminal process? Are they willing to participate with airport management to make an investment of time and attention to enable the improvement to be realized or even piloted?
- What are the space implications for a biometric solution? Consideration should be given to the type of furniture and equipment required as well as wayfinding to account for added passenger segmentation, such as non-enrollers, premium passengers, and mobility impaired passengers.
- Does the biometric solution reduce staffing expenditures and, if so, for which stakeholders?
- Are there customer service benefits to the biometric solution, such as increased airside dwell time or fewer "touchpoints"?
- Can a biometric solution improve security or reliability of certain processes?
- Does the biometric solution increase capacity of the terminal to accommodate more passengers at improved levels of service?
- Are the benefits of biometric solutions offset by the costs associated with biometrics that are allocated to the affected airport stakeholder?
- Are there governmental, regulatory, or other external considerations that necessitate a biometric implementation?

This Primer explores the opportunities and implications of implementing biometric technology at each major terminal process in the passenger journey to provide a comprehensive understanding around the various considerations discussed above.

Applying Biometrics in Terminal Processes

The airport terminal is comprised of several functional areas to support the departing and arriving passenger journey as well as the employees that work there. The functional areas evaluated for biometrics in this Primer include: check-in, health screening verification, security checkpoint access, airline lounges, concessions and retail spaces, self-boarding, immigration and customs, baggage claim, ground transportation facilities and modes, and employee access and screening. The applicability of biometrics at each of these functional areas is discussed separately and also summarized in Table 4-1.

KEY TAKEAWAY

Biometrics can play a role in almost all terminal processes, and in many cases, already does. This section identifies the stakeholders, space and capacity implications, and other benefits for biometric implementations at each terminal process in the passenger journey.

Table 4-12: Considerations for Processing of Passengers and Employees

Terminal Process	Can biometrics play a role?	How are biometrics currently accounted for or do you potentially account for it?	Stakeholders	Space and capacity benefits	Other benefits (e.g., staffing, security, customer service)
Check-in	Yes, now	Two models are being employed: • Remote biometric enrollment – passenger arrives at the airport "ready to fly" as the biometric token is already created and is recognized at each check-in stage • On-airport biometric enrollment – passenger has not enrolled in the biometric seamless journey in advance, so enrollment must occur at kiosk or other check-in touchpoint	Passengers, airport, airlines, government agencies (e.g., CBP)	• Remote biometric enrollment reduces requirements for check-in facilities in the lobby by shortening the processing times • On-airport biometric enrollment does not reduce processing time at enrollment touchpoint but does so at all check-in touchpoints downstream • Spatial implications have to be analyzed case by case based on passenger mix and check-in channel distributions	• Reduces airline staff, but reductions may be higher in some cases than others • Enhanced passenger experience • Shorter processing times at the airport (in most cases) • Enhanced security with more accurate ID matching • Postponement of capital investment in capacity enhancement
Health screening verification	Yes, future for integration with biometrics	• Programs in development to collect health information on passengers, with potential to leverage biometrics • VeriFLY (see Case Study 2 in Chapter 2) passengers enroll their facial biometric and confirm their health status to receive personalized processing; potential to connect to passenger health records • Airports and airlines providing medical testing resources in airport facilities	Passenger, airport, airlines, government agencies, medical labs	Smaller facilities dedicated to health screening required if passengers are prescreened and approved	• Reduce burden for health screening to occur on airport • Enhanced passenger experience • Reduced curb to gate time for passengers who do not require manual health check to be performed • Enhanced verification process and increased accuracy

Terminal Process	Can biometrics play a role?	How are biometrics currently accounted for or do you potentially account for it?	Stakeholders	Space and capacity benefits	Other benefits (e.g., staffing, security, customer service)
Security checkpoint access	Yes, now	• Biometric token used to verify ID at travel document checker, prior to entering screening lane, as modeled at ATL Terminal F • Pre-enrollment programs such as CLEAR® and VeriFLY provide expedited access through checkpoint queue • Checkpoint access could be incorporated in the seamless journey using single biometric token	Passengers, airport, government agencies (CBP and TSA)	• Processing times will be reduced resulting in fewer access points required, but flow will still be metered by the checkpoint lanes themselves • Queue area could potentially be reduced	• Reduced security staffing • Enhanced passenger experience (seamless and touchless) • Enhanced security with more accurate ID matching
Employee access/ screening	Yes, now	• Biometric access control already in place through SIDA badging • Programs like VeriFLY expand employee screening facilities to members of traveling party using biometric token	Airport, employees, DAC vendor services	Negligible, though some space savings possible if programs like VeriFLY can divert some traveling employees to other facilities	• Additional staff reduction if biometric access is extended to additional access points • Enhanced security with more accurate ID matching

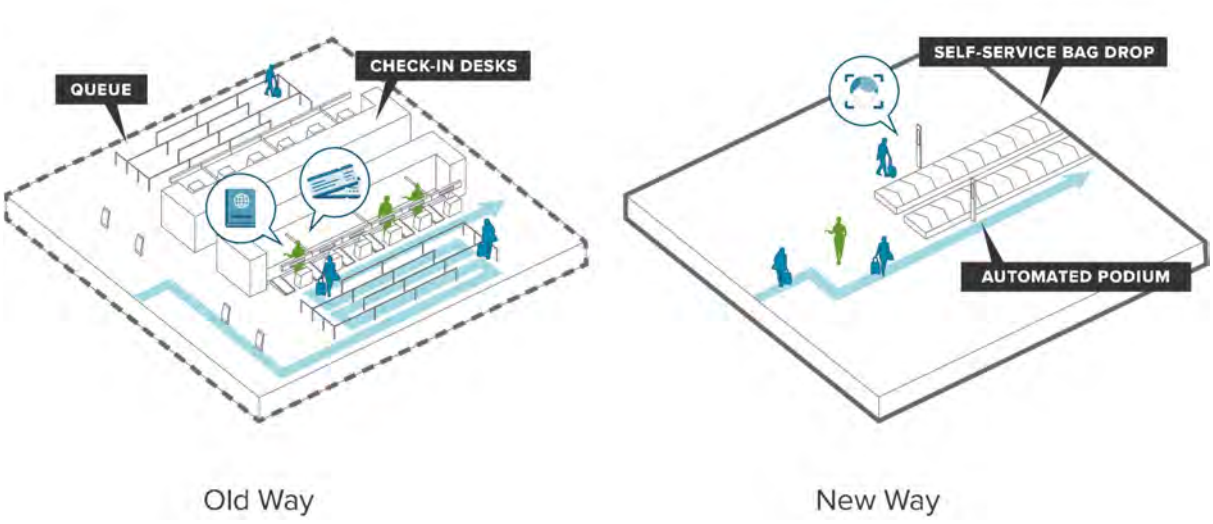
Terminal Process	Can biometrics play a role?	How are biometrics currently accounted for or do you potentially account for it?	Stakeholders	Space and capacity benefits	Other benefits (e.g., staffing, security, customer service)
Airline VIP/CIP lounges	Yes, now	• Airlines (Delta, Alaska) partner with CLEAR® to use fingerprint biometric to validate lounge access • Third party operators like American Express getting closer to biometric implementation by using QR code but still requires physical ID check • Lounge access could be incorporated in the seamless journey using single biometric token	Airlines or third-party lounge operators, passengers	Negligible	• Reduces airline or third-party lounge staff • Faster check-in process, no need to provide membership cards and IDs • Enhanced verification process and increased accuracy
Concessions/ Retail	Yes, future for integration with biometrics	• Amazon “Just Walk Out” technology shifting from supermarket application to airport application • Payments and remote ordering or delivery to gate apps can be expanded to include biometric token • Lines blurred between concession areas and holdrooms	Airports, passengers, concessionaires	• Ability to create more open space concessions not bound by physical barriers • More shared common space between airside terminal functions could reduce overall space needs	• Reduces concessionaire staffing • Seamless shopping without having to queue at check-out; fewer touchpoints • Better tracking of food/retail purchase trends • Push coupons or advertising based on traveler behavior

Terminal Process	Can biometrics play a role?	How are biometrics currently accounted for or do you potentially account for it?	Stakeholders	Space and capacity benefits	Other benefits (e.g., staffing, security, customer service)
Self-boarding	Yes, now	• Biometric boarding currently for international flights with both U.S. and foreign-flag airlines • E-gate or camera on a stick approach to validating credentials • Location of gate podium, security around boarding door, and electrical connections require consideration	Airports, airlines, passengers, government agencies (CBP)	• Could require more space than the traditional boarding to account for exception processing and mobility considerations, plus barriers to prevent passengers from bypassing • Faster boarding process could reduce space required for queue (nine minutes saved on wide body boarding)	• Reduces airline staff required to operate a flight departure, allowing them to focus on customer service issues • Faster boarding times allow passengers to spend more time relaxing or spending money in the terminal • Turning aircraft faster could allow for gates to be available for additional flights • Enhanced verification process and security
Immigration and customs	Yes, now	• CBP Simplified Arrivals process uses photographs to match against biometric token to complete passenger inspection • Traditional static booths can transition to podia and potentially to mobile units • Trusted traveler programs such as Global Entry® and NEXUS process low-risk travelers using biometrics	Airports, airlines, governmental agencies (CBP), passengers	• Shift from kiosks and counters to podia and mobile units will decrease overall size of immigration halls • Increased capacity expected since CBP can clear arriving flights an average of nearly 12 minutes faster than using the traditional processing methods • Secondary screening area for customs is still required	• Staff spend less time on low-risk passengers and more time on higher risk ones; could present staff savings • Faster processing time for passengers, especially those who are low risk • Enhanced passenger experience (seamless and touchless) • Standardized process with increased identity assurance and accuracy that reduces the imposter threat

Terminal Process	Can biometrics play a role?	How are biometrics currently accounted for or do you potentially account for it?	Stakeholders	Space and capacity benefits	Other benefits (e.g., staffing, security, customer service)
Baggage claim	Maybe, but benefits may not outweigh capital costs	• Matching passengers with bags upon arrival has traditionally been a manual process • A passenger's biometric token would be required to call for the specific bag to be delivered to bag claim, requiring replacement of traditional claim units with more of a baggage storage and recall system • A less intensive biometric implementation could simply identify stolen or mismatched bags	Airport, airlines, passengers	• Incorporating biometrics could require significant physical modifications, which may or may not replace the area currently allocated to baggage claim belts • Batching of arrival passengers may drive up requirements for bag retrieval points in baggage claim	• Staffing at bag claim is not significant (bag service counter, tug operator, bag porters) so minimal savings expected • Improves the security of the process as it is less likely for passengers to take wrong bag or for bags to be stolen, but these percentages are likely fairly low
Ground transportation	Yes, with more integration possible	• Hertz partnership with CLEAR® to expedite vehicle rental process trialed • Biometric token could be used to bypass transit ticket purchase or eliminate pay gates in an on-airport parking facility, expanding beyond toll tags	Airport, passengers, concessionaires (rental cars, parking, Transportation Network Companies, transit operators	• Smaller footprint for passenger processing in ticket lobbies • Reduced size exit plazas at parking and rental car facilities	• Staff reduction at parking exit plazas, for example • Faster and enhanced (touchless) passenger processing • Enhanced verification process and increased accuracy

Biometrics for Airline Check-In

The airline check-in process can be disjointed as some parts of the process may occur remotely from the airport (e.g., at home or work) while others may occur inside the terminal. Additionally, unlike many terminal functions, check-in differs by airline and passenger profile (e.g., need to check a bag, obtain a boarding pass). The four primary check-in processes can be summarized as: (1) online/remote check-in, (2) self-service kiosk, (3) self-service bag drop, and (4) full-service counter. Biometrics can streamline this complex multi-step process while providing a faster and more secure experience for passengers.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-16: "Traditional check-in" and "Modernized check-in"

Currently, there are two high-level scenarios for enabling a biometrics component to the improve the check-in process: remote biometric enrollment and on-airport biometric enrollment. Under the remote scenario biometric check-in begins at home with online check-in. At Delta Air Lines' biometric check-in for international departures from Hartsfield-Jackson Atlanta International Airport, for example, passengers enter and confirm their passport information remotely during online check-in. This enables the passenger to be "ready to fly" upon arrival to the airport. The passenger can approach a self-service kiosk at the airport and be immediately recognized so boarding passes and checked baggage tags can be seamlessly obtained without interaction with airline customer service representatives or the presentation of any documentation.

The biometric token is used again at the baggage drop when divesting the checked bags. Under the on-airport scenario, for passengers who did not check in online to confirm their biometric token, the passport can be scanned at the self-service kiosk and the passengers can continue the biometric check-in experience from that point forward. This process requires a longer transaction time at the self-service kiosk, however, to account for the document verification process. At any step in the check-in journey, passengers can opt out of the biometric check-in process and continue to use the self-service kiosks and counter bag drops using the traditional process. The traditional process at check-in involves physical interaction with airline customer service representatives to verify identification rather than the use of biometrics to obviate the need for such interaction.

Source: Delta Air Lines

Figure 4-17: Biometric check-in kiosk at ATL Terminal F

While biometric check-in in the United States currently has predominantly been applied to international flights because of the use of passport data as the biometric check, developments to allow biometrics for domestic flights are currently underway. Delta Air Lines is trialing curb-to-gate biometrics for domestic passengers at Detroit Metropolitan Wayne County Airport (DTW). Passengers with a passport and Known Traveler Number from enrollment in Global Entry® or TSA PreCheck™, can store these identification documents in their SkyMiles profile and opt in at check-in on the Delta mobile app. Delta is not planning to save the biometric data used. This trial is limited in scope as only domestic passengers who have both a passport and Known Traveler Number can participate.

The ability to use biometrics for domestic flights on a larger scale without a separate enrollment process will likely require access to additional databases of biometric information, such as state-issued drivers' licenses, to be able to make the facial biometric match. Leveraging drivers' license data could expand the numbers of stakeholders, which currently include passengers, the airport, airlines, and government agencies (e.g., CBP, TSA) to include state agencies as well.

There are three primary benefits that could accrue though the use of biometrics in the check-in process:

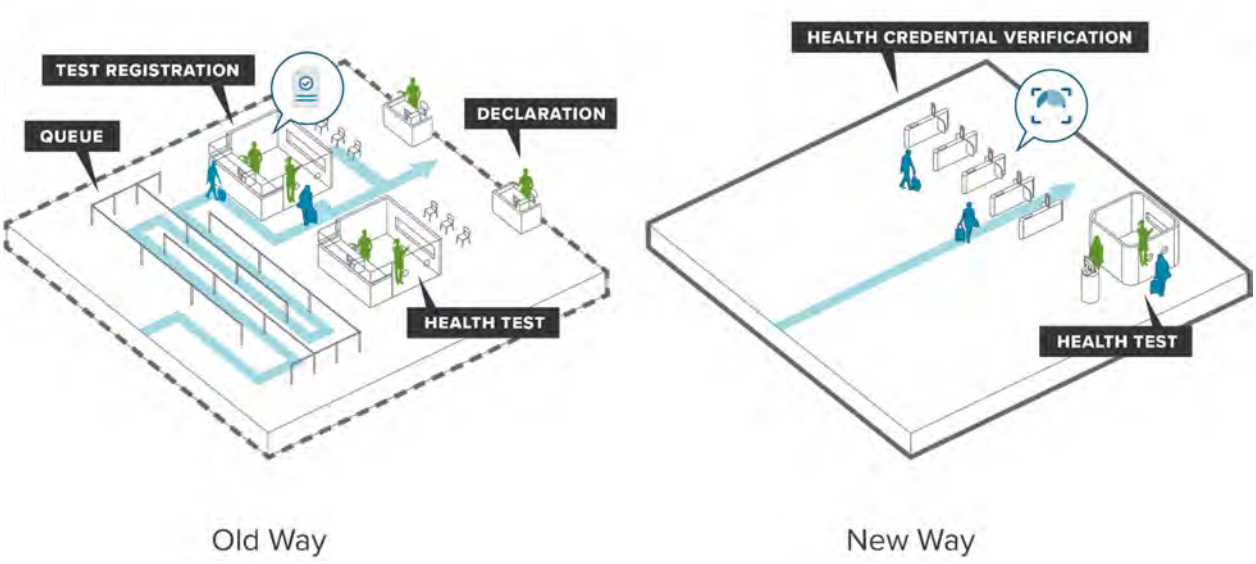
- Biometric use at terminal check-in can reduce space required for the queuing of passengers. There are benefits to both remote biometric enrollment and on-airport biometric enrollment for check-in, but remote biometric enrollment provides the most benefit to the overall check-in process as it affects more steps in the check-in process. Reduced transaction times at kiosks, bag drops, and counters should reduce

the overall requirement for the space to accommodate these processors in the check-in lobby. Even if passengers need to register their biometric on-airport at the kiosk, the remaining downstream processors can benefit from reduced transaction times. Regardless of the scenario, the spatial requirement of the check-in hall should decrease, which can postpone costly capital expansion or reconfiguration of facilities.

- Biometric use at terminal check-in can reduce the number of staff in the terminal check-in area. From a staffing perspective, biometrics in the check-in lobby should reduce airline staffing requirements. While some airline agents would still be required to roam the lobby and assist passengers who require exception handling, the number of passengers requiring direct agent interaction should be reduced. For passengers, the shorter processing times at the airport provide for an enhanced customer experience and reduced stress. In severely congested terminals, airports may also be able to reduce operational staff that are deployed to managing overflowing passenger queues.
- Accurate identification matching. By reducing the reliance on human interactions in the form of ID checks, it also creates enhanced security for all users by providing for more accurate identification matching.

Health Screening Has Received Heightened Attention Given the COVID-19 Pandemic and Biometrics can Play a Role in This Emerging Function

While solutions are currently in early development, health screening now plays an important role in the passenger travel experience. Currently most U.S. airlines ask passengers to "self-certify" their health status during the check-in process. This process involves answering a few questions on the airline mobile phone application or at the check-in counter. While not time-intensive, this self-certification does take longer and depends upon the passenger providing accurate and honest responses without external verification. As the process of health screening is better understood and more widely adopted, it is reasonable to assume that biometrics will eventually contribute to the process.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-18: Health screening touchpoint that may leverage biometrics

Programs such as VeriFLY at Denver International Airport have taken the first step to identify passengers who are willing to enroll in a program that uses their facial biometric template and enables confirmation of their health status on the day of travel to receive security screening and concourse train access isolated from the general traveling public.

Future capabilities of VeriFLY could include a connection to a passenger's health records to confirm testing certifications or vaccinations required to travel to certain destinations. Airports and airlines are also beginning to provide medical testing resources as well. As these solutions continue to evolve, biometrics could be utilized to link these results to a passenger's profile to allow them access to security or to board the aircraft.

Source: homelandsecuritytoday.us (Oct 6,2020)

Figure 4-19: VeriFLY e-gate access to security queue

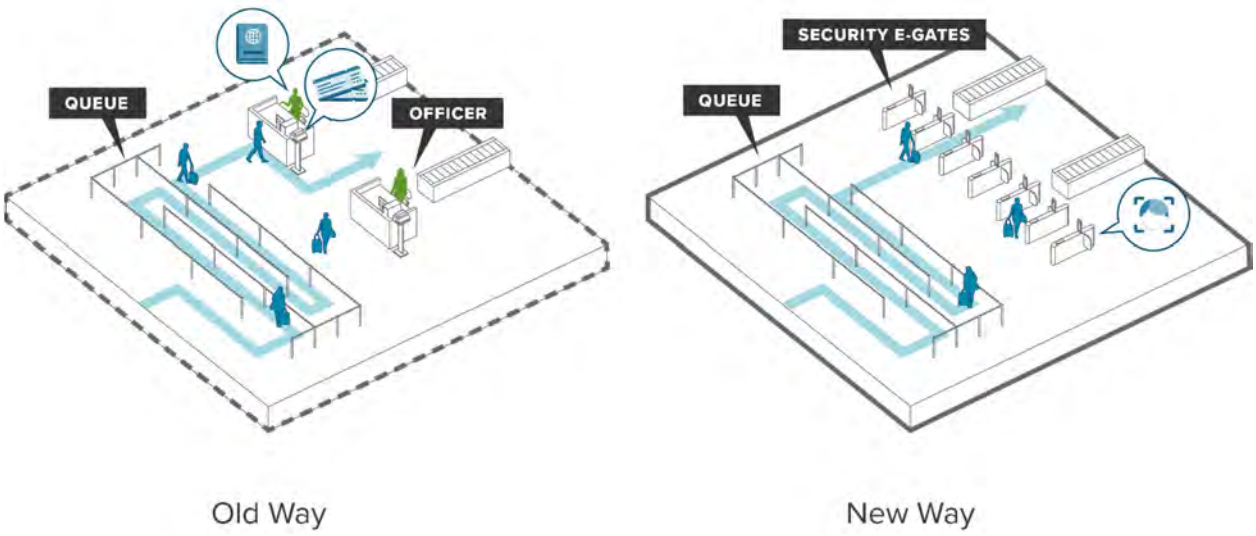
Benefits to staffing levels or terminal space are difficult to estimate as they would vary on the specifics of the implementation and the unique circumstances, but it is anticipated that biometrics may reduce the burden for health screening to occur on the airport as passenger records could be made available more easily through a biometric token. One potential benefit in times of severe outbreaks would be the ability of a passenger's identity to be determined by technological interfaces, rather than interaction with airport or airline personnel.

Biometrics are Currently Being Used to Enable Priority Security Checkpoint Access by Low-Risk Passengers to Enhance the Overall Customer Experience

Biometrics are currently being deployed prior to the security checkpoint to verify a passenger's identification and acceptance into security screening. In some cases, programs like CLEAR® or VeriFLY go a step further and allow enrolled low-risk passengers to use their biometric token to bypass the queue and reach the checkpoint faster than other passengers. As with upstream processes like check-in, biometric

identification of passengers that are not part of a membership program, like CLEAR®, is currently limited to international departures and domestic trusted travelers. Expansion to additional domestic passengers is under development and is a TSA goal as issued in their September 2018 *TSA Biometrics Roadmap for Aviation Security and the Passenger Experience*. TSA and CBP have developed proofs of concept to explore expanded use of TVS at the checkpoint through data integration between TVS and TSA Secure Flight. Additionally, in September 2018 TSA began collecting photos of travelers who renewed in person or were enrolling in TSA PreCheck™ for the first time. As an initial step, in 2020, TSA piloted a touchless self-service technology at the checkpoint to match a traveler's live photo with the photo on their government issued identification. These photographs are not being stored and are only used for identity verification.

Expanding to a larger pool of domestic passengers without requiring a separate enrollment process requires additional coordination and access to a biometric database larger than federally issued passports, such as state-issued drivers' licenses for example. Notably, the emergence of REAL ID, on its own, state-issued driver's licenses does not create a centralized database that enables the ability to match a person to their biometric data; rather, the purpose of REAL ID is to make identity documents more consistent and secure.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-20: Security checkpoint touchpoint that may leverage biometrics

Stakeholders involved with the use of biometrics at security screening include the airport, passengers, TSA, and any governmental agencies that may be required to verify identification for entry/exit purposes (e.g., CBP). Benefits to deploying biometrics at the entry to security are primarily security driven. The benefits include:

- There is enhanced security and more accurate identification matching from biometrics than from manual review of a photo ID.
- Biometrics also reduce touchpoints to create a more seamless process and one that should verify a passenger's identity in less time.
- The number of staff required to verify passenger identification and documents may also be reduced because of the increased throughput.

- The increased throughput generated from reduced transaction times at ID check however is still metered by the capacity of the security checkpoint lanes themselves, so close coordination is required to ensure that the screening lanes are providing sufficient capacity to avoid queues between ID check and the lanes themselves. As a result, there may be limited space savings in the terminal.

Employee Access and Screening

Biometrics are already in place for employees working in an airport environment. All employees who are allowed access to the secured areas of an airport must be approved for a SIDA badge. While these badges are issued by the airport and require employees to meet certain TSA requirements, additional identification verification is required to prove the person's identity. In addition, fingerprints are taken as part of the conduct of a background check.

Though their Transportation Security Clearinghouse, the American Association of Airport Executives (AAAE) handles the biometric background checks for aviation workers at many airports as well as Telos ID. As of 2015, AAAE have processed more than 15.6 million fingerprint-based criminal history records and 6.8 million STAs.

Doors and access points in the airport environment are controlled in several ways depending on the access purpose. Some access points, such as passenger boarding bridges, may require a badge scan and a multi-digit access code to allow for non-domicile airline crew to access. Others, however, may require a badge scan plus fingerprints or iris scan to gain entry, especially between non-secure and secured areas of the airport.

Given airports are accustomed to rolling out access control for employees, operators may wish to trial equipment and processes associated with biometrics for enhanced employee access points. For one, the privacy concerns of employees are different than those associated with employees who undergo background checks and documentation for the purposes of obtaining an airport badge. Secondly, airport operators can observe the performance of the equipment and the enhanced process to address: (1) whether the enhanced process faster, and if so, how much faster; (2) what is the equipment's performance in terms of maintenance; and (3) what is the backup process when equipment fails, or exceptions that must be addressed. Finally, if airports are to gather biometric data beyond that already on file (e.g., iris), airports will have a trial experience for a smaller population with respect to how much effort will go into enrollment, in terms of labor and equipment, and space requirements.

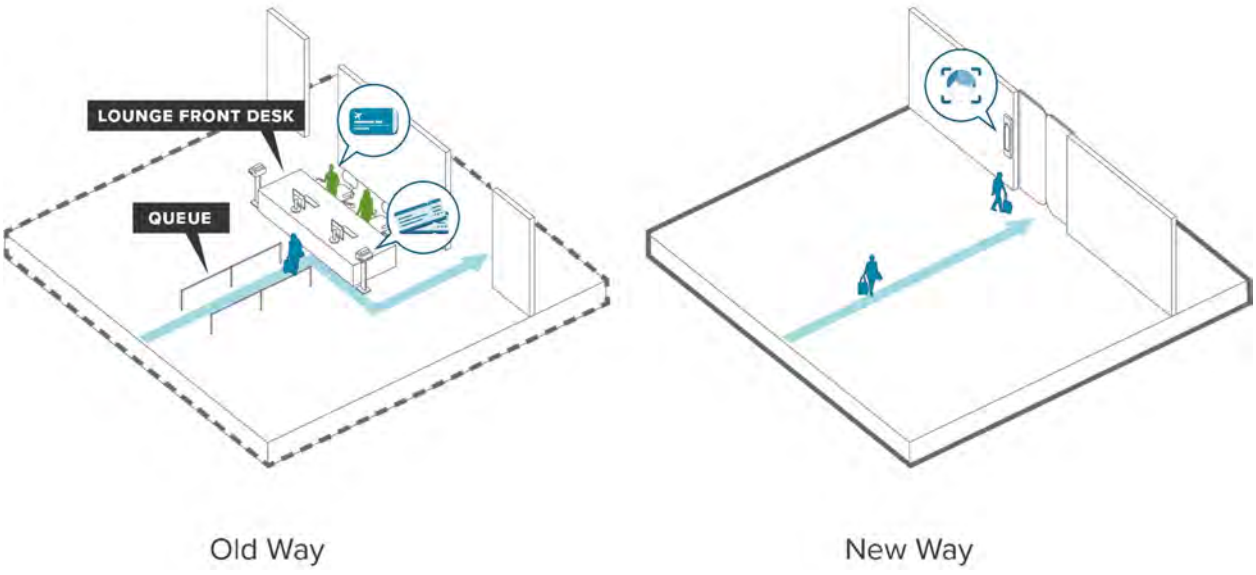
Biometrics Have Long Been Used by Airlines to Provide Access to a Smaller Subset of Passengers who Utilize Airline Club Lounges

An early adoption of biometrics at airports occurred within the airline lounge. Dating back to 2014, Alaska Airlines trialed opt-in fingerprint scanning to provide access to passengers at the airline's four Board Room airport lounges. In mid-2017, Delta Air Lines introduced biometric check-in for Delta Sky Club guests with CLEAR® memberships at its Ronald Reagan Washington National (DCA) Sky Club. The biometric check-in option rolled out to all 50 U.S. Sky Club locations in early 2018 and is free for Delta Sky Club members who are U.S. citizens or permanent residents (those who are not already paying members of CLEAR®). Other lounge providers such as American Express and their Centurion lounges have taken steps toward biometric access. These include providing QR codes as part of the access credential, however a positive ID check is currently still required. Lounge access could eventually be incorporated into the biometric seamless journey, where one biometric token is used to verify access, including at lounge entry.

Source: Delta Air Lines

Figure 4-21: Delta Sky Club fingerprint access scanner

Lounges are unique from other terminal functional areas in that they affect a smaller number of passengers and are largely controlled by an airline or third-party operator. The stakeholders involved in the biometric deployment are primarily the passengers and airlines or third-party lounge operator. Also unique from other terminal functional areas, biometrics applied to the airline lounge environment is not likely to reduce the space required. It may have a staff savings, but this would only apply to the airline or lounge operator.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-22: Airline lounge touchpoint that may leverage biometrics

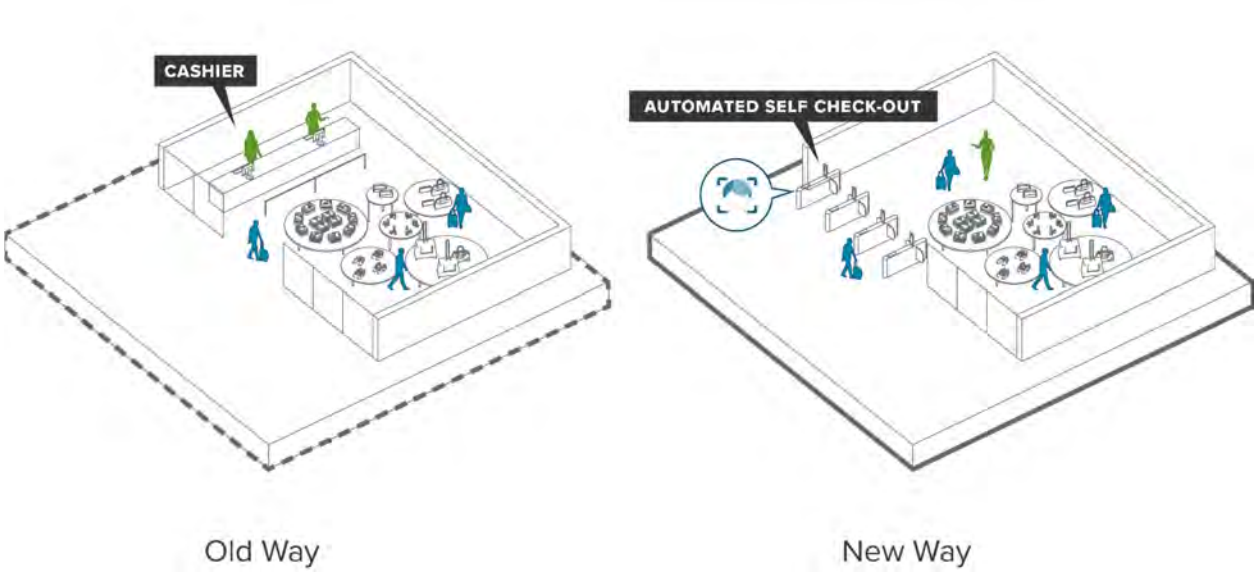
Passengers benefit from the use of biometrics at lounge check-in. The process is faster and does not require the passenger to produce an ID or membership card. Additionally, this provides an enhanced verification process and reduces any potential membership errors.

Biometrics have not yet Been Integrated into an Airport Concessions and Retail Environment

Biometrics do not currently play a large role in the airport concession and retail arena. While self-checkout and app delivery services have been introduced in the airport environment, these services have not yet been tied to a biometric token. In Schiphol Plaza, located at Amsterdam Schiphol Airport, Dutch supermarket chain Albert Heijn trialed a digital store accessed by customers with their contactless debit card.

A future step could involve adding a biometric token to increase security and further expand mobile payments. Additionally, technologies, such as those used by Amazon in its Amazon Go convenience stores are being made available for adaptation to other environments. This "Just Walk Out" technology could shift from a supermarket application to an airport retail environment, for example. As with Amazon Go stores, access could be restricted by an e-gate to limit those travelers who do not have the biometric token available.

Additionally, third party programs such as CLEAR® have been exploring biometric opportunities at concession stands in baseball and football stadiums. In Seattle, for example, fans can link their driver's license and a credit card to their CLEAR® account and use their fingerprint to purchase food and drinks. At Citi Field in New York, concession items are placed on a self-checkout unit where they are scanned and charged to the CLEAR® account associated with the fingerprint.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-23: Concession and retail stores that may leverage biometrics

The primary stakeholders for integrating biometrics into concession and retail areas are passengers, concessionaires, and the airport.

Removing traditional cashier positions and payment systems provides the ability to break down many of the physical barriers separating concession spaces from other functional areas like the holdroom to create

a more open-space and open-flow concept. Biometric payment systems would also reduce the staffing needs of the concessionaire and allow employees to focus their time assisting customers. As has been seen in Amazon Go convenience stores, a seamless, touchless shopping experience would reduce queues, reduce stress, and increase the time passengers have to spend money before departure.

Self-Boarding has Been Using Biometrics for Several Years and its Deployment may be Accelerated

In recent years, biometrics has been applied to the aircraft boarding process with a focus on international departing flights. American Airlines, Delta Air Lines, and JetBlue are among some of the U.S. based airlines using biometric boarding for international departures. In addition, there is participation by foreign-flag carriers such as British Airways and Lufthansa. There are two primary biometric boarding systems being utilized at U.S. airports: (1) e-gates, and (2) camera on a stick.

In both models, a passenger walks up to a camera where their photo is compared against the biometric templates of other passengers on the flight. No passport or boarding pass is required. Once a match is made, either the e-gate opens, or an airline gate agent allows the passenger to board. If a passenger chooses to opt out or if there is an error in the matching, a passenger must see an airline gate agent for manual processing of the boarding pass and passport.

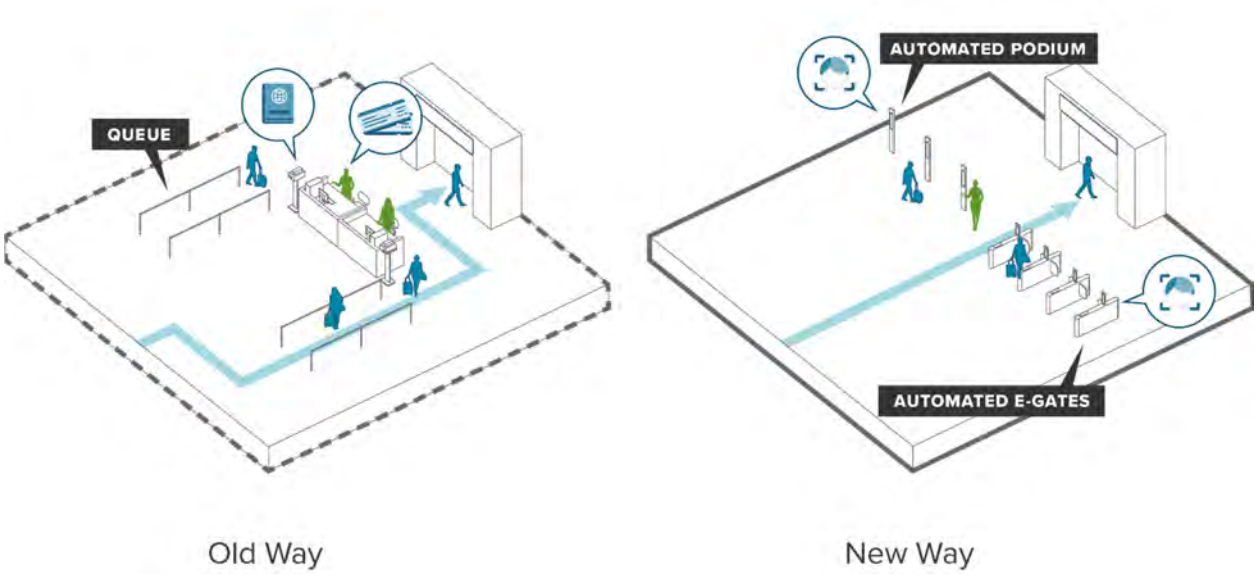
Source: Vision Box, LAX

Figure 4-24: Self-boarding lanes at LAX TBIT

It is important to understand these two self-boarding systems as they relate to exclusive-use and common-use terminal systems. Many airlines prefer to utilize their own equipment and have exclusive connections to their Departure Control Systems (DCS), limiting access to other airlines. Common-use facilities require connections to multiple DCS and must accommodate different airline operating procedures. For the e-gates installed at Los Angeles International Airport (LAX) Tom Bradley International Terminal, a common-use facility, airlines are enabling use of the system on an individual basis. While installation of the e-gates was funded by the airport authority as part of a terminal capital project, planned recovery of full projects costs would occur through landing fees, terminal rates and charges, and other non-aeronautical revenues.

As a result of the extra equipment required to accommodate biometric boarding, the location of the customer service podium may need to be relocated to ensure there is sufficient clearance around the

boarding door for the camera podium and possibly the e-gate. Electrical connections are also required in this area, though some may exist already to accommodate the boarding pass scanner and agent computer. If e-gates are utilized as the preferred process, additional factors require consideration including providing an Americans with Disabilities Act compliant lane as well as barriers to prevent passengers from bypassing the e-gate.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-25: Boarding gates may leverage biometrics

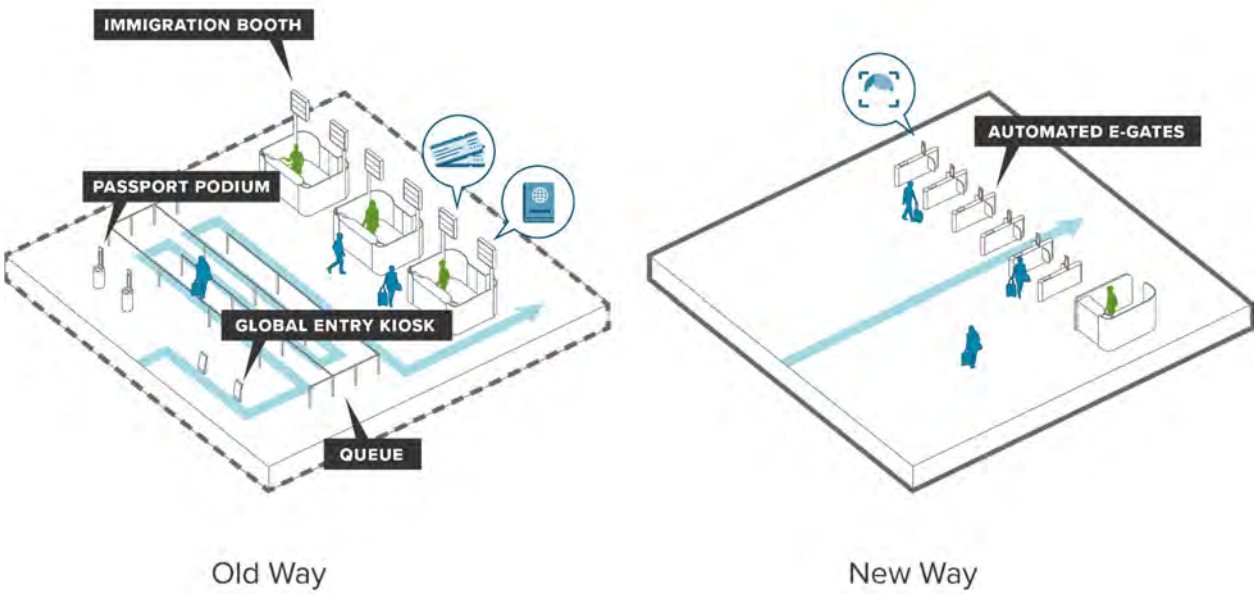
Participation by several stakeholders is required to successfully implement biometric boarding. These include the airport, airlines, passengers, and CBP in the case of international departing flights.
There are three primary benefits that could accrue through the use of biometrics at boarding:

- Biometric boarding can improve the passenger experience and enhance security. Passengers are provided with a touchless experience without the need to present identification or boarding passes. There is also the added level of security and safety in ensuring that the current passengers are boarding the aircraft.
- Biometric boarding can help airports with constrained gate facilities. According to initial feedback from Delta Air Lines, biometric boarding reduced each passenger's boarding time by two seconds, which resulted in nine minutes of savings on a wide body aircraft. For Lufthansa, its trials showed that 350 passengers could be boarded onto an Airbus A380 in 20 minutes. Reducing aircraft ground time and gate occupancy time could allow for additional flights to be accommodated at airports with constrained facilities.
- Biometric boarding can reduce holdroom congestion. Faster aircraft boarding times could reduce the space required for passenger queueing inside the holdroom, allowing that space to be used for seating or other purposes.

CBP has Been a Recent Model for Biometric Adaptation Through "Simplified Arrival" and Trusted Traveler Programs

Over 50 million passengers have been processed to date upon entry to the United States through what CBP refers to as the "Simplified Arrival" process. Using an airline manifest and a cloud-based matching

service, CBP retrieves existing traveler images from government records and builds a photo gallery of expected travelers prior to the flight's arrival. As arriving passengers approach the primary inspection booth, CBP takes a photo of each traveler and compares it against the pre-assembled gallery to find a match. With a match, the CBP officer can complete the inspection in a few seconds. If a match cannot be made, the CBP officer reverts to the original process and manually inspects the passenger's travel documents.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-26: CBP leveraging biometrics

Biometrics is also currently implemented as part of Global Entry®, NEXUS and other CBP trusted traveler programs as a way of processing low-risk travelers to the United States. Recent updates to Global Entry® have created a more streamlined process where, in addition to shifting from fingerprint to facial biometrics, the typical customs-related questions put to passengers have been eliminated from the process completely.

The three primary stakeholders for a biometric implementation at immigration and customs include the airport, airlines, passengers, and CBP. There are three primary benefits that could accrue though CBP' use of biometrics:

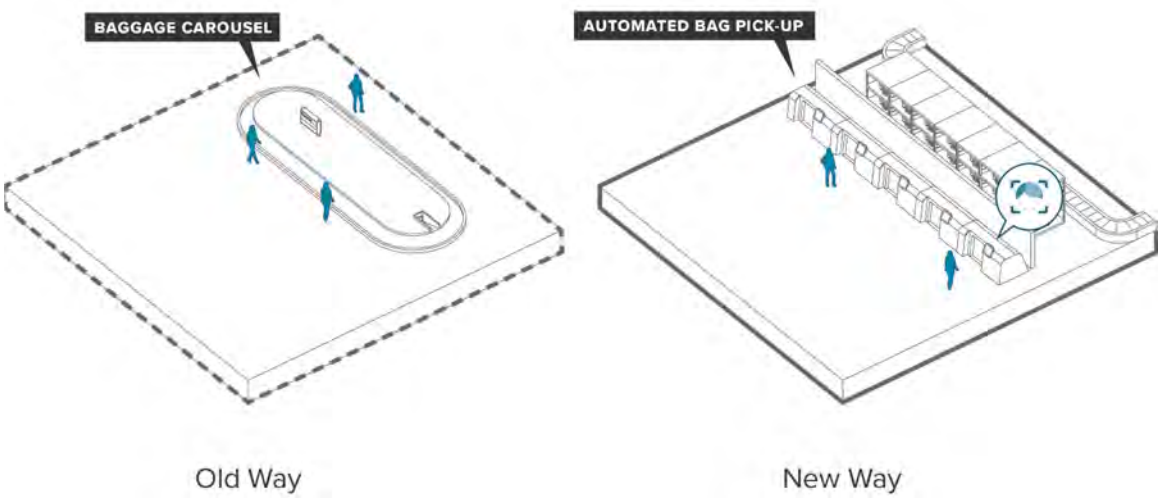
- Integrating biometrics into the immigration process will reduce the spatial needs within the terminal. Large fixed immigration booths organized in a linear fashion can be replaced by smaller podia and eventually by mobile units. These touchpoints can shrink in size over time since less of the passenger processing will need to occur at the booth or podia.
- Biometrics increase throughput capacity and reducing passenger processing time. Under Simplified Arrival, CBP can clear arriving flights an average of near 12 minutes faster than using the traditional manual processing methods. In addition to the savings generated by Simplified Arrival, CBP says the new Global Entry® kiosks have reduced the processing time of eligible passengers by nearly 90%, from 45 seconds to less than six seconds. Passengers benefit both from faster processing times and an increased touchless experience.
- CBP offices can spend more time on higher-risk passengers. Shifting away from the longer manual process allows CBP officers to refocus their time from low-risk passengers to higher-risk passengers.

This streamlines the passport check process and provides a safety and security benefit, as there is reduced risk of the imposter threat and increased identity assurance. These efficiencies may provide a staffing benefit to CBP as they can be more efficient in their resourcing.

The model CBP used for biometrics could serve as a basis for identity verification for TSA. Several airports already have systems deployed to use CBP's model to facilitate touchless identity checks through security screening checkpoints.

Biometrics in the Baggage Claim Will Require the Largest Structural Modification to the Arrival Process

Reuniting passengers with their checked baggage has remained a largely manual process, requiring passengers to self-identify their bags from a wide selection on an arriving flight. This "honor system" process has traditionally been validated, when necessary, by matching the serial number on the bag tag against the passenger's receipt. For biometrics to be integrated into the baggage reclaim process, a passenger's biometric token would be required to call for the specific bag to be delivered to bag claim. This would likely require the replacement of traditional sloped- or flat-plate baggage claim units with something resembling more of a back-of-house baggage storage system or Amazon locker system. Bags would be retrieved one at a time once called for by the passenger's biometric token. While the elimination of baggage claim belts would free up space in baggage claim, this space would possibly be replaced by infrastructure required for baggage storage and retrieval systems, similar to a bag drop machine. Passengers on an arriving flight tend to approach baggage claim in a much shorter time distribution than departing passengers, potentially driving up the baggage claim retrieval requirement.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-27: Baggage reclaim leveraging biometrics for self-service

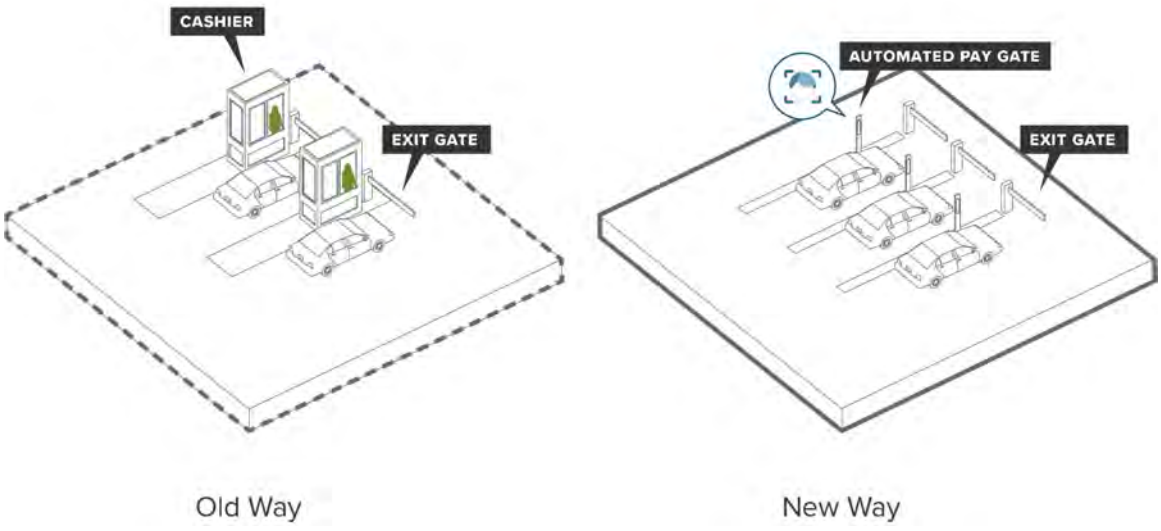
The stakeholders required to consider a biometric implementation at baggage claim would include the airport, passengers, and airlines or their ground handlers. Unlike many of the other functional areas in the airport, incorporating biometrics would require significant physical modifications, so increased coordination among stakeholders would be required to ensure a successful deployment.

Biometrics would improve the security of the baggage retrieval process as there would be fewer opportunities for bags to be stolen or picked up by mistake. Staff savings are not expected to be significant as the baggage claim process is generally less staff-intensive compared to other functional areas. Staff would still be required at the baggage service desk, as tug operators, and as bag porters. Given that the number of bags stolen or lost at baggage claim is relatively low and limited airline resources are already available at baggage claim, the true benefits of implementing a full biometric reclaim process may not outweigh the costs of added security patrols and the airline liability associated with baggage replacement.

A less intensive implementation of biometrics in the baggage claim could focus primarily on identifying bag thefts or mismatched bags, as opposed to ensuring that the chain of custody between the bag and the passenger is maintained. Biometric readers and bag tag scanners installed at the baggage claim exits could be used to confirm that a bag, which is claimed from the belt as it is done today, belongs to its owner. This concept would have significantly less capital cost and require less modification to the facility but would not completely ensure that the passenger receives the correct bag. It would simply identify mismatched or stolen bags. Facility modifications would include creating a controlled access to the baggage claim area, to ensure bags are scanned when leaving the baggage claim. The cost for the biometric implementation would have to be weighed against the liability incurred with lost or stolen bags.

Ground Transportation Biometrics are Being Trialed Using Some Modes Such as Rental Cars and Rail

Ground transportation is the first and last stage in the passenger journey to and from the airport. Residents may use the on-airport parking facilities, for example, while visitors may rent a car. Biometrics have had limited exposure to airport ground transportation. The most prominent example is in the rental car industry. At the end of 2018, Hertz announced a partnership with CLEAR® to launch *Hertz Fast Lane powered by CLEAR®*, a service that would use biometrics to speed up the car rental and exit process to get customers on the road in 30 seconds or less. Customers would use their facial biometric to confirm identity in place of showing the exit booth employee a driver's license. This was the first use of biometrics by a major rental car company. The program was expanded to several airport locations but in July 2020 due to the Hertz bankruptcy, it was announced that the program would be discontinued.

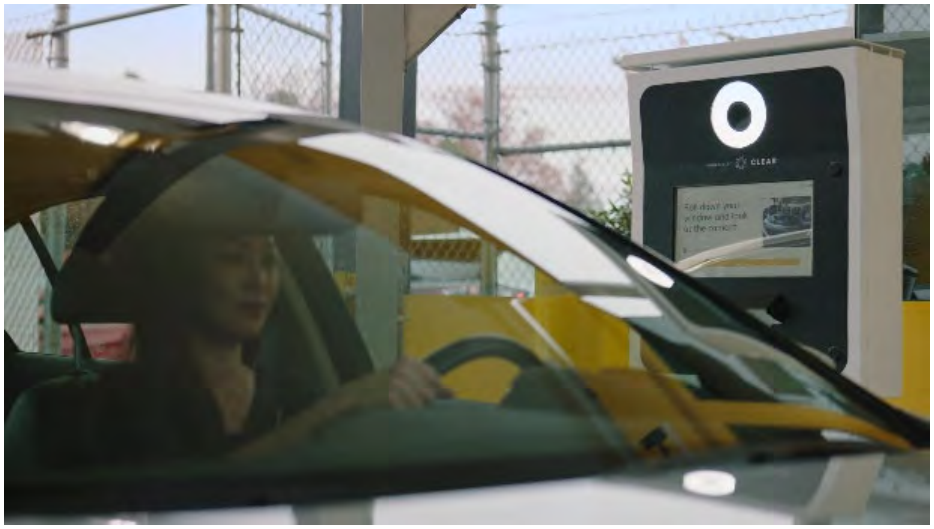


Source: Inter*VISTAS* Consulting Inc.

Figure 4-28: Ground transportation touchpoints leveraging biometrics

It is anticipated that biometric tokens will soon allow passengers to pay for other ground transportation services such as parking transactions as well as train tickets. Biometric trials for train ticket checks and border exit processes are expected to start in March 2021 on the Eurostar departures from London St. Pancras. Biometrics could be expanded to parking facilities to allow passengers to pay for parking transactions without needing to stop at a pay station or pay gate.

Stakeholders would include passengers, the airport, ground transportation operators and concessionaires (e.g., parking concessionaire, transportation network companies, rental car companies), as well as local transit agencies (e.g., bus, rail).



Source: Hertz

Figure 4-29: Hertz Fast Lane exit

Applying biometrics to ground transportation modes is not anticipated to provide a significant space savings, though the need for ticket lobbies could be reduced. The primary benefit would be felt by passengers who would experience a faster, touchless, and more automated experience.

Evaluation of Biometric Implementations in the Airport Environment

Biometrics can be applied to several functional areas in the terminal and throughout the airport, but airport decisionmakers must decide if there is a strong business case to move forward with a biometric solution and how to best accomplish it. One way to evaluate these questions is to understand where biometrics provide the greatest impact and if there are tradeoffs.

KEY TAKEAWAY

For airport decisionmakers, establishing a strong business case for biometrics is likely to extend beyond financial considerations to include customer service, airport technology goals, passenger safety, operational efficiency, and competitive concerns.

As discussed, biometrics should be treated like an emerging technology with a moving target that is constantly evolving. This technology is leading edge in that:

- There is not a complete U.S. database of biometrics, as eligible passengers are currently limited to those with passports and Trusted Traveler program participation.

- There is a patchwork of laws governing the collection and use of biometric data, which must be navigated, adding to the complexity.
- Biometrics is moving toward multi-stakeholder solutions, with the potential for future use cases to be added over time.

Since every airport is unique, biometric implementations that work at some airports may not be viable at others. This could depend on several factors including passenger demographics, airport size and geography, and the operational profile (e.g., primarily serving international or domestic traffic). Airports that are capacity constrained in some manner will likely be the early adopters with regard to the use of biometrics given the imperative that any incremental benefit, regardless of magnitude, may offer a meaningful overall improvement. Critical factors to be considered:

- Would passenger or facility security (e.g., identity assurance and accuracy) be enhanced?
- Would a small increase in capacity or level of service be meaningful to the overall experience of the population affected?
- Are there reasons besides capacity enhancement and security to implement biometrics, such as the desire to reduce staffing costs or improve the reliability of certain processes?
- Are the stakeholders required to implement the changes supportive of the end goals?

The most mature use of biometrics at the airport involve: (1) airport employees (e.g., access to secured areas); (2) self-boarding of international flights; and (3) the international passengers arrivals process (e.g., CBP's Simplified Arrivals); these models are the most mature in that they have proven to provide greater benefits than other opportunities. Many of these successful implementations have also been driven by airport stakeholders such as airlines and CBP rather than the airport operator. Accordingly, for airport management seeking to implement changes at their facilities, they may place a greater emphasis in these areas rather than others to derive the greatest benefits. Additionally, some airport operators may choose to simply participate in biometrics implementation rather than drive its implementation because:

- CBP, TSA, and the airlines control many of the facilities in the passenger terminal that would be affected by biometrics.
- These stakeholders can access passenger biometric data via CBP/ TVS, and build an enrolled population of passengers, perhaps more easily than airports.

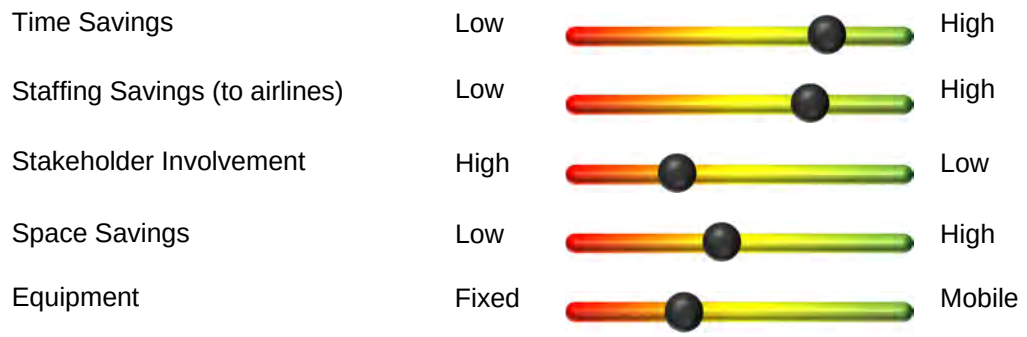
In most cases, the return on investment (ROI) for the airport operator goes beyond strictly financial considerations for the implementation of biometric solutions. Instead of making decisions based solely on the financial ROI, airports are evaluating several additional considerations such as customer service, airport technology goals, passenger safety, operational efficiency, and competitive concerns. To better understand these considerations, airport operators may consider the following questions when evaluating implementation of a biometrics solution.

Do the passengers using your airport have a high rate of passport ownership or Trusted Traveler program membership? Airports with high passport and Trusted Traveler program participation rates provide a significant population of passengers immediately eligible to participate in biometric programs. Further, no additional enrollment process is required for these passengers as the database of biometric data is already developed and maintained. Airports with lower passport and Trusted Traveler participation can still consider biometrics, but operators should consider that an extensive effort to enroll the passenger population will be required. This is an important consideration for states such as Mississippi: there is a major impact on the ability for TSA or self-bag drop processing (where biometrics is required) to use TVS. If an airport operator cannot leverage the existing TVS, the case for a positive overall ROI will be more challenging as more labor, more space in the passenger terminal, and increased marketing of the program by the airport would likely be required.

Do the airlines wish to implement biometrics at your airport and who is paying for the up-front capital investment and the ongoing operations and maintenance of the equipment? In some instances, airlines may be willing to fund biometric implementations, including paying for new equipment, operations, and maintenance, thereby reducing the financial burden on the airport operator. If airlines are not willing to participate in the funding of the program, or if the potential biometric implementation occurs in a common-use facility, the ROI calculation is dramatically different. For example, if an airline wants to install biometric boarding at the gate, the airport may have to pay for the electrical infrastructure to enable the automated boarding gate equipment installation. If there are costs borne by the airport on either the capital or Operations and Management side, this should be a considered as part of the decision for implementation.

Does biometrics significantly reduce processing time, reduce staffing, or reduce space needs? Labor savings may not directly accrue to the airport operator, but savings to airport stakeholders like the airlines, TSA, or CBP can indirectly benefit the airport operator. A lower cost structure for airlines affects their decisions whether to introduce additional service or in more challenging economic circumstances, maintain existing service. In terms of customer service, reduced processing times improve the passenger experience and decrease passenger stress levels. Calm passengers who have additional free time beyond the security checkpoint have been shown to spend more money at airport concession offerings. Finally, if significant reductions in space would accrue as a result of biometrics implementation, the airport operator may be able to defer capacity expansion plans or lease newly available space to interested tenants. As discussed in Chapter 1 and Chapter 2, Biometric interoperability may provide for the most impactful gains in capacity and reductions in space needs. A biometric solution that is applicable to multiple processes along the passenger journey compounds the benefits, however small they might be individually.

Airport operators should review the pros and cons of specific biometric implementations to decide whether implementation is warranted. A graphical example of such a comparison is provided in Figure 4-17 for biometric self-boarding gates. Five dimensions for ROI calculations are advanced that can help assess the overall benefits of costs of biometric implementation.



Source: Inter*VISTAS* Consulting Inc.

Figure 4-30: Sample Evaluation of Biometric Self-Boarding

As described earlier, a biometric self-boarding implementation at the gate has been shown to reduce aircraft boarding time, which provides benefits to both the airlines since time is money and also the airport, since expensive gate expansion projects might be deferred. Some airline customer service staff savings is anticipated, or at a minimum, the reallocation of staff to serve other customer needs is enabled. Depending on whether self-boarding is implemented in an exclusive-use or common-use facility, stakeholder involvement may be limited to one airline or several airlines. The space required for self-boarding may increase, especially if e-gates are utilized, as additional space may be required to handle passenger

exceptions. However, the faster boarding times may reduce passenger queue length in the holdroom, providing needed space for other functions (e.g., increased seating or standing space). Finally, regardless of whether e-gates or camera on a stick is selected as the preferred implementation, the equipment is largely fixed, which means that it is not easily moved with changes in facility layout or facility modifications.

This more-focused evaluation of a specific biometric implementation will also bring to light some unforeseen capital costs that could be required to implement the solution. Examples of these costs include expansion of communication rooms or network bandwidth to accommodate additional data feeds, tinting of windows to help the resolution on camera or document scanners, or the relocation of existing infrastructure.

Reviewing the aforementioned questions, as well as the spectrum of specific implementation considerations like those shown in the slider graphic above, should help airport operators better understand whether to move forward with biometric implementations.

Chapter 5

System Design and Information Technology Architecture

Summary

This chapter focuses on the Information Technology (IT) architecture, when considering biometric technologies and solutions. First, the focus is on the variety of types of biometric credentials, choices for storage of biometric data, and different biometric interaction touchpoints such as e-Gates, camera-on-a-stick, kiosks, and walk-through tunnels. Thereafter, the chapter identifies and explains five distinct IT architecture models to illustrate how the above options tie together, with a real-world example of each to demonstrate its use case.

It is acknowledged that a secure digital biometric identity credential will bring many possibilities and advantages for passenger processing. Nonetheless, the supporting IT architecture design faces a larger challenge with more stakeholders, as interoperability and scalability becomes more complex. With stakeholders in multiple countries, their respective privacy laws also impact the design. On the other hand, with ICAO DTC, an international standard is being developed to create common technical specifications allowing technologies to interact smoothly, while abiding to multiple nations' (and state) laws, and being software, hardware- and vendor-agnostic.

Although the U.S. market is big enough for the broad application of biometric systems such as TVS, U.S. stakeholders might want to consider compliance with future global standards. U.S. stakeholders that invest in systems that are or can adapt to interoperable systems now, may be challenged to change later when a global standard is adopted. In other words, where there is a development of a range of different systems, country specific and extraterritorial application are the norms that will need to be contended with in the future.

Introduction

One of the challenges of a biometric implementation is assessing the IT architecture and associated business cases that can drive the ROI equation. Various drivers such as the existing IT architecture at an airport, meeting performance standards and requirements, and the delivery of the desired objectives may greatly impact that equation.

Many airports are challenged with the exercise because of the scale of the capital investment and the technical know-how required, as well as the complexity to meet stakeholder requirements, achieving alignment and trust. The Primer is not meant to be an all-encompassing standard guide for technicians, rather it provides senior management and executives a comprehensive introduction to the most important concepts and acquaint them with the typical issues covering a range of business risks. By business risks in biometric rollouts, we mean:

- Will the capital program be right-sized for the objectives?

- Are performance specifications (false accept/false reject rates/speed) adequate to meet the desired customer experience?
- Are there risks/vulnerabilities that are introduced by the range of privacy and cybersecurity issues.
- To what extent is scalability built-in in Year 1 versus lifecycle reinvestment in future phases?

For biometric rollouts this is indeed part of the environment due to the different mixture of the facilities age, existing sunk costs as well as the dynamics of the market.

For instance, airports with a population of a low number of passport holders will require more emphasis in their IT strategy on the enrollment of passengers. Other airports using current technologies such as fiberoptic infrastructure backbones will have an opportunity to leverage existing investments.

This chapter represents the culmination of key areas associated with lessons learned on technology architecture that compromise most facilities. Invariably there will be more detailed technical advice needed as well as local program requirements to be solved. These challenges are best solved by project teams that systematically create technology solutions, detail designs, implementation programs, and rollouts. This chapter enables airport management to address some of the pre-emptive questions and considerations to evaluate one's requirements, understand the risks, and evaluate various investment scenarios.

What Is an Information Technology Architecture?

At any airport, the IT architecture describes the IT software, IT platform and IT infrastructure components, as well as how these are designed to work together. In software we recognize the applications, computer programs, and data that drive the airport's processes, passenger services and operational systems. The IT platforms are the operating systems and middleware on which the software runs. As for the IT infrastructure, or hardware, we note the actual computers, network cabling, servers, switches and other physical equipment that are needed for the IT system to function properly. But beside these, software, platform and infrastructure components, the IT *architecture* describes how these are designed to work together in a framework of principles. The IT architecture principles include, for example, technology standards, policies, and guidelines.

KEY TAKEAWAY

An IT architecture is comprised of the IT software, the IT platform and IT infrastructure components, together with the IT architectural principles which describe how these different technology components are designed to work together.

In order for the airport to have a well-functioning IT system that is able to meet the airport's needs, the IT architecture must be well-designed, maintained and upgradable when needed. With airports developing rapidly over time, especially with more technology solutions being implemented in airport processes, services and systems, the IT architecture should be aligned with the airports business/strategic direction, supporting transitional requirements in support of future technology needs. With every airport being unique due to its demography, size, location, culture and other influencing factors, IT architectures are designed to best match the airport's needs.

When it comes to implementing biometric technologies and solutions, existing IT architectures are often redesigned to incorporate these new biometric hardware and software components, and updated principles. For new airports, the IT architecture can be designed from the ground up.

Summarizing:

- **IT architecture software:** the applications, computer programs and data that drive the airports processes, passenger services and operational systems. Examples of biometric software are the

mobile applications or programs used for access control with a fingerprint, or check-in via facial recognition.

- **IT architecture platforms:** include the operating systems and middleware. Operating systems such as Microsoft Windows, Apple OS or Linux are common examples seen on today's laptops and personal computers. Larger IT systems might run on cloud-based platforms such as Amazon Web Services, or Azure. In the latter case, when platforms host sensitive biometric data, it can be important where the platform is located, as it might be in a different country. Middleware is the collection of software that is needed to run certain software or applications.
- **IT architecture infrastructure** is the 'hardware' components such as computers, network cabling, servers, switches and other physical equipment that are needed for the IT system to function properly. Biometric IT infrastructure components are, for example, a fingerprint scanner, a camera that is used for facial recognition or a self-service kiosk with biometric capabilities.
- **IT architectural principles:** Principles should be defined in a solution free manner. This means that the principles are not prescribing any technology, software, hardware or solutions, but only act as criteria for the assessment of the different options when choosing specific solutions or technology. Examples of principles are: (1) privacy-by-design; (2) modularity of components instead of monoliths; (3) performance is more important than costs (or vice versa); (4) stability is more important than innovation; and (5) user experience is most important.

Designing an Airport IT Architecture for Biometrics

When designing an airport IT architecture that incorporates biometric technologies or solutions, several generic architecture models can be chosen as a starting point. In considering the different architecture models, it is good to take note of several factors that influence the architecture model choice.

Governance of the IT Architecture

When designing and implementing an IT architecture, the right governance model must be taken into account. A governance model appoints roles and responsibilities to enterprise architects, solutions architects, product managers, product owners, design thinkers and procurement experts who orchestrate all the developments in line with the design and/or upgrading of the IT architecture.

Single-party or Multi-party Technology Solutions

One of the first main crossroads that the airport/airline/government finds itself at is whether to choose between one of generally two options:

- **A "Single-party"** biometric technology solution is typically the best choice when the airport aims to create a system that services only the one airport, thus leading to an IT architecture that supports the operations for a smaller user group, with less stakeholders.
- **A "Multi-party"** biometric technology solution provides interoperability between multiple stakeholders, often across multiple countries or locations (airports), which thus greatly increases the complexity of the IT architecture. The national Digi Yatra system, utilizing India's government's Aadhaar database (See Chapter 2), is such a solution, where all airports and airline stakeholders are to be users of the country-wide solution.

Stakeholders

Stakeholders are key to determining the feasibility of a concept in a real-world environment. Private and public-sector stakeholders must collaborate to pilot a prototype, apply iterative development methodologies to demonstrate its value, and seek continuous feedback from each other to adapt accordingly. The use of an iterative approach encourages the necessary paradigm shift among stakeholders and establishes an environment for large-scale adoption. Each airport will find itself with a unique mix of stakeholders affecting the IT architecture in a similarly unique way.

Existing IT Architecture

Implementations of biometric technologies and solutions need to align with the existing IT architecture. The existing IT architecture may or may not be ready to support biometric additions, and thus should be assessed.

Airport Size

The airport size has a direct impact on the IT architecture, and the type of (biometric) services to be considered. Due to some IT infrastructure components having a limited range, large airports will need a very different and more extensive network topology to connect hardware over longer distances.

Funding Options

Throughout the world there are major funding gaps as well as insufficient budgets to maintain assets and their IT architecture, which can lead to a higher risk to public safety. Therefore, airport operators may need to evaluate their mechanisms to fund capital and maintenance expenditures. Other mechanisms, beyond the traditional methods, include the following:

- Public-private partnerships can be an effective way of transferring life-cycle costs of infrastructure off public-sector budgets and simultaneously create investable assets for the private sector.
- A regional approach to infrastructure rather than direct funding from a country's government. This is especially true as urbanization transforms many of our global cities into mega-regions, requiring broad and interconnected infrastructure systems.
- Dynamic pricing is a usage charge policy that can both increase revenues and ensure the efficient use of infrastructure assets. This policy can be linked to peak hour congestion and passenger facility fees during peak travel times.

Depending on the funding, the IT architecture design may need to be very selective of what it hopes to achieve, or be able to expand on its design and incorporate more generous flexibility for future expansion.

Biometric IT Architecture Infrastructure Components

In the implementation of biometric technologies and solutions, there are three design choices that have the largest impact on the actual physical infrastructure components, or the hardware of the IT architecture. These are:

- What biometric *credential* to use?
- How to *store* biometric data?
- How do we design the *interaction* of the passenger at biometric touchpoints?

KEY TAKEAWAY

There are various IT aspects which need to be considered, from the type of credential, how it is stored, and how the interaction at touchpoints is designed, when implementing biometric technologies and solutions. These choices greatly impact the hardware components of the IT architecture.

Often, technology specifications of infrastructure, communication protocols, and other details such as how data is stored are left to the designer of the system, which in many cases is the vendor of the technology solution. Nonetheless, choices that an airport/airline/government makes related to performance, envisioned use and interoperability, have a significant impact on which infrastructure components should be considered. Also, these can have significant capital impacts such as upgrading existing infrastructure, or replacing various components to address legacy issues and new technology standards and performance. For that reason, it is good to be familiar with the following considerations:

- **Type of biometric credential:** The credential is an object or data structure that authoritatively binds an identity to an authenticator. This can be done via one or multiple authenticators, such as a biometric. Examples of physiological biometrics are one's face, fingerprints, hands or irises. Examples of behavioral biometrics are one's signature, voice and keystroke. The selection of the biometric affects the choice of the type of credential and inherently affects the IT architecture.
- **Type of storage for biometric data:** The type of storage, in this case for the storage of the biometric data, opens the discussion of data ownership, location and also protection against data theft or misuse. Biometric data can for instance be stored in a database, locally or over the internet in the cloud, it can be stored on one's own smartphone or on an access card or token. The type of storage chosen impacts how the passenger can use his biometrics with the airport processes, services, and systems, and how the IT architecture is to support those uses.
- **Type of interaction with passenger/customer/user at biometric touchpoints:** There are several types of kiosks, e-Gates, camera-on-a-stick, or other forms of touchpoint hardware which may facilitate the interaction of a passenger/staff member with the biometric technology and solutions. The choice for the type of interaction impacts which infrastructure components are utilized and thus the IT architecture.

Biometric Credentials

A biometric credential is an object or data structure that authoritatively binds an identity—via an identifier or multiple identifiers—to at least one authenticator owned and controlled by a subscriber (passenger or airport staff). The following credential types are discussed in this section:

- e-Passport
- Card, token or pass
- Digital credentials of three types
- Government issued identity cards

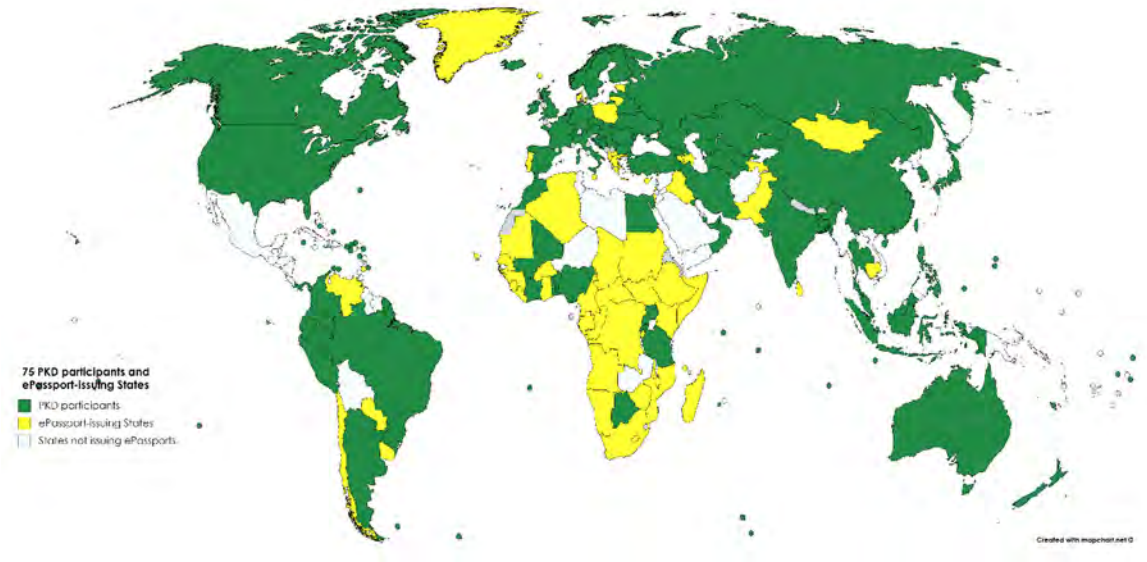
e-Passport

The most evident globally accepted process to verify a person's identity is a physical passport that is issued by the passport holder's home authorities. Under auspices of ICAO the first standardization of the details on a passport developed in 1980. Standardization included the person's image, a standard format machine readable zone and the passport holder's biographical information. The identity of a person can be verified by border officers manually, comparing a live person to the image in the Passport. In 1998 the format was upgraded with the introduction of an embedded electronic microprocessor chip (hence e-Passport) which could contain both biographic and biometric information. It uses contactless smart card technology, including a radio-frequency identification chip embedded in the passport. The passport's critical information is printed on the data page of the passport, repeated on the machine-readable lines and stored on the chip with a country specific "digital signature".

Currently there are more than 100 countries issuing e-Passports. Their digital signatures are unique to each country and can be verified by using the originating country's respective certificates. A digital signature on an e-Passport is authenticated by the issuing State's security certificates—the Country Signing Certification Authority (CSCA) Certificate and the Document Signer Certificate. Together, the signature and certificates form a trust chain wherein the CSCA certificate is securely anchored in the authority of the issuing State and the Document Signer Certificate is securely stored in the chip of the e-Passport as the Document Security Object.

To validate an e-Passport at an international border, the border control system retrieves the Document Security Object from the chip. The CSCA certificate can be derived from the ICAO Public Key Directory, which is a database maintained by the ICAO to facilitate the secure, online sharing of information between States. Certificates, however, can also be exchanged through a bilateral exchange process.

The data elements that are contained on the chip of the e-Passport are the biographic details of the passport holder as well as an encoded digital photograph. An e-Passport contains additional data fields for fingerprint and iris data. The actual storage of this biometric data on the e-Passport is optional, depending on the individual country's legislation and policies.



Source: http://gis.icao.int/epassport/

Figure 5-1. Countries that issue biometric e-Passports as of mid-2019

Card, Token, or Pass

A token system (portable) uses a smart card or a fob to store biometric data. This means that your fingerprint, once captured, is stored within the token. The benefits of storing biometric data on a portable token are that it need not be transferred over a network for verification purposes, and so this reduces the risks that can come with network-related vulnerabilities. When using this method, the user will need to present his/her card or fob and then his/her biometric data as a two-step authentication process.

Digital Credential, Self-Sovereign Identity

The most recent development in biometric passenger processing is the concept of Self-Sovereign Identity (SSI). An SSI is "owned" by the individual just like a physical passport. As owner, the individual has access to, can refer to and share components of this identity at his/her discretion. While certain components of the identity are established by issuing authorities (i.e., passport number, bank details), the individual must consent to the sharing of his/her identity and any related data. This is achieved by individuals securely storing their own identity data on their own mobile devices and providing it upon request to those who need to validate it.

Just like with the format of the e-Passport, the New Technologies Working Group of ICAO has recently published guidelines for developing these digital travel credentials, titled the "Guiding core principles for the development of a Digital Travel Credential". The ICAO workgroup defined four basic criteria with which the credential needs to comply:

- It should be produced from a Travel Document Issuing Authority:
- Capable of being supplied unaltered to verifying entities in advance of the traveler's journey or arrival:
- Globally interoperable to ensure that it can be used for different use cases; and
- Adopted by travelers.

The DTC workgroup is opting for a hybrid credential which is a combination of a virtual credential (biometric template) that is linked to one or more physical credentials (authenticators). The credentials could be stored in a remote system, such as a database or webserver, and the authenticator could be an e-Passport, smart card, or mobile phone.

In developing a credential, it will need to be embraced by governments, industry, and citizens, and accepted throughout the world which is an inherently complex undertaking that will take time. With the recent COVID-19 experience, travel documents may need to incorporate health certificates, and consideration of this is needed in the development of the DTC. This requirement could increase the need to develop a global solution.

Digital Credential, on a Mobile Device

Smart mobile devices provide a platform for individuals to carry and provide a digital credential which is trusted, with a unique ID number which resides on the device. This allows the individual to provide a digital credential in place a traditional physical credential. It also offers the same functionality of a physical credential when accessing a secure or controlled area.

Digital Credential, In a Blockchain

Distributed ledgers, such as blockchain, are a developing technology that are proving to be adaptable across industries, providing cost effective and secure real-time (data) transactions between two parties. The data stored is secure and immutable by design, because the data transferred is recorded and verified by all the different "participants" or computers (called nodes) in the system (thus the term distributed). This creates a database of data records that offers transparency and traceability.

In many biometric identity solutions that utilize blockchain technology, it is not the actual credential that is stored in the blockchain, but rather a record of successful verification of that identity. These records are called verified claims of identity, which can be shared as proof of verified and authentic identity.

These solutions often connect through an untrusted medium (e.g., the Internet) and thus require a secure connection and strong authentication (of the device, software, user, environment, etc.). Due to their complexity, implementation is often achieved with the involvement of specialized technology partners.

Government Issued Identity Cards

Identity cards are issued in many countries while some countries are still discussing their implementation. These cards can also contain biometrics, much like the e-Passport.

Biometric Data Storage

There are various forms of storage which are utilized, and they will work with more than one mechanism to be able to deliver the desired solution. In this chapter we discuss the following storage mechanisms:

- Centralized server or in a local data center (on premise)
- Secure cloud in a remote data center
- Mobile devices such as smartphones
- Distributed databases and ledgers

Centralized Server or Data center

A centralized server is one way to store data, which allows biometric technologies and solutions to access data at any location connected to the server. In some cases, the centralized server only offers connections to the systems at the airport, not outside it. In cases where the server is connected to the internet, it is susceptible to a cyber-attack. To reduce the risk of the server being breached and the data stolen or copied, the data must be encrypted when stored or transferred over the network. The issue with encryption is deciding where encryption keys will be stored and who will be trusted with their access. With the implementation of data and privacy protection, there are increased responsibilities for managing and securing data.

Secure Cloud

The use of biometric security systems in cloud computing is progressively gaining ground in terms of usage. In general, storage in the cloud comes with a separation of responsibilities when it comes to maintenance of the IT systems. The cloud provider such as Amazon Web Services, Microsoft Azure or Google Cloud, is responsible for maintaining the underlying hardware, software and security and the entire cloud provider's organization is aimed at reaching the highest levels of security and performance in this. No single organization can reach the same amount of security and quality offered by these providers. The client organization, such as an airport or its supplier, is solely responsible for the configuration of the storage of the data, and the trouble of hardware, software and network maintenance is taken out of its hands.

Biometric security systems have the potential to take cloud computing to the next level as they guarantee an extremely high level of security and ensure that the rendered services are accessible only to a legal or authorized user and no one else.

There is a clear distinction between cloud service providers and the customer. Breaches of data in the cloud are not typically breaches of the underlying cloud provider's infrastructure. To make a cloud secure it is vitally important that responsibility is shared. The customer is responsible for securing how he/she uses the cloud services, including properly configuring identity and access management, storage and

computation settings, threat analysis and defense, along with the security of the application and data processed and stored in the cloud.

Cybersecurity for centralized server solutions and cloud-based services, is the protection of IT connected systems and protecting them from cyber threats.

Mobile Device e.g., Smartphone

Biometric data can also be stored on an end user's device. This is most common on smartphones that use touch ID fingerprint sensors. On-device storage can be used to store biometric data through a chip that holds the data separately on the device's network. When storing the data on the authentication device itself, the organization implementing the biometric verification process does not have control over it nor the ability to copy the data. They are also not liable for the theft of large databases with personal data.

Distributed Databases or Distributed Ledgers (Blockchain)

Public blockchains are a collaborative creation, with their goal being to create a world that is completely decentralized, and where the ownership of digital assets is always protected and transferable. Blockchain can concurrently achieve high security, decentralization and scalability. The core value of blockchain technology is not to provide rudimentary data services (like the decentralized database), but to build a new ecosystem of digitized data assets and automated trust services. The global blockchain updates its state autonomously, and data is traceable to its source. Data contained in a blockchain is immutable, and therefore supports the privacy concerns when personal data needs to be stored.

In contrast, a distributed database is centrally managed by a service provider. The goal is to create a logical center, that can provide efficient, low-cost services with great scalability.

The core value of distributed database is to supply data storage, and access services to business systems, focusing on the analysis and retrieval processes.

Biometric Touchpoint Interactions

Travelers are required at various points of their journey to interact with various customer facing biometric solutions. Some of these are already commonplace in many countries. They comprise the following.

- e-Gate
- Camera-on-a-stick
- Kiosk
- Walk through gate or tunnel

There is a major debate on the optimal technology types to use for flow control. e-Gates are the prevailing methodology used outside the United States to control flows. Several U.S. airlines and CBP on the other hand prefer a "camera-on-a-stick" method. Both require staff intervention to some extent: dealing with exceptions when an e-Gate does not open, as well as monitoring a successful passage through a visual/audible signal from the camera-on-a-stick model. In this section we describe some system architecture implications to match the concept of operations of these different solutions.

e-Gates

Automated e-Gates at checkpoints with the capability to use biometric technologies for the verification of identity or granting permission for entry by scanning a biometric (credential), are by now common solutions at airports. With an e-Passport, the e-Gate can be used worldwide at border control checkpoints, for customs, immigration and emigration, allowing for automated self-service border crossing.

The e-Gate might use the data stored in the chip in biometric passports to verify the user's identity. Travelers undergo biometric verification using face, fingerprint, iris recognition or a combination of modalities. In some locations systems such as Global Entry® in North America are used for verification. Functionality can be extended so that the e-Gate can authenticate the "signature" on the e-Passport against the origin country certificates, read the biometric image, and match it with the live person in front of the barrier (1:1 matching).

After identification, the person's details can be digitally vetted according to the national border control checks and procedures. Typically, e-Gate providing biometric identification and verification will provide a two-gate option allowing the traveler to cross a border with no ability to return unless following and meeting the entry or exit criteria of the country.

Automated e-Gates used for boarding usually has a single gate system where a traveler presents a boarding pass to board a flight. This type of e-Gate is controlled by the team responsible for managing boarding issues and incorrect boarding procedures.

After positive identification and authentication there is no need to store the passenger's data in a database. Since the data is stored on the passport and not in a database, the passport bearer is the keeper of its own data.

The advantage of e-Gate is the ability to manage flows with a device that physically obstructs passage if there is no biometric match to confirm identity. In other words, e-Gate serve as a mechanism similar to the payment system gates used for mass-transit. The disadvantage is that e-Gates are bulky and require more planning around wiring and data as well as lifecycle wear-and-tear of gates.

"Camera-on-a-stick" – "Gate"- less Interaction Point

The point of interaction is where biometric identification or identity verification can take place, without the passenger needing to go through an automated gate. These points are in many instances currently manned by ground agents, or airline representatives, but still offer the opportunity to increase security performance and decrease processing times. Many different applications can be designed to be incorporated in a "totem", the most common being the "camera-on-a-stick" which refers to the camera being used for facial recognition.

The advantage of CBP and some airlines' views of camera-on-a-stick is that the overall capital cost is low, and the biometric processes are integrated within other customer interaction. For CBP officers, it is the questioning of passengers. For airline agents it is a face-to-face customer service driver to help with additional services. There are some clear disadvantages: a camera-on-a-stick model is less bulky physically but negates the full passenger self-service potential. In other words, to truly get hundreds of passengers through without the need for staff time is much harder if the concept of operations is built on front-facing passenger interaction. Moreover, with social distancing measures and reduction of face-to-face time for customer service, there is also a realignment of how to use methodologies that do not require a gate.

A hybrid model may be developed that uses a wayfinding approach to direct passengers to "Point A" if successful and "Point B" if a biometric match has not been achieved. In so doing, the bunching up of people is minimized, and there are methodologies to ensure that individuals are not routed to the wrong location.

Kiosk

Passenger check-in via mobile phones, airline desks or kiosks are the typical choices available at airports. Kiosks provide self-service devices that are simple to use and convenient, making it possible for passengers to check in any time on the day of departure.

The next generation of kiosks is being tested by various airports and airlines which include sensors to help with touchless check-in via infrared. Robotic kiosks which can move to check-in areas where congestion is being experienced.

Contactless check-in using a smart device remotely and at the airport may be used to print boarding passes (if necessary) and baggage tags at kiosks.

Check-in using a smart device or website may be used to obtain a boarding pass and provide personal details including passport information. There is an increased focus from airports and airlines to enhance existing processes with touchless options using passenger smart devices, and possibly the introduction of biometrics through smartphone cameras. Alternatively using Apple iOS or Android based on-device biometrics to confirm identity is a methodology of SSI that can limit the amount of transmission of information, but still validate individual identity.

Walk Through Gate/Tunnel

This technology is being tested in various airports, allowing passengers after enrollment to clear immigration in seconds by walking through a defined path (touchless tunnel). Iris biometric technology is utilized to authenticate each passenger, ensuring queuing is eliminated.

IATA OneID or Seamless Flow

The IATA OneID concept envisions an end-to-end travel journey where the passenger enrolls with his/her biometric details prior to each journey and is then able to pass several processing steps before and at the airport by simply showing his/her face, e.g., check in, bag drop, security, border control, boarding or even airline lounge entry and duty-free purchases. The concept aims to include both the departure and arrival processes, at both the destination and origin airport. In addition to smooth processing of the passenger, the system can also recognize and differentiate passenger personas and provide services tailored to the persona on their journey (for example, for priority or disabled passengers).

IATA has been working on this initiative for fifteen years, with the aspiration that its solution can be adopted initially in markets struggling with capacity. The rollout of “OneID” has seen several pilot projects, however, a wider adoption will take time. A more detailed description of the complete system can be found in Appendix M.

IT Architecture Models

Introduction to 5 Models

KEY TAKEAWAY

Five different IT architecture models differ predominantly in terms of: (1) who “owns” the biometric data; (2) which entity is responsible for the verification of the passengers identity; and (3) how long is biometric data is stored.

In this chapter, we identify and compare five different models focusing on the enrollment, verification, data facilitation and authentication of the various credentials allowing the categorization of the case studies of biometric implementations as seen in Chapter 2. Literature often references at least two pillars: a per-trip model and a per-life model, where the differences are obvious. In the first, the system architecture aims not to retain information such as biometric data much longer than necessary, past the duration of one competed “trip”. In the latter, enrollment or the retention of information is for a much longer period, in this case for “life”. A distinction added to these two main models, also due to trends in society focusing more and more on privacy protection, data storage and the governance of the system, is whether the system architecture

facilitates biometric data to be governed by either the passengers themselves, by a third-party or by an authoritative party such as a local or national government.

This results in the following five models which are reviewed in more detail in subsequent sections:

1. Identity as a Service – Centralized – Government/authority model
2. Identity as a Service – Centralized – Third-party model (not bound by national/state borders)
3. Trip model- Semi-Federalized model
4. Life model - Federalized Model
5. Life model – Federalized model with SSI

Table 5-13: Comparison of models

	Model 1	Model 2	Model 3	Model 4	Model 5
	Gov/Authority	Third-Party	Per Trip	Per Life Federalized	Per Life SSI
Example	e-Passport*	CLEAR®	Happy Flow	Digi Yatra	DTC on blockchain
Enrollment					
How to enroll	Every 5/10 years, at a Government location outside the airport.	Once, at airport.	Every trip, prior to check-in at or outside airport.	Once at Government location, outside airport.	Once, on a personal device, verified by a government agency.
Ability to opt-out.	Yes	Yes	Yes	Yes	Yes
Data (biometrics/biographic) used.	Biographic, facial, fingerprint.	Biographic, facial, (iris).	Biographic, facial, flight information.	Biographic, facial (iris).	Biographic, facial.
Type of hardware used.	Government enrollment office or online.	Kiosk.	Kiosk or on a personal device.	Government enrollment office or at airport kiosk.	On a personal device.
Type of software and architecture required.	Government cloud platform.	Cloud based orchestration platform.	Cloud based orchestration platform.	Government cloud platform.	Distributed ledger.
Enrollment process.	Apply or renew before expiration.	Online plus Clear enrollment center or just Clear enrollment center.	Check-in kiosk or counter.	Register with central system, validate ID at start of first trip at registration kiosk.	Download App and upload information.
Retention period.	Period of validity.	Life of the credential, until one's membership is termination.	Length of a trip, or limited number of hours after departure.	Per life.	Per life.

	Model 1	Model 2	Model 3	Model 4	Model 5
Integration of reservation data.	Separate.	Integrated.	Separate.	Integrated.	Integrated.
(Biometric) Verification of identity					
Where in biometric journey is it required.	Check-in, bag drop, security, border, e-Gate.	Security/border/boarding.	Check-in, bag drop, security, border, e-Gate.	Check-in, bag drop, security, border, e-Gate.	Check-in, bag drop, security, border, e-Gate.
Verifying party.	Airline, airport, government.	Third-party, government.	Airline, airport, government.	Airline, airport, government.	Airline, airport, government.
Data (biometrics/biographic) used.	Facial.	Facial (iris).	Facial.	Facial (iris).	Facial.
Hardware used.	Kiosk/e-Gate.	Kiosk/e-Gate.	Kiosk/e-Gate.	Kiosk/e-Gate.	Kiosk/e-Gate.
Software required.	Facial recognition on orchestration platform.	Facial recognition on cloud platform.	Facial recognition on local template database.	Facial recognition on cloud platform.	Facial recognition on orchestration platform, mobile DTC application.
Method of verification.	Picture of face (live) matched to stored biometric on the physical credential.	Picture of face (live) encrypted and sent as photo/template to third-party for matching with on-file biometric.	Picture of face (live) matched to stored biometric on personal device or temporarily on airport system.	Picture of face (live) encrypted and sent as photo/template to government for matching with on-file biometric.	Picture of face (live) matched to biometric on personal device (verified by Issuer of digital credential).
Data facilitation					
Type of platform.	Local or cloud-based orchestration platform.	Private cloud-based orchestration platform.	Local template database and orchestration platform.	Cloud based orchestration platform.	Orchestration platform, distributed ledger and mobile DTC app.
Storage of data at location.	Government, airline and airport servers (temporary).	Private, airline and airport servers.	Temporary: airline, airport servers, record of immigration, emigration may be kept by authorities.	Government server.	Blockchain, records of immigration, emigration may be kept by authorities. All stored data is immutable.
Connectivity through.	API^.	Platform.	API^.	API^.	Ledger.

	Model 1	Model 2	Model 3	Model 4	Model 5
Data and privacy protection.	Laws governing government data retention, and protection.	Laws governing commercial companies' data retention, use and protection.	Privacy by Design integrated.	Laws governing government data retention, and protection.	Privacy by Design integrated.
Authentication of credential					
When in journey?	Check-in, bag drop, security, border, e-Gate.	Security/ border/ Boarding.	Check-in, bag drop, security, border, e-Gate.	Check-in, bag drop, security, border, e-Gate.	Check-in, bag drop, security, border, e-Gate.
Authenticating party.	Government.	Third party.	Airline, airport, government.	Government.	Airline, airport, government.
Data (biometrics/bio graphic) used.	e-Passport, facial.	e-Passport, facial (iris).	e-Passport, facial.	e-Passport, facial (iris), digital credential.	Digital credential (on mobile device), facial.
Hardware used?	Kiosk/e-Gate.	Kiosk/e-Gate.	Kiosk/e-Gate.	Kiosk/e-Gate.	Kiosk/e-Gate.
Software required.	Orchestration platform connecting to government authentication service.	Orchestration platform connecting to government authentication service.	Orchestration platform connecting to government authentication service.	Orchestration platform connecting to government authentication service.	Orchestration platform connecting to blockchain API^.
Method of authentication.	Scan of e-Passport for check of authenticity of certificate of issuing authority.	Third-party checks authenticity of identity documentation upon registration.	Authenticity of identity documentation (e-Passport) checked upon enrollment.	Government is issuer of digital identity, checks the authenticity of identity upon enrollment.	Identity documentation authenticity checked upon enrollment, stored on Blockchain as verifiable claim.

Notes: *specific requirements made differ slightly per country.
^ Application Programming Interface.

Model 1: Identity as a Service - Centralized - Government or Authority Model

The "Government-Driven" model is a centralized approach to passenger and data facilitation. The government establishes and verifies the traveler's identity and serves as the identity management service provider to other stakeholders within the airport ecosystem.

This model does not depend on formal traveler enrollment or adoption, as the government uses centralized databases of pre-verified "own nationals" and foreigner biometrics (facial) to authenticate a traveler. No further data is collected, and no booking information is integrated to create a digital identity.

The core platform is a cloud-based biometric matching service. The government can extend this to private sector providers as an Identity as a Service (IDaaS), which provides a scalable, secure and seamless solution that easily integrates with providers' systems through web-based Application Programming Interface (API) connections.

Upon arrival at any journey touchpoint, a traveler's image is captured by facial recognition technology (e.g., e-Gate, stand-alone facial recognition cameras) and sent to the government verification system for authentication, returning a match result to the travel provider.

The "Government-Driven" model demonstrates applicability and implementation success at touchpoints across the airport ecosystem. Any traveler providing consent to participate experiences a streamlined journey without having to enroll in advance. The core challenge with this model is legislative restrictions that prevent the extension of IDaaS beyond its current mandated realm. As a result, there may be limitations when attempting to integrate car rental services and hotels into a model that was developed and approved for use only in the airport/governmental ecosystem.

Example: Border Control Authorities

Various border control authorities across the world use an e-Gate or kiosk that support biometric microchip passports:

- France – Charles Du Gaulle Airport allows citizens from the European Economic Area (EEA), Andorra, Monaco, San Marino & Switzerland to use the PARAFE gates. These gates can only be used by citizens aged 18 or over holding valid biometric passports.
- United Kingdom – e-Gate are in place at 15 air and rail ports across the UK. Users must be 12 and over, and a British citizen or a national of the following countries, EU, Australia, Canada, Iceland, Japan, Liechtenstein, New Zealand, Norway, Singapore, South Korea, Switzerland or the United States.
- The Netherlands – e-Gate can be used if you are 16 years or older and hold a valid EU passport.
- United States – CBP is in the midst of rolling out "Simplified Arrival" to speed clearance for international arrivals. Simplified Arrival uses facial biometrics to automate the manual document checks and provide travelers with a touchless process.

Model 2: Identity as a Service - Centralized - Third-Party Model (not Bound by National or State Borders)

The European Commission is implementing a central Biometric Matching System (BMS) that will serve the Biometric Identity requirements of multiple applications that are essential to European Security. This system is ground-breaking in terms of scale, transactional support and strategic approach, offering many valuable lessons in the use and adoption of biometric identity capabilities. The system is currently in development and expected to be live during 2022. The system aims to instantiate a new Entry/Exit System (EES), creating a unified information system for recording data on the entry and exit movements of short-stay third country nationals crossing the external borders of the EU.

The key body of the EES is EU-LISA, the European agency for the operational management of large-scale IT systems, which is headquartered in Tallinn, with an operational site in Strasbourg and a back-up site in St Johann Im Pongau (Austria). The agency is responsible for the following four tasks:

- Development of the central system
- Implementation of a National Uniform Interface in each Member State
- Secure communication between EES and Visitor Information System, or VIS, central systems
- Communication infrastructure between the central system and National Uniform Interface.
- Responsibility by each Member State for the organization, management, operation and maintenance of its existing national border infrastructure and its connection to the EES.

The EES will be a centralized system through which the Member States cooperate, hence the need for a common architecture and operating rules. Secure Internet access to a web service hosted by EU-LISA will allow third country nationals to check their remaining authorized length of stay at any time. Carriers such as airlines will also be able to use this function to check whether their passengers are authorized to enter the EU.

Example: Traveler Verification Service

A digital ID verification service that is provided in the United States is the TVS. This service, which is provided by CBP, is based on the concept of IDaaS. CBP utilizes a biometric matching service: the system compares a new photo taken at the time of departure with a DHS stored subset of a larger DOS dataset (based on the flight manifest), which include images from photographs taken by CBP during the entry inspection, photographs from U.S. passports, U.S. visas and other travel documents, as well as photographs from previous DHS encounters.

TVS can be applied at all entry/exit locations in the United States – by air as well as by sea. For air travel, instead of the airline conducting a manual passport verification and a registration of the boarding card of the passenger in the flight manifest, the process can be automated by means of facial biometrics.

TVS can be applied at security, check in, bag drop or the boarding gate, using facial recognition software, a live captured image is matched with the person's identity credentials that are stored in the TVS database. Upon a match the system returns the biographic data of the person together with a unique identifier which the airline can use to link the passenger to its DCS, and access or passage through the touchpoint.

Model 3: Per Trip – Semi-Federated Model

The "Per Trip" model is a semi-federated approach to traveler and data facilitation throughout the traveler journey. Unlike the "Government-Driven" model, the traveler has the choice to opt-in to participate in "Per Trip" travel experiences at the time of enrollment.

The enrollment process for "Per Trip" travel experiences typically begin upon arrival at the airport. Using a biometric check-in kiosk, the passenger verifies his/her identity with his/her e-Passport, biographic information, and facial image (biometric token). The data orchestration platform creates a digital identity that lasts only for the duration of the journey.

In this model, data is stored, managed, and facilitated by an orchestration platform, which all stakeholders trust to supply verified traveler data. Connections between the orchestration platform and travel provider or government agency systems normally only require API integrations. These platforms are built to adhere to "Privacy by Design" principles and securely store and send encrypted traveler data to stakeholders on a "need to know" and "authorized to know" basis.

A traveler is authenticated upon arrival at a touchpoint, with facial recognition technology capturing the traveler's image and transmitting it to the orchestration platform, to then receive an authentication status as well as any data required for the touchpoint stakeholder to finish processing the traveler.

The "Per Trip" model has emerged as one of the most prevalent models tested and implemented worldwide. This model is widely accessible to a broad set of travelers, including occasional travelers and non-nationals of that country. It is also relatively easy to implement from a technical perspective and easy to use from a customer experience perspective. A key challenge for designing an end-to-end model will be extrapolation beyond the airport environment as well as ensuring disparate parts of the journey (e.g., connecting flight at another airport) are included without needing to re-enroll.

Example: Happy Flow

The model is based on collaboration among public and private stakeholders, which includes the Government of Aruba, the Aruba Airport Authority, the Netherlands, KLM, and the Schiphol Group. Over

the past four years, this group has piloted a streamlined, user-friendly, end-to-end experience at Aruba International Airport.

Enrollment after opting in creates a single biometric token which is only kept for 24 hours. When created, the passengers e-Passport is used for authentication, after which the holder's identity is verified at each touchpoint using facial recognition.

Model 4: Per Life Enrollment – Federated model

The "Per Life" model is a federated approach to traveler and data facilitation throughout the traveler's journey. The traveler has full discretion over how much, to whom and at what point his or her data is shared. The traveler also keeps data integrity by storing his or her digital identity on a mobile device.

The "Per Life" travel experience typically begins with the creation of a digital identity on a traveler's mobile device using a digital identity management app. This initial enrollment allows the traveler to upload and verify core pieces of his or her identity (e.g., passport biographic information, facial image) using the app's built-in e-Verification capabilities as well as verification by government. Upon completion, the digital identity resides on the traveler's mobile device "for life". The traveler may add as much additional information as desired and can perform one-time verification of this information with relevant, trusted stakeholders (which may be but are not required to be government agencies). Finally, the traveler easily integrates bookings into digital identity to allow for seamless data management and sharing.

Pre-journey, a traveler "pushes" minimum required data to relevant travel providers or government officials from a mobile device. Data facilitation is managed by distributed ledger technology and cryptography, ensuring the secure transfer of data. Upon receiving traveler data, stakeholders can perform a host of activities: government officials can perform risk-based assessments to streamline security processes and travel providers can leverage shared data to enhance the traveler experience. Upon touchpoint arrival, a traveler is authenticated via facial recognition technology, which captures the traveler's image, authenticates it against received data, and receives an authentication status.

The "Per Life" model offers numerous opportunities for secure, seamless travel experiences across a multitude of use cases. The key challenge for end-to-end model consideration will be ensuring stakeholder acceptance and trust in this level of federated digital identity.

Example: Digi Yatra

This platform is an industry led initiative overseen by the Indian Government which utilizes the link to the Aadhaar system (12-digit unique identity number of all Indian citizens) in partnership with airlines and other ecosystem players during the booking process facilitating, faster airport entry, an automated check-in without the need for any paper-based interventions.

Dubai International Airport has recently introduced a pilot where enrolled travelers can walk through a biometric tunnel without stopping due to the advanced biometric security solutions. The biometric tunnel uses iris and facial biometrics for identification and verification.

Once the traveler has successfully cleared the tunnel, the traveler can receive real time notifications about congestion, delays as well as greater visibility on the next step of journey which includes navigation though the airport using a smart phone, or via an interactive kiosk and various augmented reality applications. Returning passengers can receive alerts about his/her luggage and its arrival on the baggage belt, submit baggage claims, and provide customer feedback.

Model 5: Life Model – Federalized Model with SSI

An SSI is "owned" by the individual. As owner, the individual has access to and can refer to and share components of this identity at their discretion. While certain components of the identity are set up by issuing authorities (i.e., passport number, bank details), individuals must consent to the sharing of their identities

and any related data. This is achieved by individuals securely storing their own identity data on their own personal devices and providing it efficiently to those who need to confirm it, without relying on a central repository of identity data.

Example: Known Traveller Digital Identity

WEF has published a white paper describing in detail its proposed biometrics-backed paperless international travel concept, the KTDI, a limited pilot project involving travel between Canada and the Netherlands.

A KTDI would be an international traveler's digital profile, one that is detailed, secure and shareable (at a traveler's discretion). The new profile model would be decentralized and facilitated by blockchain processes, biometrics, mobile devices, and cryptography.

The KTDI concept is a public-private endeavor which the pilot consortium launched midway through 2019. The pilot is being run by the WEF, government agencies of Canada and the Netherlands, KLM Royal Dutch Airlines, Air Canada, Amsterdam Airport Schiphol, the Greater Toronto Airport Authority, Aéroports de Montréal, and Accenture Plc.

An open source blockchain Hyperledger Indy has been chosen as the decentralized identity platform. Hyperledger is a global enterprise blockchain project that offers the necessary framework, standards, guidelines, and tools, to build open source blockchains and related applications for use across various industries. For the Hyperledger platform, a person's digital identity, authenticated by a national government, would be linked to the person through biometrics. The identity would be encrypted and stored on the traveler's phone. The KTDI application would keep an ongoing list of attestations, beginning with the government authentication, and continuing with a running travel history that includes border crossings and transactions with trusted vendors. Information shared by the traveler is verified by checking trusted databases.

Evaluation of Architecture Models

The table below provides an evaluation of the five architectural models, their differentiators, benefits, and challenges. Each model needs to be carefully evaluated based on one's circumstances, as it may be more appropriate than another. Some key considerations are the types of air services offered, (domestic, regional, or international) or a combination of all. Other considerations include the airport type, its size, and types of airlines providing services.

Table 5-14: Evaluation of 5 Architecture Models

Metric	Notes:	Model 1	Model 2	Model 3	Model 4	Model 5
		Gov/ Authority.	Third-Party.	Per Trip.	Per Life Federalized.	Per Life SSI.
	Example:	e-Passport.	CLEAR®	Happy Flow.	Digi Yatra.	DTC on blockchain.
Enrollment						
Pre-journey enrollment is possible.		No	Yes	Yes	Yes	Yes
Accessibility for all passengers.	Passengers with reduced mobility, families with	Low	Low	Medium	High	Medium

Metric	Notes:	Model 1	Model 2	Model 3	Model 4	Model 5
	children, the elderly, requirement for a passport?					
Speed of enrollment.		Low	High	High	Medium	Medium
Integration of booking data is possible.		No	Yes	Yes	Yes	Yes
Authentication/Verification						
Level of acceptance (quality of authentication).	Authentication of an identity, is the identity (digital) credential authentic and accepted by government/ country/ authority.	High	Medium	Low	High	High
Quality of verification (confluence of verifiers).	In case of facial recognition.	High	High	Low	High	High
Potential for U.S. preclearance	U.S. preclearance: some models allow for data sharing that is required by United States.	Yes	if third-party is a trusted partner of CBP.	No	Yes	Yes
Government acceptance (likelihood).	check Oliver Wyman rep.	High	Low	Medium	Low	Low
Data & Privacy						
Traveler ownership of data, ID.	Does the traveler own the data?	No	No	?	No	Yes
Privacy protection.		Low	Low	High	Medium	High
Data security (of the platform) from external manipulation.	Difference between distributed ledger vs. central database.	Medium	Medium	Medium	Medium	High
Operational Efficiencies						
Time savings (Speed at checkpoints).		Medium	Medium	High	High	Medium

Metric	Notes:	Model 1	Model 2	Model 3	Model 4	Model 5
Customer experience improvement.	Assuming a faster, relaxed journey is delivered, disregarding preference for data ownership (considered in a different metric).	Medium	High	Low	High	High
Space and Resource savings.	Related to chapter 4, task 3.	Low	Medium	Medium	High	High
Applicability outside airport system.	Outside the passenger journey inside the airport (ride share/taxi).	No	Yes	No	Yes	Yes
Other considerations						
Availability of technology (now).		Yes	Yes	Yes	Pilot	Pilot
Sharing data with stakeholders.	Airport, airline, government authorities.	Yes	Yes	Yes	Yes	No
Sharing data with third parties (anonymized).	Retail, food & beverage, hotels, etc.	Yes	If third-party shares with airport.	Yes	Yes	No
Operational big data applications (passenger flow tracking, prediction).		Medium	If third-party shares with airport.	High	High	High

Stakeholder Challenges: Interoperability, Scalability, and Privacy Protection

There are multiple challenges to the design of an IT architecture and this often merits careful collaboration between the airport, airline, government and the stakeholders to achieve the desired interoperability. With airports developing faster each year, IT architectures must be increasingly capable and scalable to incorporate new technology needs of airports. Many are also dependent on the local or national laws, especially when it comes to the protection of privacy and biometric data. On top of that, the designer will want to implement best practices, as well as make the architecture secure and user friendly. With more stakeholders, this will become increasingly complex.

KEY TAKEAWAY

The IT architecture design faces a larger challenge with more stakeholders, as interoperability and scalability become more complex. With stakeholders in multiple countries, their respective privacy laws also impact the design.

On the other hand, although typically 2-3 years behind the technology development, global standards aim to create common technical specifications allowing technologies to interact smoothly, while abiding to multiple nations' (and state) laws, being software-, hardware-, and vendor-agnostic. More specific to biometrics, the ICAO DTC development is an example of an emerging global standard and is explained at the end of this section.

Single-Party Biometric Solution

In this scenario, every person/airport/airline/government has designed a system for themselves, which applies to very local conditions. This is a technology solution which can be implemented quicker, easier and with less capital investment than the multi-party biometric technology solution. A few models exist and a broader range of possibilities exists for choosing infrastructure components, as these generally do not have to be agreed upon by multiple stakeholders. This option also has the advantage of offering more opportunities for a stricter set of guidelines and allows for more transparency and broader privacy protection guidelines.

Around the world, governments, airlines and airports have rolled out or are testing passenger processing systems based on, for example, biometric recognition systems. Many of those platforms and systems are developed based on national law, international border agreements, stakeholder interests and limitations of existing facilities, which leads to a varied implementation of solutions.

Stakeholders focus on individual interests and not the interests of others and thus data sharing across borders and to other stakeholders is not realized.

Multi-Party Biometric Solution

Multi-party biometric solutions comprised of all other systems using biometric technology, aim to allow functionality across multiple stakeholders, parties, and countries or even aim to allow global implementation, and are to a certain extent interoperable and scalable. Technology solutions are typically much more complex in design to allow for interoperability. Ideally, infrastructure components are made compatible and not vendor specific, although operational requirements need to be specified to guarantee functionality across different infrastructures. Technology guidelines are the greatest hurdle, with many stakeholders having to agree on issues like privacy protection, data sharing, data protection, data retention and more.

Stakeholders

As highlighted above, the direction taken for a single-party or multi-party biometric solution affects the number of stakeholders at the table. The list below presents an overview of the main stakeholder (groups), which will each have a different effect on addressing the challenges of interoperability, scalability and privacy protection.

- Border control authority (CBP) – responsible for carrying out customs, immigration and emigration procedures on airport premises. CBP has multiple biometric-ready implementations linked to the use of TVS.
- Security screening (TSA) - Offers passenger screening at the airport as part of the layered approach to security to get you safely to your destination. TSA's screening procedures are: intended to prevent prohibited items and other threats to transportation security from entering the sterile area of the airport and being introduced onto the aircraft; and are developed in response to information on threats to transportation security; providing expertise and specialist processes to protect passengers, staff, aircraft, and airport property from accidental/malicious harm, crime, terrorism and other threats. Aviation security is a combination of human and material resources to safeguard

civil aviation against unlawful interference. Unlawful interference could be acts of terrorism, sabotage, threat to life and property, communication of a false threat, bombing, etc.

- Airlines – responsible for the verification of valid travel documents of passengers for entry to the destination country. They are concerned about delivering an optimum passenger experience and therefore a stakeholder in the entire passenger journey – at all touchpoints.
- Airport (operator) – responsible for verifying that passengers carry a valid boarding pass upon entering the security checkpoint, and facilitates the passenger process in its terminal. In addition, the airports have a special interest in improved efficiencies in space usage and improving the passenger experience at its airport.
- Technology providers – responsible for the development, delivery and installation of the biometric systems applied at the airports.
- IATA – as representative of the airlines and initiator of the OneID concept, responsible for guidance and facilitation of the biometric passenger processing developments. IATA advocates striving for efficiencies for all airlines and their passengers.
- ACI – as a representative of the airport industry responsible for guidance and facilitation of biometric passenger processing developments. ACI strives for efficiencies in the entire industry;
- ICAO - the collective body of member state representatives with the role of setting global aviation standards and rules to protect and safeguard. ICAO strives for efficiencies in the entire industry, and notably resulting in, for example, Doc 9303. ICAO also has the Facilitation Panel established in 1995 that plays a critical role in the accomplishment of priorities and helps to ensure that Annex 9 is kept current.
- The Passenger – requiring a seamless travel journey without the need to continuously present the same documents at each point in the journey. The passenger seeks travel safety and security and an easier process to facilitate entry to a country (visa, supporting documentation, validation).

ICAO Digital Travel Credential

A global standard that has been under development under ICAO, is the Digital Travel Credential, or DTC. Its policy paper “Guiding Core Principles for the Development of DTC version 4.4”, was published in October 2020, and sets out a clear set of principles that lay the foundation for a digital credential standard, which would also apply to biometric credentials stored on tokens, on a mobile device, or in a database.

The policy paper relates much of the technical specifications to current standards for e-Passports, an example of an Electronic Machine-Readable Travel Document (eMRTD). Following the current security of the eMRTD which results the verification and consistency of the data between the physical and electronic document, the intent is to validate to the CTD same level of the eMRTD process. More on the DTC specifications can be found in Appendix N. For airport management considering implementing biometric technologies and solutions, it is important to track the DTC standard developments, and make decisions that guarantee the IT architecture is able to incorporate or adapt to such emerging global standards.

Lessons Learned

Large facilities such as an airport have existing IT installations, which are not necessarily designed to support biometrics due to their current architecture, ability to scale, as well as meeting privacy protection requirements. There are key aspects which need to be considered to support biometrics such as network cabling, managing processing loads, balancing network traffic and applying network standards that address communication between a large number of devices connected to the network. If these are not addressed in your planning, network bottlenecks can lead to passengers waiting an unusually long time for a response from the system, leading to the creation of unnecessary queuing.

KEY TAKEAWAY

Supporting your biometric solution and taking into consideration your existing architecture and systems ensures the efficient use of existing and future investments and best practices. Learning from prior completed biometric implementations, much risk can be prevented going forward.

Cabling, Local Area Network

The main artery to the IT network in a large facility such as an airport is the cabling, which will link all devices connected to the network. This needs to be maintained and managed at all times. Existing IT installations are not necessarily designed to support biometric requirements, due to their current design and use. Your network must have the ability to scale, as well as meet privacy protection requirements. Before starting on your biometric journey, one needs to evaluate your present network architecture not only to ensure the best use of existing assets but more importantly to identify limitations and the required best practices to provide you with the relevant biometrics foundation.

Network Processing Loads and Network Switching

This refers to the concept of ensuring that the network is efficiently designed, properly balanced and that no item in the network is doing all the work which leads to reduced performance. All the devices which are connected are sharing the required “workloads” to make sure that there are no delays, bottlenecks or slow response times.

A vital part of a biometric network design is what is known as “Data Packet Switching” (transfer of small pieces of data across various networks). For example, when at least three or more biometric devices are connected, or when a biometric device is connected to three or more central servers, different network routes may be used to reach the destination biometric device.

Network Protocols

A network protocol can be defined as the format and the order of messages exchanged between two or more communicating entities (e.g., computers), as well as the actions taken on the transmission and/or receipt of a message, or another event.

Biometric devices connected with each other must use certain network protocols to transmit their Data Packets back and forth.

A biometric enrollment kiosk includes in most cases a passport reader to verify the person’s identity based on the image in the passport. Such a kiosk can also have full Common Use Self Service (CUSS) functionality to guide a passenger through the airline’s boarding process and obtain a boarding card for the passenger in the same step.

Facial Recognition: Liveness Detection

Face recognition technology uses a biometric reference database to compare an individual's identity with a verified credential – the biometric template. Facial recognition software performs a series of tasks before it stores a person's biometric template, and at a later moment in time when an image is captured at a biometric touchpoint conducts a similar series of tasks to perform the facial recognition operation.

An important element to the first and second operation that should be performed in parallel is liveness detection. This detects people spoofing or bypassing the system by showing photos, videos, masks, or artifacts to the camera. There are many different techniques available to check the liveness of the person with variable accuracy and response time. Which technique is needed may depend on the scale of the threat that can be expected and the actual location and layout of the touchpoint? Supervision of the touchpoint during operating hours may deter certain threats.

Facial Recognition: Lighting

Facial biometrics supplies an easy-to-use method of verifying an individual's identity. However, the accuracy of the verification is significantly less than other biometric methods. One of the shortcomings is that many facial biometric algorithms are overly sensitive to even minor changes in lighting and thus requires standardized lighting.

This can prove to be challenging as facial biometric kiosks are incorporated into existing buildings. Modulated light sources synchronized with video cameras can be used to supply images that are lighting independent for these situations. The amount of modulated light needed is minimally obtrusive. The lighting arrangement should be appropriate for the application. One should also remember that good lighting can suppress the background in closed and open spaces.

Facial Recognition: Face Capturing Hardware

The equipment that is used to perform the facial capturing operation may be less susceptible to variations in performance, but the hardware and physical layout of a touchpoint can influence the match results. With a high-quality image and the right composition, the face match system will be more accurate. First, the quality of the camera can influence the performance (light sensitivity, number of pixels, and encoding type).

In addition, the enrollment station and verification touchpoint can be designed in such a way that every person is lined up in front of the camera in the same way – leading to the same composition. And accuracy can be further improved by ensuring that the face of a person receives enough and equal lighting conditions at every touchpoint. Decent quality images will require less processing by the facial recognition software for detection and normalization, which in turn will lead to better quality biometric templates. Equal conditions for images taken at enrollment stations and images at verification touchpoint will lead to more reliable match results.

The following features can be provided at biometric touchpoints to improve the quality of face capturing:

- Stickers of feet on the ground that show the position for the passenger.
- Camera on a moveable stick – manually pointed at the target person to improve the composition.
- Speed gate with barriers to position a person in front of a camera.
- Camera that can move position vertically.
- Dynamic indicator or an avatar to attract attention.
- Illumination of the face, supplying more lighting.

Facial Recognition: Accuracy

With the application of facial recognition systems in aviation it is important that all stakeholders are aware how accurate these systems are. Passengers should not be allowed passage at a border checkpoint,

or enter a plane, due to the facial recognition not being accurate enough (false positive match). On the contrary, the algorithm should not be too strict causing a high number of falsely rejected passengers (false negatives). Finally, the time to render the facial recognition and matching must not take too long. A balance between accuracy and speed of computation needs to exist, as well as the need to abide by national/State and local laws and security and facilitation. A more detailed piece is included in Appendix O.

Technology Will Fail and an Opt-out Will Need to be Ever Present.

Technology has revolutionized consumer experiences for the past 30 years, however, as airlines and the infrastructure that serve them become increasingly reliant on technology, vulnerabilities become clearer and minor technical failures can cause catastrophic outcomes.

Insufficient investment in technology infrastructure over the past decade can result in many technical outages that can cripple airport and airlines operations for days on end. As exposure to technology increases, so too do the risks of an IT failure. Measures can be introduced to try to limit the risk, but it is obvious air travel of the future will be prone to IT failure risks. Using legacy systems which are already overstretched will increase the likelihood of an IT failure.

It is paramount to plan for the inevitable as the biggest risk areas are the loss of landside or airside activity, and loss of baggage systems that work between landside and airside, leading to major impacts on an airport and airlines, and its passengers. One needs to focus on the development of contingency plans with a recognized structure and model to address "what happens when things go wrong."

The very nature of IT; seamlessly working in the background, means it is often not obvious that a problem is just around the corner. The next best thing to preventing it is being ready when it happens.

Findings

Implementing Biometrics

Biometric technology takes the role and benefits of passenger automation in airports a significant step forward. With the innovations that are taking place now and, in the future, passengers will be able to move through the airport with limited human contact using technology to create their own seamless journey at their own pace.

Airports are already using automation to improve the passenger experience allowing for the flexibility to scale up and down their activities due to seasonal changes, passenger growth and major disruptions to the industry.

KEY TAKEAWAY

Three areas derive value from a biometric implementation: the use of cloud security; data ownership; and the opportunities of digital travel credentials.

The introduction of biometric technology needs to be implemented carefully without major interruption to present operations, disruption to the passengers as well as integrating into present systems and technologies. Planning is critical as the replacement of assets is intrusive, linked to current technologies, and the introduction of a multitude of solutions providers and contractors, as well as existing infrastructure which is operating in different types of building and terminal designs. One of the challenges, is to develop an interoperable identity management system that can be used worldwide rather than countries and stakeholders investing in localized solutions that are not interoperable or accepted by different authorities.

Biometric systems should be designed to anticipate development and easily adopt new technological advancements, modularizing components which are likely to become obsolete such as biometric sensors and matching systems. A life-cycle approach is needed, considering capabilities and limitations of the technology and devices. This approach must also be flexible enough to manage the unexpected reactions of users, operators, and other stakeholders.

Cloud Data Security, Ownership and Technology

Data security has consistently been a major issue in information technology. Biometrics use cloud computing environments, primarily because the data can be stored in different locations across the globe. Data security and privacy protection are the two main factors of the user's concerns about the cloud technology. Data security and privacy protection issues are relevant to both hardware and software in a cloud architecture.

Cloud computing allows processing on-demand, and a convenient, ubiquitous network access to shared configurable computing resources such as storage, networks, servers, services, and applications. This type of solution is suitable for biometric solutions. Biometric identification management systems are multimodal, and they generate large amounts of data. Processing petabytes of data cannot single-handedly be addressed by sheer CPU power and needs flexible and economical infrastructure that can manage the variable processing and data requirements.

Data ownership in any environment relates to both the possession of and responsibility for information. In other forms of control of information cloud services not only provide the ability to access, create, modify, package, derive benefit from, sell or remove data, but also to protect by applying rules relating to the assignment of privileges to others.

In a cloud environment the use of blockchain technology is beneficial when low processing volumes are expected, storing transactional records in a distributed ledger database (blocks) with links to numerous stakeholder databases (chain). The records are unchangeable and signed cryptographically with a consensus protocol to confirm that the data is true or not.

In order to deliver a biometric solution across different geographies these standards will need to be applied.

Digital Travel Credential and Self-Sovereign Identity (SSI)

Potentially when booking or checking in, travelers could send their virtual credential in advance from their mobile phone to the border authority, or to an airline for Advanced Passenger Information/PNR purposes. As ICAO’s DTC standards is implemented by different countries, it could simplify biometric enrollment, or potentially augment legacy systems such as ESTA.

For the DTC, ICAO has a role to coordinate and establish the digital identity format between all nations. Border authorities are the direct stakeholders charged with the responsibility of ensuring that border processes comply with national legislation. Airports and airlines are indirect stakeholders that may benefit from more efficient passenger processes. Technology providers have an interest in developing systems that they can sell on a global scale.

The digital travel credential can be used as part of the credential issuing stage of a biometric process. This step can be performed from a passenger’s mobile phone and the credentials can be sent to any system or database. Related to the DTC where no specific facilities are required, this will depend on the use case that is to be applied at the airport. Theoretically all passengers could be able to prove their identity, store their biometric details digitally and have it certified with an identity verifier.

A secure digital biometric system will bring many opportunities and advantages for passenger processing and can be adopted internationally. A similar timeframe to the adoption of e-Passport standards could be foreseen.

Due to individual countries developing and adopting their own biometric solutions, we are moving towards a wide range of different systems per country and on an extraterritorial basis where, this can be the norm in the future.

Chapter 6

Future Directions

Suggestions for Further Study

Acknowledging that this Primer has been developed at a time when biometric technologies, the related laws and policies, and most importantly our understanding of the technology, are developing, the research team recommends a timely update of this research, ideally within 2-3 years.

The research team is also mindful that a Primer has limited scope to address emerging issues, especially regarding the tools deployed for COVID-19 pandemic recovery that are driven by the need for a touchless environment. There are five core recommendations for further study, which may be additional research scopes, pilot projects or other proof-of-concept ideas that government and industry stakeholders could pursue.

Running Inventory of Airport Pilot Projects and In-The-Field Research

Regarding additional research scopes and especially pilot projects, the research team realizes the immense value that feedback from in-the-field research into biometrics, together with new applications of biometrics, as well as (in some cases on-going) pilot projects have provided our research and development of this Primer. For future projects, a running inventory of commencing, ongoing and recently completed in-the-field research as well as pilot projects testing new technologies, procedures or ideas would be an invaluable resource for Principal Investigators and their teams. Maintaining such an inventory, in a collaborative manner would benefit the ACRP community, possibly through the IdeaHub platform.

For Further Study

The five core recommendations below have separately been developed further in a memo titled: “Further Recommended Research Memo”.

1. Human Factors Research

There are core aspects of biometrics that are heavily driven towards technological solutions. The language of solutions development is largely around “false accept” and “false reject” rates, as well as the architecture and solutions to share information. While many solutions have a holistic review of human factors, more research is needed to assess the acceptability and suitability of solutions to the very subject of biometrics: the humans themselves.

Research could involve a range of tests around the solutions and devices themselves, or with emerging areas on passenger communications. Digital transparency in the public realm, for example, is an area that requires more attention to uncover the opportunities to improve the way passengers and employees understand about the use of biometric data.

2. Self-Sovereign Identity, Middleware & Traveler Verification Service

Self-sovereign identity could provider passengers and staff at airports with greater ability to own identity data fully without intervention from outside administration. At the same time, systems that are geared towards admissibility to the United States, are structured around longer (75 year) retention periods that challenge both the control function and privacy concepts such as the right-to-forget.

As systems like TVS are geared around the ability to host identity information in a government-controlled cloud system, there is an emerging area of problem solving that requires more detailed use cases to bridge the gap between self-sovereign identity and models such as TVS. Middleware is likely needed as a way of defining the models for the ability for TVS to work with emerging global standards such as ICAO Digital Travel Credential.

Whether the research effort is suitable for a hack-a-thon or series of hack-a-thons to deliver potential solutions, there is an aspect of creating an environment to maximize the strengths of self-sovereign identity and the power of the existing TVS framework.

3. Biometrics Best Practice Designations

The current state of facial recognition and biometrics is one where the language is expansive and unclear to the end user. There is an equation of the methodologies used by Clearview AI, hack of Perceptics data, to the processes used by airlines, airports and many government agencies.

Whether it is green buildings, genetically modified food product certification, or other applications that are driven by potentially risky issues, there is further research needed to codification of best practice designations in biometrics that cover the gamma of privacy, operational, technology or other aspects of uses that are used to differentiate the myriad of uses in airports.

Research that has led to the to the WEF publication on “Responsible Use of Facial Recognition”, should be regarded in the research, and, ideally, be implemented at airports, especially as the evolution of tackling the ability for domestic TSA checkpoint biometrics accelerates.

4. Equity, Diversity and Inclusion Reviews

High profile cases of biometric systems that have different performance by race are indicative of issues from a societal and technological point of view. Where one community is adversely impacted compared to another, there are issues that can challenged the perception of biometrics at airports, especially with a population of passengers from all around the world. Moreover, there are also known issues for the ability for individuals with different mobility issues that can both benefit from or be challenged by biometric solutions.

5. Digital Twins and Biometric Models

Lastly, an area of research is the ability to create a digital model of facilities for airport operators and aviation industry participants to better understand the potential of biometric systems. In the past, the U.S. Commercial Aviation Partnership had an econometric model in place to assess the value of new measures advanced at airports. This research effort was conducted under the Aviation Security Advisory Committee. There may be the need to augment past efforts to emulate across airports, airlines, and government agencies a standing model based on digital twins that is able to predict the power of different modes of biometric implementation across major passenger and employee flows.

References

Accenture. 2018. The Known Traveller Digital Identity System. Accenture Canada Newsroom. https://www.accenture.com/ca-en/company-news-release-canada-test-advancements.

Accenture. 2018a. The Known Traveller Unlocking the potential of digital identity for secure and seamless travel. WE Forum. http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.

Airport Technology. 2019. Kempegowda Airport launches biometric boarding solution. Airport Technology News. https://www.airport-technology.com/news/biometric-boarding-kempegowda-airport/.

Airport Technology. 2020. Telos ID to carry out background checks at Seattle-Tacoma Airport. Airport Technology. https://www.airport-technology.com/news/telos-id-background-checks-seattle-tacoma-airport/.

Amazon Go. 2020. Amazon Go Launch Page. Amazon.com. https://www.amazon.com/b?ie=UTF8&node=16008589011.

Amazon. 2015. Introducing Amazon Go and the world's most advanced shopping technology. Youtube. https://youtu.be/NrmMk1Myrxc.

Amazon. 2020. Just Walk Out. Bringing Just Walk Out shopping to your stores. https://justwalkout.com/.

Aruba Happy Flow. 2020. The first 100% self-service passenger experience, based on traveler-centric biometric technology, from curb to boarding! Secure, quick and easy! Aruba Happy Flow. http://www.arubahappyflow.com/.

Aviation Transportation Security Act, 49 USC. §§ 44936 et. seq. (Pub. L. 107-71); 49 CFR part 1542; TSA Directive 1542-04-08G. *See also*, 49 USC. §106(l)(6)), stating "the Administrator is authorized to enter into and perform such contracts, leases, cooperative agreements, or other transactions as may be necessary to carry out the functions of the Administrator and the Administration.

Awtaney, A. 2019. DigiYatra: The good and the bad of using your face as a boarding pass for your flight. cnbctv18.com. https://www.cnbctv18.com/views/digiyatra-the-good-and-the-bad-of-using-your-face-as-a-boarding-pass-for-your-flight-4344871.htm.

Ayers, T. and Lucini, D. E. 2012. Aerospace and Defense Technology Alert. . Telos ID. http://www.telosid.com/wp-content/uploads/2019/02/TelosID-FrostSullivan-Jan31.pdf.
Bacco, E. M. and Hiatt, D. K. 2010. Activity verification.

Badgley, S. 2020. Telephone interview with Sonya Badgley, Section Chief for Regulatory Analysis and Stakeholder Management, TSA. personal.

Baran, M. 2020. First U.S. Biometric Screening Terminal Opens in Atlanta. AFAR. https://www.afar.com/magazine/the-first-us-biometric-screening-terminal-is-coming-to-atlanta.

Beroukhim, R. and Exum, A. 2018. NeoFace Express. NEC Today. https://nectoday.com/tag/neoface-express/.

Beunardeau, Y., Beeson, A., Wilcox, S. and Price, A. 2019. IATA Ground Handling Conference 2019. In The Future of the Passenger Process. Madrid.

Bhavan, R. G. 2018. Digit Yatra: Reimagining Air Travel in India. https://www.civilaviation.gov.in/sites/default/files/Digi%20Yatra%20Policy%2009%20Aug%2018.pdf.

Bishop, T. 2020. Our first-hand experience with Amazon's new palm reader, and what it says about the future of retail. GeekWire. https://www.geekwire.com/2020/first-hand-experience-amazons-new-palm-reader-says-future-retail/.

Bishop. 2020. AmazonGo delivers a dramatic increase in retail productivity metrics. Brick Meets Click. https://www.brickmeetsclick.com/amazongo-s-retail-productivity--at-least--2700-sq-ft-selling-area---50-inventory-turns-year.

Boyd , A. 2019. An Inside Look at All the Data CBP Collects About Everyone Crossing U.S. Borders. Nextgov.com. https://www.nextgov.com/emerging-tech/2019/09/inside-look-all-data-cbp-collects-about-everyone-crossing-us-borders/159946/.

Boyd, A. 2020. CBP Expands Facial Recognition for Global Entry Travelers. Nextgov.com. https://www.nextgov.com/emerging-tech/2020/01/cbp-expands-facial-recognition-global-entry-travelers/162498/.

Bureau, E. T. 2019. Biometric journey goes live at Bengaluru airport. The Economic Times. https://economictimes.indiatimes.com/industry/transportation/airlines-/-aviation/biometric-journey-goes-live-at-bengaluru-airport/articleshow/70345610.cms?from=mdr.

Burriesci, K. A. 2020. Telephone interview with Kelli Ann Burriesci, Assistant Administrator, Enrollment Services and Vetting Programs, TSA. personal.

Burt, C. 2019. Vision-Box biometric technology launched for Digi Yatra at Bengaluru airport: Biometric Update. Biometric Update. https://www.biometricupdate.com/201907/vision-box-biometric-technology-launched-for-digi-yatra-at-bengaluru-airport.

Burt, C. 2020. Privacy and Civil Liberties Oversight Board assesses Atlanta airport biometrics. Biometric Update. https://www.biometricupdate.com/202001/privacy-and-civil-liberties-oversight-board-assesses-atlanta-airport-biometrics.

Business Traveller India. 2020. Bengaluru airport extends biometric-based self-boarding solution to Air Asia India. Business Traveller News. https://www.businesstraveller.com/business-travel/2020/08/03/bengaluru-airport-extends-biometric-based-self-boarding-solution-to-air-asia-india/.

Cabrera, Frederico. Interview with Frederico Cabrera, Airport Operations & CX Manager at Aeropuerto de Carrasco . Personal, September 16, 2020.

Calixte, M.(2020. Telephone interview with Marc Calixte, Program Manager, Traveler Entry Programs, Admissibility and Passenger Programs, CBP. personal.

Cantor, J. R. 2020. Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (2020). Department of Homeland Security - Customs and Border Protection.

Cerri, R. 2020. COVID-19: Using technology in airports to fight a pandemic: ACI World Blog. ACI Insights. https://blog.aci.aero/covid-19-using-technology-in-airports-to-fight-a-pandemic/.

Cheng, A. 2019. Why Amazon Go May Soon Change The Way We Shop. Forbes. https://www.forbes.com/sites/andriacheng/2019/01/13/why-amazon-go-may-soon-change-the-way-we-want-to-shop/#6c90e2856709.

Curtis, L. 2020. Telephone interview with Lauren Curtis, Senior Manager, Aviation Security, Credentialing and Assessment, SEA. personal.

DEN Talks. 2020. Innovative Airport Experiences. Youtube.com. DEN Talks: Innovative Airport Experiences.

Department of Homeland Security. 2008. U.S. Customs and Border Protection; Announcement of Program Pilot: International Traveler (IRT) Registered, 73 Fed. Reg. 19,861 (April 11, 2008)

Department of Homeland Security. 2008a. U.S. Customs and Border Protection; International Registered Traveler Pilot Program Name Changed to Global Entry; Program Starting Date Accelerated; Changes to Enrollment Center Information, 73 Fed. Reg. 30,416 (May 27, 2008)

Department of Homeland Security. 2008b. U.S.Customs and Border Protection; Expansion of Global Entry Pilot Program, 73 Fed. Reg. 47,204 (August 13, 2008)

Department of Homeland Security. 2009. U.S. Customs and Border Protection; Expansion of Global Entry Pilot Program, 74 Fed. Reg. 39,965 (August 10, 2009)

Department of Homeland Security. 2012. Establishment of Global Entry Program, 77 Fed. Reg. 5,681 (February 6, 2012)

Department of Homeland Security Inspector General. 2013. Transportation Security Administration's Aviation Channeling Services Provider Project, https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-42_Feb13.pdf

Department of Homeland Security. 2020. Biometrics Technology. Transportation Security Administration. Accessed August 2020. https://www.tsa.gov/biometrics-technology.

Devaiah, D. 2019. Bangalore airport to introduce facial recognition tech for passengers. The Indian Express. https://indianexpress.com/article/cities/bangalore/bangalore-airport-to-introduce-facial-recognition-tech-for-passengers-5727299/.

Daon. 2020. VeriFLY: For a faster return to safe, in-person experiences. Verifly Product Page. Accessed August 2020 https://www.daon.com/products/verifly.

Easy Airport. 2020. Fácil - ágil - seguro. EasyAirport. Accessed September 2020. https://www.easyairport.biz/.

The Economist. 2020. Atlanta airport launches America's first "biometric terminal". The Economist. https://www.economist.com/gulliver/2018/10/17/atlanta-airport-launches-americas-first-biometric-terminal.

ET Government. 2020. DigiYatra Project: AirAsia India joins Bangalore International Airport to improve contactless boarding. ETGovernment.com. https://government.economictimes.indiatimes.com/news/technology/digiyatra-project-airasia-india-joins-bangalore-international-airport-to-improve-contactless-boarding/77330075.

FlyDenver. 2020. Services: VeriFLY. VeriFLY: Denver International Airport. Accessed August 2020. https://www.flydenver.com/verifly.

Future Travel Experience. 2019. Overcoming obstacles to the mass rollout of biometrics in air transport. Future Travel Experience. https://www.futuretravelexperience.com/2019/08/overcoming-obstacles-mass-rollout-biometrics-air-transport-industry/.

Future Travel Experience. 2019a. Bengaluru International Airport introduces kerb-to-gate biometric journey. Future Travel Experience. https://www.futuretravelexperience.com/2019/07/bengaluru-airport-kerb-to-gate-biometric-journey/.

Gendreau, P. 2020. Interview with Patrick Gendreau, Director, Planning - Terminal Operations chez ADM Aéroports de Montréal. personal.

Government of India. 2020. Digi Yatra- A New Digital Experience for Air Travellers. National Portal of India. https://www.india.gov.in/spotlight/digi-yatra-new-digital-experience-air-travellers.

Gyori, B. J., Medrano, I., Frenkel, A. M., and; Java, P. N. 2018. Shelf with integrated electronics.

Hamilton, S. 2020. Telephone interview with Stephanie Hamilton, Branch Manager, Vetting Programs Branch, TSA. personal.

Harper, J. 2018. Bye-bye Boarding Pass: Delta Will Offer Curb-to-Gate Facial Recognition. Point Me to the Plane. https://pointmetotheplane.boardingarea.com/bye-bye-boarding-pass-delta-will-offer-curb-to-gate-facial-recognition/.

Hautala, L. 2019. Facial recognition can speed you through airport security, but there's a cost. CNET. https://www.cnet.com/news/facial-recognition-can-speed-you-through-airport-security-but-theres-a-cost/.

Heathrow. 2018. Heathrow moves toward cutting-edge travel with world's largest biometrics roll out . Heathrow Media Centre. https://mediacentre.heathrow.com/pressrelease/details/81/Brand-News-22/10209.

Heathrow. 2020. Testing equipment to make Heathrow faster and safer Heathrow Departures, until April 2020. Biometric Testing. https://www.heathrow.com/at-the-airport/security-and-baggage/biometric-testing.

Heathrow. 2020a. Regulatory Sandbox Final Report: Heathrow Airport Ltd. . (2020, June). Information Commissioners Office. https://ico.org.uk/media/for-organisations/documents/2618024/heathrow-airport-ltd-regulatory-sandbox-final-report.pdf.

Kaplan, P. S. 2018. Privacy Impact Assessment for the Traveler Verification Service. 2018. Department of Homeland Security - Customs and Border Protection.

Kelleher, S. R. 2019. Paradigm Shift: Biometrics And The Blockchain Will Replace Paper Passports Sooner Than You Think. Forbes Magazine. https://www.forbes.com/sites/suzannerowankelleher/2019/06/28/paradigm-shift-biometrics-and-the-blockchain-will-replace-paper-passports-sooner-than-you-think/?sh=2c10b5095c7f.

Khadakbhavi, S. 2019. India's answer to a capacity problem country-wide: Digi Yatra. International Airport Review. https://www.internationalairportreview.com/article/90158/india-capacity-digi-yatra.

Khadakbhavi, S. 2020. Telephone interview with Suresh Khadakbhavi, Assistant Vice President Innovation Lab at Bangalore International Airport. personal.

Khan, S. 2020. What is Digi Yatra? Enrollment, security, benefits of biometric boarding at Bengaluru Airport. IBTimes India. https://www.ibtimes.co.in/what-digi-yatra-enrollment-security-benefits-biometric-boarding-bengaluru-airport-812105.

Knoppers, J. 2020. Interview with Jordie Knoppers, Customer Journey Manager Seamless Travel & Biometrics at KLM Royal Dutch Airlines. personal.

Known Traveller Digital Identity. 2020. Unlocking the potential of digital identity for secure and seamless travel. KTDI.org. https://ktdi.org/.

Kumar, D., Kim, S., Veikherman, D., Smith, K. J., Peterfreund, N., Orlov, N., … Aggarwal, M. 2018. Accessed on 2020, December 22. Non-contact biometric identification system.

Kumar, D., Kornfield, E. M., Prater, A. C., Boyapati, S., Ren, X., & Yuan, C. 2013. Accessed on: 2019, April 23. Detecting item interaction and movement.

Lakshman, R. 2020. Bengaluru International Airport Proposes Biometric-Based Technology To Reduce Immigration Queues. Aviationscoop. https://aviationscoop.com/bengaluru-international-airport-proposes-biometric-based-technology-to-reduce-immigration-queues/10868/.

Linder, C. 2020. How Coronavirus Has Ushered In the Airport of the Future. Popular Mechanics. https://www.popularmechanics.com/technology/infrastructure/a32703817/future-airport-tech-coronavirus/.

Mayhew, S. 2018. Vision-Box bringing biometric self-boarding tech to BLR airport: Biometric Update. Biometric Update. https://www.biometricupdate.com/201809/vision-box-bringing-biometric-self-boarding-tech-to-blr-airport.

McLaughlin, C. 2020. Daon VeriFLY Interview. personal.

Merrit, G. 2021. Interview with George Merrit of VeriFLY by Daon. personal.

Mongin, S., and Danisek, D. 2019. Department of Homeland Security Privacy Impact Assessment Update for the Global Enrollment System (GES): Global Entry Facial Recognition. Department of Homeland Security.

Montevideo Carrasco Airport. 2020. General Information. AirMundo. Accessed on July 2020. https://airmundo.com/en/airports/montevideo-carrasco-airport/.

Mujica, F., Hernandez, J., Robinson, M., Jordan, C., Tydeman, J., Simeone, E., and; Ricarte, A. 2020. Customer Reviews. SKYTRAX. https://www.airlinequality.com/airport-reviews/montevideo-airport/.

Murph, D. 2018. Delta Launching First U.S. Biometric Terminal in Atlanta. The Points Guy. https://thepointsguy.com/news/delta-launching-biometric-terminal/.

Mutzabaugh, B. 2018. Delta says U.SA.'s 'first biometric terminal' is ready to go at Atlanta airport. USA Today. https://www.usatoday.com/story/travel/flights/todayinthesky/2018/11/29/delta-usas-first-biometric-terminal-ready-go-atlanta-airport/2145655002/.

NEC. 2020. About Us - Brand. NEC. https://www.nec.com/en/global/about/brand/.

OT Staff. 2019. No More Lines: Bengaluru Airport To Introduce Biometric Technology For Immigration. Outlook Traveller. https://www.outlookindia.com/outlooktraveller/travelnews/story/69899/bengaluru-airport-to-introduce-biometric-technology-for-immigration.

OTG Management. 2020. OTG to Use Amazon’s Just Walk Out Technology to Bring Checkout-free Shopping to Airports. Aviation Pros. https://www.aviationpros.com/airports/airport-revenue/concessionaire-retail/press-release/21129357/otg-management-otg-to-use-amazons-just-walk-out-technology-to-bring-checkoutfree-shopping-to-airports.

Patterson, T., Russell, L. 2018. U.S. airport opens first fully biometric terminal. CNN. https://www.cnn.com/travel/article/atlanta-airport-first-us-biometric-terminal-facial-recognition/index.html.

Pilli, S. 2020. Transportation Security Clearinghouse. American Association of Airport Executives. https://www.aaae.org/aaae/AAAEMBR/AAAEMemberResponsive/About_AAAE/AAAE_Affiliate_Organizations/Transportation_Security_Clearinghouse.aspx.

Pitrelli, M. B. 2020. Five ways the pandemic may change airports for the better. CNBC. https://www.cnbc.com/2020/05/27/what-will-flying-be-like-how-coronavirus-is-changing-airports.html.

Press Trust of India. 2020. Bangalore Airport extends biometric-based self-boarding facility to AirAsia. Business Standard. https://www.business-standard.com/article/companies/bangalore-airport-extends-biometric-based-self-boarding-facility-to-airasia-120080301061_1.html.

Puerini, G. L., Kumar, D. and Kessel, S. 2014. Accessed on 2019, January 8. Transitioning items from a materials handling facility.

Rouaix, F. M. 2012. Position-based item identification in a materials handling facility.

Shorr. 2018. Are We Ready for Amazon Go? Are We Ready for Amazon Go? Shorr Packaging Corporation. https://www.shorr.com/packaging-news/2018-02/are-we-ready-amazon-go.

Steele, K. 2019. Delta expands optional facial recognition boarding to new airports, more customers. Delta News Hub. https://news.delta.com/delta-expands-optional-facial-recognition-boarding-new-airports-more-

customers#:~:text=Over%20the%20next%20month%2C%20Delta,recognition%20boarding%20at%20ATL%20Concourse.

Steele, K. 2020. Delta unveils first biometric terminal in U.S. in Atlanta; next stop: Detroit. Delta News Hub. https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit.

Steenbergen, A. 2020. Interview with Annet Steenbergen, OneID Advisory Board to the Government of Aruba . personal.

Stewart, L. (Ed.). 2019. Making the Passenger Experience More Efficient, Optimised and Human-Centered. Passenger Connected Digital Magazine.

Tarver, E. 2020. Which Industries Have the Highest Inventory Turnover? Investopedia. https://www.investopedia.com/ask/answers/051915/which-industries-tend-have-most-inventory-turnover.asp.

Telos ID. 2020. About Telos ID Enrollment Services. Telos ID: Identity Access and Management Solutions. https://www.telosid.com/solutions/enrollment-services/idvetting/.

Telos ID. 2020a. Submit Fingerprints & Enrollment Information to TSA: Telos ID DAC. Identity Access and Management Solutions | Telos ID. https://www.telosid.com/solutions/aviation-channeling/about-dac/.

THALES. 2021. DHS's Automated Biometric Identification System IDENT – the heart of biometric visitor identification in the USA. THALES. http://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/ident-automated-biometric-identification-system.

Today.com. 2020. Inside Delta’s 1st Biometric Airport Terminal In Atlanta. Youtube.com. https://www.youtube.com/watch?v=gYbNqjatGNA.

TSA. 2018. SIDA Airport Security Fiscal Year 2017. (2018, February 6). Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/TSA%20-%20SIDA%20Airport%20Security.pdf.

TSA. 2020. TSA PreCheck®. Transportation Security Administration. https://www.tsa.gov/precheck.

TSA. 2020a. Biometrics Technology. Transportation Security Administration. https://www.tsa.gov/biometrics-technology.

U.S. Customs and Border Protection. 2018. Global Entry Celebrates 10 Years of Expediting International Travel with Launch of Facial Recognition Pilot at MCO. Official website of the Department of Homeland Security. https://www.cbp.gov/newsroom/national-media-release/global-entry-celebrates-10-years-expediting-international-travel.

US Customs and Border Protection. 2021. CBP officer, Simplified ARRIVAL nabs impostor to U.S. passport at Dulles Airport. Retrieved March 28, 2021, from https://www.cbp.gov/newsroom/local-media-release/cbp-officer-simplified-arrival-nabs-impostor-us-passport-dulles-airport

U.S. Department of Homeland Security, Office of Inspector General. 2019. *CBP's Global Entry Program Is Vulnerable to Exploitation (REDACTED)*. (Publication No. OIG-19-49).

U.S. Government Accountability Office. 2014. *Trusted Travelers: Programs provide benefits, but enrollment processes could be strengthened.* (Publication No. GAO-14-483). Retrieved from GAO Reports Main Page via GPO Access database: https://www.gao.gov/reports-testimonies/by-topic/

U.S. Government Accountability Office. 2020. Facial Recognition: CBP and TSA are taking steps to implement programs, but CBP should address privacy and system performance issues. (Publication No. GAO-20-568). Retrieved from GAO Reports Main Page via GPO Access database: https://www.gao.gov/reports-testimonies/by-topic/

Vision-Box. 2018. Vision-Box closes major deal with Bangalore International Airport Limited. Vision-Box Pressroom. https://www.vision-box.com/pressroom/press-releases/vision-box-closes-major-deal-with-bangalore-international-airport-limited.

Vision-Box. 2018a. Corporación America will automate airports in Latin America and Europe with Vision-Box contactless biometric platform. Vision-Box Press Room. https://www.vision-box.com/pressroom/press-releases/carrasco-airport-first-fully-digital-ariport-in-latam.

Vision-Box. 2018b. Carrasco International Airport - 1st fully digital airport in Latin America. Youtube.com. https://www.youtube.com/watch?v=hrjmAybsgdY&feature=youtu.be

Vision-Box. 2019. Kerb-to-Gate Biometric Journey goes live at Kempegowda International Airport. Vision-Box Pressroom. https://www.vision-box.com/pressroom/press-releases/digi-yatra-seamless-flow-goes-live-at-blr-airport.

Walters, T. 2020. Does Amazon Go + GDPR = Amazon No-Go? Digital Clarity Group. https://www.digitalclaritygroup.com/gdpr-amazon-no-go/.

Wilcox, S. 2019. Using biometrics in multiple stages of the passenger's journey. International Airport Review. https://www.internationalairportreview.com/article/94368/using-biometrics-in-multiple-stages-of-the-passengers-journey/.

Wilcox, S. 2020. Telephone interview with Simon Wilcox, former Head of Innovation at Heathrow and program lead for the seamless travel initiatives. personal.

World Economic Forum. 2020. Shaping the Future of Security in Travel. WE Forum. https://www.weforum.org/projects/shaping-the-future-of-security-in-travel.

World Economic Forum. 2020a. Known Traveller Digital Identity Specifications Guidance. WE Forum White Papers. http://www3.weforum.org/docs/WEF_KTDI_Specifications_Guidance_2020.pdf.

World Travel & Tourism Council. 2019. Seamless Traveller Journey Emerging Models Overview & Findings Report. Oliver Wyman. https://bit.ly/31C64WI.

Yamanouchi, K. 2019. As Delta expands facial scanning, opposition to technology grows. https://www.ajc.com/news/delta-expands-facial-scanning-opposition-grows/wI68thmbgXnNUJu4Khwe9J/.

Yamanouchi, K. 2019a. Privacy Advocates Raise Concerns as Delta Airlines Expands Use of Facial Scanning at Atlanta International Airport. Governing.com. https://www.governing.com/news/headlines/Privacy-Advocates-Raise-Concerns-as-Delta-Airlines-Expands-Use-of-Facial-Scanning-at-Atlanta-International-Airport.html.

Abbreviations, Acronyms and Initialisms

AAAE – American Association of Airport Executives
ACI – Airports Council International
ADIS – Arrival and Departure Information System
AGTS – Automated Guideway Transit System
APC – Automated Passport Control
API – Application Programming Interface
APIS – Advanced Passenger Information System
ATL – Hartfield-Jackson Atlanta International Airport
ATS – Automated Targeting System (CBP)
BIPA – Illinois Biometric Information Privacy Act
BOS – Boston Logan International Airport
CBP – U.S. Customs and Border Protection
CHCR – Criminal History Records Check
COVID-19 – the coronavirus disease associated with the virus designated as SARS-CoV-2 virus
CSCA - Country Signing Certification Authority
CUSS – Common Use Self Service
DAC – Designated Aviation Channeling
DCA – Ronald Reagan Washington National Airport
DEN – Denver International Airport
DHS – Department of Homeland Security
DCS – Departure Control System
DOS – Department of State
DTC – Digital Travel Credential
DTPR – Digital Trust in Places and Routines
DTW – Detroit Metropolitan Wayne Country Airport
EEA – European Economic Area
EES – Entry/ Exit System
eMRTD – electronic Machine-Readable Travel Document
ESTA – Electronic System for Travel Authorization
EU – European Union
EWR – Newark Liberty International Airport
FAA – Federal Aviation Administration
FBI – Federal Bureau of Investigation

FIS – Federal Inspection Service
FIPPs – Fair Information Practice Principles
FLL – Fort Lauderdale-Hollywood International Airport
FTC – Federal Trade Commission
FTCA - Federal Trade Commission Act
GAO – Government Accountability Office
GDPR – General Data Protection Regulation
GES – Global Enrollment System
HART – Homeland Advanced Recognition Technology
IATA – International Air Transport Association
IAD – Dulles International Airport
IAH – George Bush Intercontinental Airport
ICAO – International Civil Aviation Organization
ICE – Immigration and Customs Enforcement
IDaaS – Identity as a Service
IDENT – DHS Automated Biometric Identification System
IdMS – Identity Management System
IT – Information Technology
JFK – John F. Kennedy International Airport
INSPASS – INS Passenger Accelerated Service System
KTDI – Known Traveller Digital Identity
LAX – Los Angeles International Airport
LDAP – Lightweight Directory Access Protocol
NEXTT – New Experience Travel Technologies
NGI – Next Generation Identification
NIST – National Institute of Standards and Technology
PII – Personal Identifiable Information
PNR – Passenger Name Record
POE – Port of Entry
QR code – Quick Response code
Rap Back - Record of Arrest and Prosecution Background (FBI)
ROI – Return on Investment
SEA – Seattle-Tacoma International Airport
SEN – Secure End Node
SIDA – Secure Identification Display Area
SORN – System of Records Notices (Privacy Act)
SPII – Sensitive Personally Identifiable Information
SSI – Self Sovereign Identity

STA – Security Threat Assessment
TSA – Transport Security Administration
TTP – Trusted Traveler Program
TVS – Traveler Verification System
UK – United Kingdom
UPAX – Unified Passenger Module
US – United States
VIP – Very Important Person
VPC – Virtual Private Cloud
WEF – World Economic Forum

Glossary

Specific Terms Explained in Relation to One Another

For the definitions and differences between the terms **Authentication**, **Detection**, **Identification**, **Matching**, **Validation**, **Verification**, see Chapter 1, in the section Fundamentals of Biometrics.

Relating to sensitive and personal information, the following classification:

Personally Identifiable Information (PII) – information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.

Sensitive Personally Identifiable Information (SPII) – is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Sensitive Personal Information (SPI) – information that does not identify an individual, but is related to an individual, and communicates information that is private or could potentially harm an individual should it be made public.

Sensitive Security Information (SSI*) - information that, if publicly released, would be detrimental to transportation security.

*in this Primer, the abbreviation SSI is used for Self-Sovereign Identity

General Terms

Artificial intelligence - a branch of computer science dealing with the simulation of intelligent behavior in computers.

Bias - systematic error introduced into sampling or testing by selecting or encouraging one outcome or answer over others.

Biographic data – information describing non-physical characteristics of a person, e.g., one's name, date of birth and place of birth.

Biometric data – information describing physical characteristics of a person, e.g., height, color of one's eyes, fingerprints, or a photo.

Biometrics - the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity.

Biometric touchpoint – a device where a person can get his/her identity verified by showing a biometric credential (face) to a camera, and after identification perform operations that interact with a specific airport system.

Biometric template – a record of data that is created by encrypting biometric information through cryptography, creating a random sequence of numbers and letters. A biometric template can not be reverted to its original form, it is a one-way method of encoding data.

Blockchain technology - a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network.***

Border Search Exception - a Supreme Court recognized exception to the Fourth Amendment in U.S. law that allows searches and seizures at international borders, without a warrant or probable cause.

Bypass - Biometric data that is tampered with post-capture, or when the camera is by-passed altogether.

Cashierless – the absence of an employee (as in a store) or self-service checkout kiosk to handle monetary transactions.

CPU - the component of a computer system that performs the basic operations (such as processing data) of the system, that exchanges data with the system's memory or peripherals, and that manages the system's other components.

Credential - An object or data structure that authoritatively binds an identity—via an identifier or multiple identifiers—to at least one authenticator possessed and controlled by a subscriber (passenger or airport staff).

Credential Authentication Technology – a TSA technology that ensures ID authentication, reservation verification and Secure Flight pre-screening status at airport security checkpoints.

Cybercrime - criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data.

Cybersecurity - measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Dactyloscopic identification - identification by comparison of fingerprints.

Database - a large collection of data organized especially for rapid search and retrieval (as by a computer).

Data Packet Switching – a method of transmitting data over a digital network, by grouping it into smaller packets of data.

Designated Aviation Channeling (DAC) – a service in the aviation industry that supports conducting required background checks of employees in the sector, ensuring the safety and security.

Digital identity – a digital version of one's identity, the distinguishing character or personality of an individual.

Digital Trust in Places and Routines (DTPR) – Formerly Digital Transparency in the Public Realm, is an open-source initiative by Helpful Places that aims to promote an open-source communication standard to enable transparency, accountability, and control for people.

Distributed ledger (blockchain technology) – a mechanism for storing data, replicated numerous times and in a synchronized manner, geographically spread across multiple computers in different locations. A consensus of all the computers is kept current, making the unsollicatated mutation (e.g., a cyber attack) of the data generally impossible.

e-Passport - a formal document issued by an authorized official of a country to one of its citizens that is usually necessary for exit from and reentry into the country, that allows the citizen to travel to a foreign country in accordance with visa requirements, and that requests protection for the citizen while abroad.

EU-U.S. Privacy Shield program – a framework designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

Fair Information Practice Principles (FIPPs) – are 5 main guidelines published by the U.S. Federal Trade Commission, that represent widely accepted concepts concerning fair information practice in an electronic marketplace for privacy protection

Global Entry® - a U.S. Customs and Border Protection program that allows enrolled members expedited clearance for pre-approved, low-risk travelers upon arrival in the United States.

Health passport – similar to a passport, a health passport contains biographic (and biometric) data as well as imporant health information such as the results of certain tests, vaccinations, and specific medical conditions.

Interoperability - ability of a system (such as a biometric system) to work with or use the parts or equipment of another system.

Known Traveler Number – a number issued by the U.S. Transportation Security Administration (TSA), Department of Homeland Security (DHS), or Department of Defense (DoD) that indicates that a passenger has undergone a pre-flight background check or other screening before checking in for a flight.

Machine Learning - the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data.

Mass surveillance – a form of indiscriminate surveillance that uses systems that collect and analyze surveillance footage, with the intent to identify people for a specific purpose, or range of purposes.

NEXUS – is a voluntary program designed to speed up border crossings for low-risk, pre-approved Canadian travellers into the United States.

OneID - is a concept by IATA which aims to promote a robust, integrated identity management across the end-to-end passenger process, and allows an individual to assert their identity online or in person.

Opt-in – to voluntarily choose to participate.

Passenger journey – the journey of a passenger travelling between an origin destination and a final destination.

PreCheck™ - is a TSA program that lets eligible, low-risk travelers enjoy expedited security screening.

Preclearance – a program that allows a passenger and his/her bags to be inspected and cleared at a foreign airport by U.S. CBP officers prior to travel to the U.S.

Privacy by Design – refers to a set of 7 principles in system or process design that advance the view that privacy assurance must ideally become an organization's default mode of operation and be incorporated from the start of the project.

Rap back (FBI) – refers to the notification returned to an organization when an employee who has undergone a fingerprint-based, state or federal criminal history record information check has a subsequent state or federal criminal history event.

REAL ID - The REAL ID is an act of Congress that mandated minimum security standards for drivers' licenses and identity documents and prohibited federal agencies from accepting "for any official purpose" state driver's licenses or identification cards unless those documents meet the standards set forth therein.

Reasonable expectation of privacy- a person's reasonable expectation of privacy generally means that someone who unreasonably and seriously compromises another's interest in keeping his/her affairs from being known can be held liable for that exposure or intrusion.

Risk-profiling – in the aviation world, the screening of passengers within a specific framework, aiming to address security risks.

Seamless - having no awkward transitions, interruptions, or indications of disparity

Self-Sovereign Identity (SSI)– recognition of the requirement that an individual owns and controls their identity without the intervention of an administrative authority.

Special Needs Exception - an exception to the Fourth Amendment requirement that government searches be supported by a warrant and probable cause which allows government searches that are primarily aimed at advancing some special need other than criminal law enforcement (e.g., security checkpoint searches) and the search program is reasonable given the balance of public and private interests.

Single Sign On (SSO) – an authentication scheme that allows a user to log in with a single set of login credentials, such as a username and password, to access multiple independent applications.

Spoof - A non-living object that exhibits human traits (an "artifact") that is presented to a camera or biometric sensor.

Supremacy Clause – a provision in the U.S. Constitution that establishes that the Constitution and federal laws take priority over any conflicting State laws.

Touchpoints – points of contact and/or engagement between a passenger and a business (i.e., airline, TSA, concessionaire) that can occur at any time throughout a passenger's journey.

Transportation Network Companies – businesses that provide prearranged transportation for compensation using an online-enabled application or platform (such as smart phone apps) to connect drivers using their personal vehicles with passengers.

Trusted Traveler – a passenger who is a member of a risk-based program (i.e., Global Entry®, TSA Pre✓®, SENTRI, NEXUS, and FAST) to facilitate the entry of pre-approved travelers

VeriFLY – the VeriFLY Pass application allows a passenger to verify the required credentials necessary to obtain a valid pass that will enable access to a service where a person must be physically present.

APPENDIX A

Case Study: Amazon Go Cashierless Retail Experience (EWR)

Executive Summary

Initiated by Amazon, the Amazon Go retail experience uses a combination of cameras, sensors, computer vision techniques, machine learning, and artificial intelligence to create a cashierless retail experience. (Amazon Go, 2020) This technology called "Just Walk Out" requires customers to identify themselves when they enter the store. (Amazon, 2020) The customer's identity is verified either by scanning the Amazon Go mobile app (in the case of an Amazon Go store) or their credit card (for other retailers equipped with the "Just Walk Out" technology). A biometric variant also exists, where instead of a QR code or credit card, the customer enrolls at the storefront enrollment kiosk by scanning their 3D hand palm biometric and linking that to their account. (Bishop, 2020)

Source: Amazon.com

Figure A-31: Amazon Go Shopping experience

The "Just Walk Out" technology leverages computer vision and machine learning to distinguish between customers and the items picked out and added to their virtual cart. The system does not rely on facial recognition but movement tracking.

Each customer is associated with a name, an account, and a consumer profile reflecting all interactions with items on the shelves (which items are stared at, picked up, and/or bought). Future use of the customer's data is still undefined. However, the initial patent application included some examples when the customer's purchase history could be used to confirm which items are being picked by the user.

The main benefits include significant time savings for customers, and financial savings for retailers (reduced to no cashiering cost). (Bishop, 2020a) The system architecture relies on Amazon's "Just Walk Out" technology and includes the camera and sensor hardware as well as the software system.

Key Facts

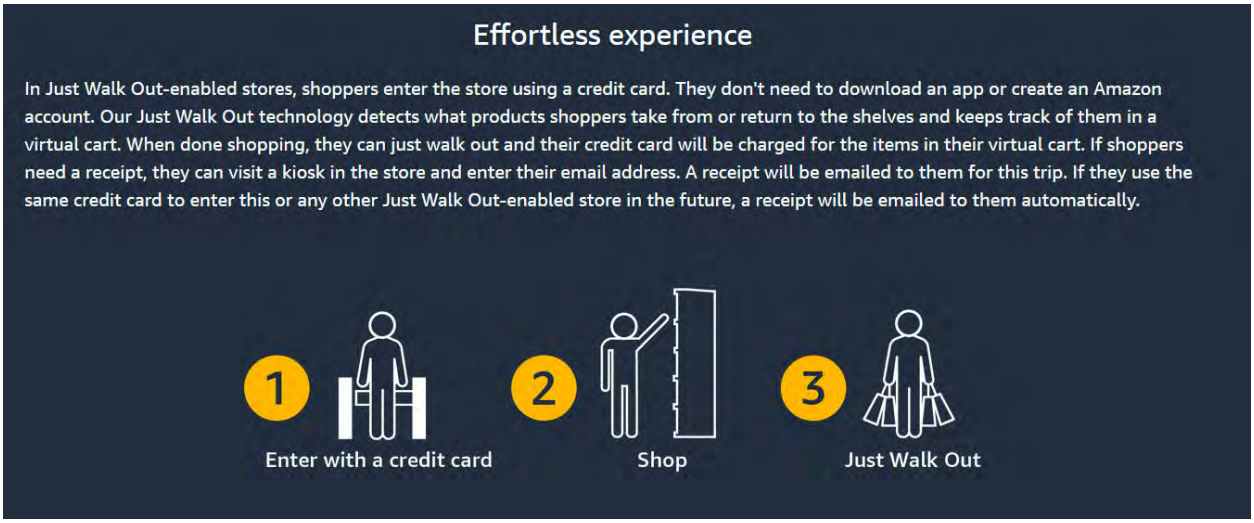
Table A-15: Key facts for the Amazon Go Case Study

What?	• Cashierless retail technology • Project implemented by Amazon
Where?	• 26 Amazon Go stores across the United States (Chicago, New York, Seattle, San Francisco) • Deployment at a few airports across the United States in stores of realter OTG ("On-The-Go"), including at Newark Liberty International Airport (EWR) (OTG Management, 2020)
Customer process steps:	• To access Amazon Go stores: – Create an Amazon account – Download Amazon Go app – Amazon Go mobile app interface generates a QR code, or add a hand palm scan to the account at an enrollment kiosk – Customer enters the store by scanning the QR or hand palm (or credit card for other retail stores with Just Walk Out technology) – "Just Walk Out" technology tracks the customer and their interaction with store items – Virtual cart validation – Exit
Who?	• Amazon patented the "Just Walk Out" technology. They provide the hardware (camera and sensors) along with the software.
Why?	• Amazon's goal is to create a seamless shopping experience where the customers would not have to wait in line.
How?	• The concept relies on the combined use of cameras, sensor fusion, computer vision, deep learning algorithms to track each customer during their time in the store, noting each item picked up/put back, and adding them to their virtual cart. For the biometric hand palm variant, 3D hand palm scanners and a palm recognition software is used.
Enrollment / Digital Identity creation and verification	• An amazon account can be made online, and enrollment is done at the store front, at the enrollment kiosk. There, the online amazon account can be linked to the hand palm biometric, by scanning one's hand at the kiosk.
Verification of identity how?	• Each customer is identified with either a QR code generated by the Amazon Go app in Amazon Go stores, or their credit card in third-party retail stores where the "Just Walk Out" environment is available
For?	• Amazon account holders

How Does it Work?

Before the Customer Journey

- Amazon Go relies on sensor fusion (analyzing and aggregating data from multiple sensors, including weight and movement sensors), advanced data hosting services through Amazon Web Services, and advanced computer vision-based machine learning. (Amazon, 2015)
- The hardware includes electronic shelves, cameras, fixtures, and a facility management system.
- Their inventory management involves data storing and item identification.
- In the case of Amazon Go stores, customers create an Amazon account and download the Amazon Go app.
- In the case of "Just Walk Out" enabled stores, customers access the store with their credit card.



Source: Amazon.com

Figure A-32: "Just Walk Out" enables seamless store experiences for other retailers as well

The Customer Journey

The customer journey can be described in the following steps:

- Each shopper (along with their party) enters and is identified with a QR code generated by the Amazon Go app, biometric hand palm or a credit card in the case of stores equipped with the "Just Walk Out" technology.
- The technology tracks the customer's movements and interactions with the different store items. As customers remove items from the shelves, those items are added to their virtual cart. (Kumar, et al. 2013)
- The customer receives a receipt and is charged when they exit the store.

Retention and Storage

Account data that is saved on Amazon's own servers

- Cameras tracking throughout the store in real time using the video feed streaming from the ubiquitous network of cameras. (Bacco, 2010)

- Amazon Go stores retain data on the interactions of individual customers with the items on the shelf. These data are used to further train the artificial intelligence running the architecture.
- Accuont data is retained and stored at Amazon until the passenger opt for the deletion of their account.
- Customers can elect to delete their biometric data.

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

System Specifications

The system relies on an artificial intelligence to track the customer in the store. The artificial intelligence architecture relies on Amazon Web Services for streaming services, as well as advanced computer vision-based machine learning.

Source: Amazon 2019 re:MARS conference

Figure A-33: Amazon artificial intelligence for the Amazon Go retail experience

Computer Vision-Based Machine Learning

To associate the right items with the right customers, the technology relies on aggregating data from different sensors linked with their locations. The artificial intelligence driving the architecture tracks the customers in the store by aggregating data from different sensors through sensor fusion and solving different identification and linking problems to associate customers, their location, and their interaction with items in the store.

Person Detection

The "Just Walk Out" technology does not use facial recognition technology but relies on Red-Green-Blue cameras equipped with depth and distance sensing capabilities. Each customer is associated with a general profile, an anonymized 3D point cloud. During the customer time in the store, a deep learning algorithm predicts the customer's location and associates that location with their actions and interaction with store items.

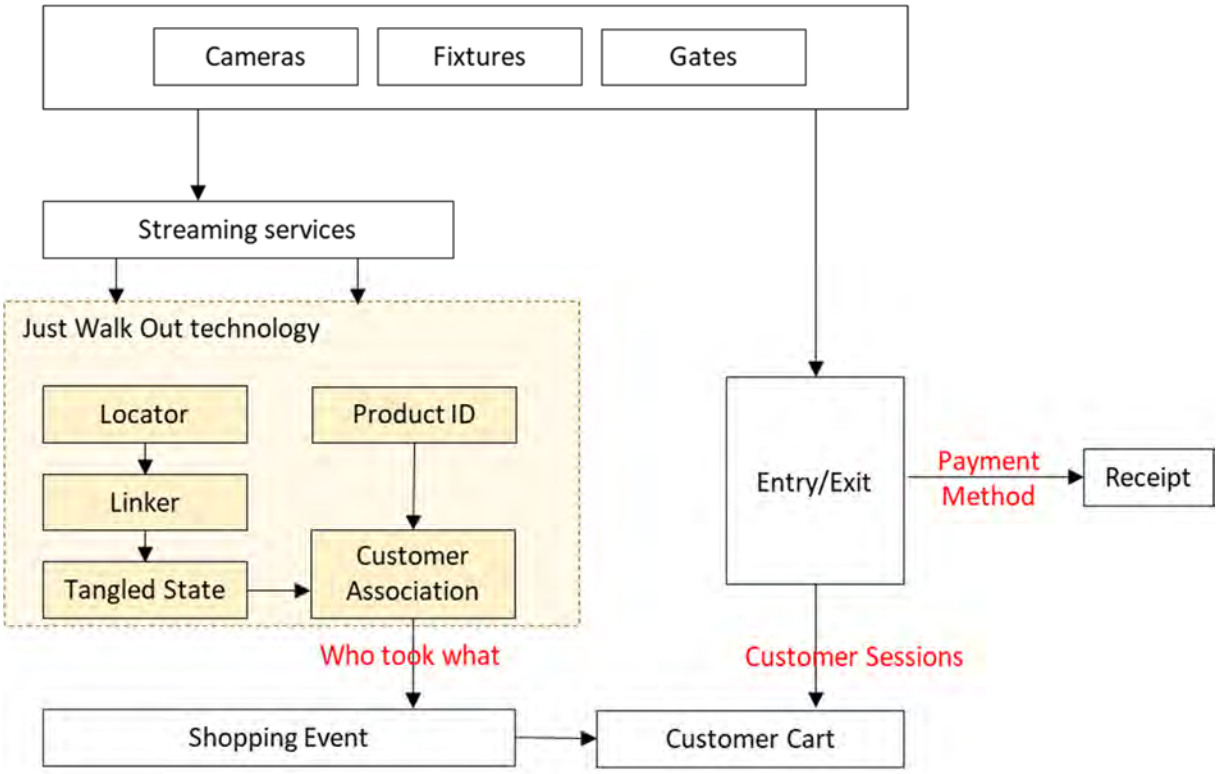
Stakeholders and Responsibilities

Stakeholders

- The main stakeholders of Amazon Go concept is Amazon, and the third-party retailers who have purchased "Just Walk Out" technology services.

Responsibilities

- Amazon owns the "Just Walk Out" concept which builds upon a series of patents submitted by Amazon Technologies since 2013. (Puerini et al. 2014)



Source: 2019 Amazon re:MARS conference

Figure A-34: Logic structure of Amazon Go and technology components

Case Study Review

Benefits

The Just Walk Out technology presents benefits both for the customer, and the retailer. Benefits to customers include:

- Improved customer experience over time with deep learning allowing for faster tracking and more accurate identification of interaction with store items
- Limited contact and interaction with store employees
- Reduced time spent in the store
- No use of facial recognition

Benefits for the retailers providing the "Just Walk Out" enabled experience include:

- Adaptability of the "Just Walk Out" technology to different store layouts
- Financial savings due to reduced staff cost related to cashiering or inventory
- No use of facial recognition
- Improved customer experience
- Detailed consumer profile data

Responses From Customers

Crowd-sourced reviews for individual stores rate on average more than 4 stars out of 5. A stated choice survey conducted by the Shorr group in 2018 found that "84% of respondents to a survey said that they see Amazon Go as a 'type of grocery shopping experience' they'd enjoy more than traditional grocery shopping" and "over 25% of respondents said that they would pay more for grocery products if it meant they didn't have to wait in line at checkout". (Shorr, 2018)

System Performance and Specifications Review

The "Just Walk Out" technology requires approximately $1 million in hardware investment. Customers spending less time in the store allow for higher customer throughput per hour compared to a traditional store. (Cheng 2019) The system is designed for 99% accuracy, including during the busiest periods. On average, Amazon Go stores process 550 customers per day, and as many as 90 people at any given time.

Fall Back Options

- Despite the absence of cashiers, a few store staff are present to assist customers with any technical issues, answer questions, and process cash transactions.
- If a customer is incorrectly charged for an item, they can contest the charge and be reimbursed.

Concerns

- Privacy & use of collected data – lack of transparency on how the collected data factors into the overall Amazon personalized marketing strategy. The architecture relies on deep learning, and data mining of the customer's activity in the store would improve the experience and accuracy over time.
- Lack of transparency around the use of data slowed the adoption of the technology in Europe because of confrontation with GDPR regarding consent to the processing of personal data. In the

context of the regulation, every consent request must state the precise purpose for which the data will be processed. (Walters, 2020)

Lessons Learned

The "Just Walk Out" technology initially relied on motion tracking and an anonymized cloud of data to identify individual customers. However, in December 2019, Amazon submitted a patent for a non-contact biometric identification system to identify customers with their hands. (Kumar, et al. 2018) Introducing hand biometrics as one of the identifying features of each customer is expected to simplify the "Person Detection" component of the Just Walk Out architecture.

Findings and Trends

Findings

The "Just Walk Out" technology is a potential template for future models of touchless and cashierless retail, at airports and other shopping locations. The use of biometrics for identification, camera tracking devices, image analysis software and a program that automates the product billing has proven to create a new user-friendly experience, that is more efficient, touch free and seamless. Amazon has now several versions of this retail experience in operation, and future revisions of the concept will only improve the accessibility. Enrollment challenges may be resolved with biometric palm geometry recognition as currently also being trailed, or with a simple two-step authentication process. Another option is the use of not 1 biometric, but two or several, providing options for customers to choose from.

The main benefits behind utilizing this type of software are; significant time savings for customers and financial savings for retailers, through lower operational expenditures on employees (e.g., labor wages, benefits, etc.). Some enrolment challenges that may be resolved with simple two-step palm enrolment, interesting because may seem less 'invasive' when compared to a picture of one's face. Furthermore, this type of software presents a potential alternative to current and future models for touchless retail for both airports and airlines.

Future Situation and Broader Implementation

As mentioned above, Amazon submitted a patent application for a touchless hand scanning system named "Amazon One" and started implementing it in Amazon Go stores in October 2020. Upon entrance in the store, customers scan their hand at the entry gate.

System Architecture, Pre-Existing Systems and Databases

- The information collected at the entry gate through 'Amazon One" hand scanning device.
- The identification of distinctive future on the hand(s) of the customer relies on a proprietary algorithm, with distinctive features of the hand specific to this proprietary technology architecture.
- Hand biometrics data that are collected are either stored if the customer has an Amazon account, or is deleted once the customer exits the store.
- Referred to as "active" biometrics", as the customer holds their palm over the device to opt in.

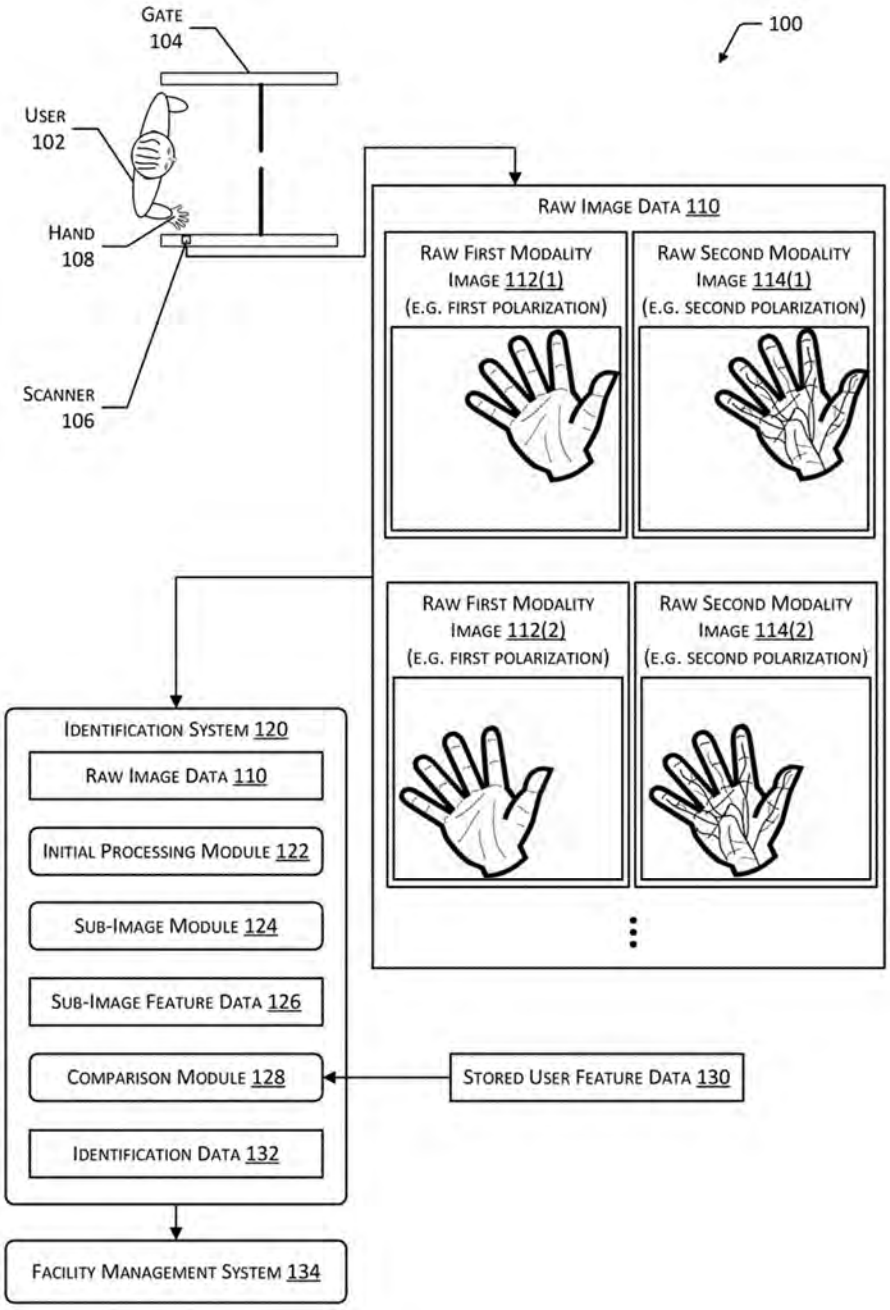


Figure A-35: Hand biometrics identification process

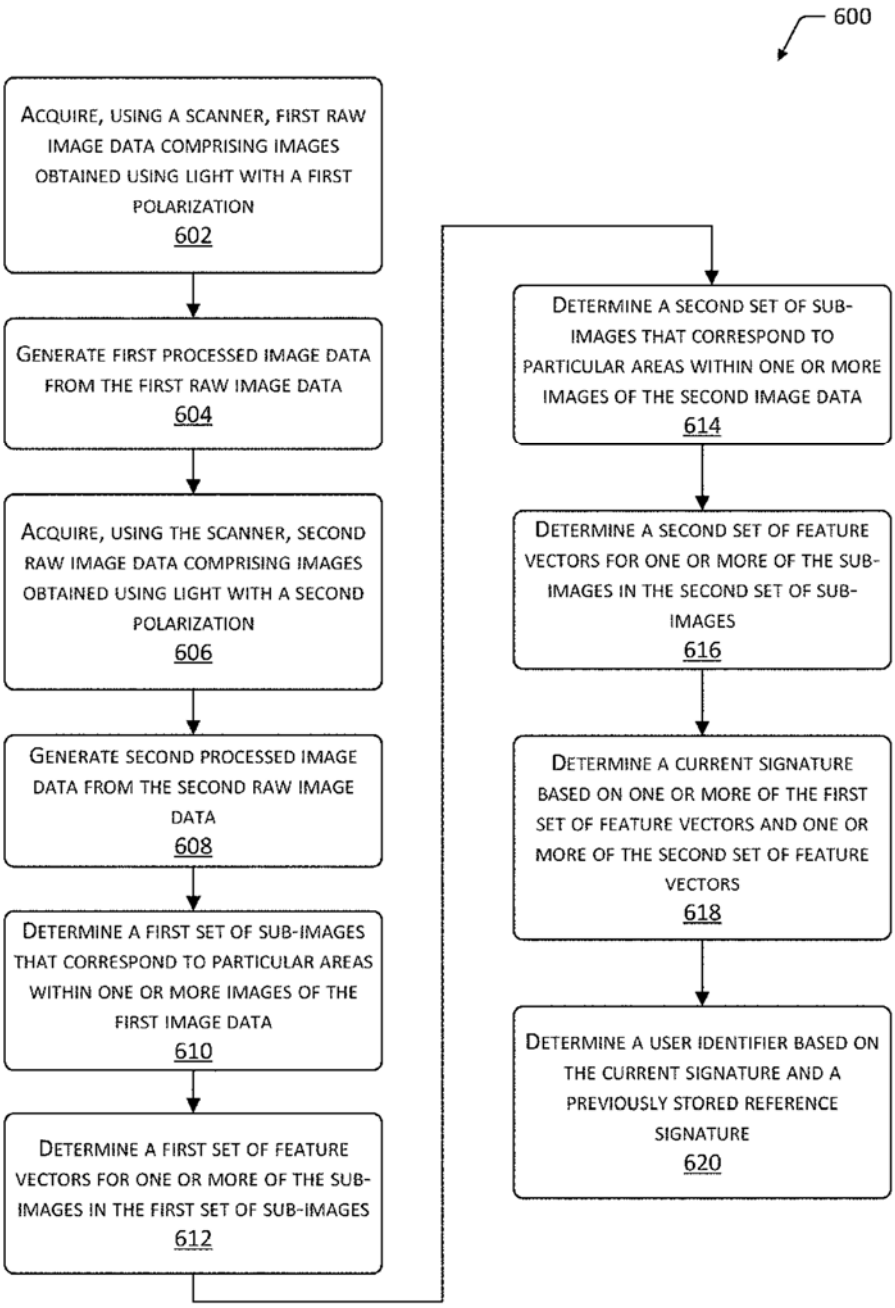


Figure A-36: Hand biometrics characteristics identification

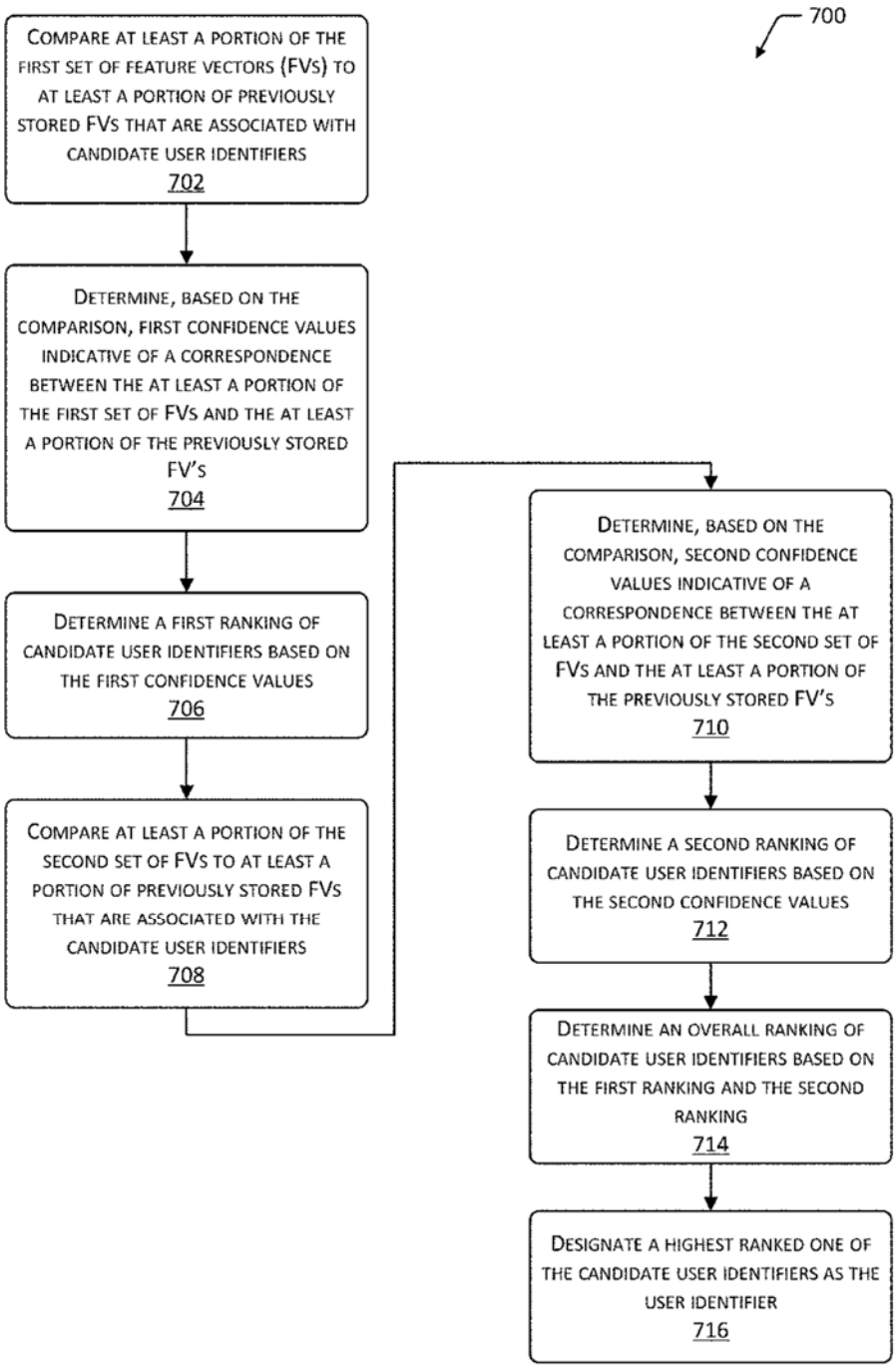


Figure A-37: Person detection based on hand biometrics Identity

Trends Identified

A trend identified in the Amazon case study in which the hand palm geometry is used, with respect to the use of biometrics is that it aims to facilitate a more efficient user friendly (retail) experience. Due to a cashierless system, time is won, the shopping requires less fumbling of personal items for payment, and the simplicity for the user can bring satisfaction. In this specific case, it is not only the biometric technologies enabling this, also the camera tracking system and software that allows for the automatic charging of

customers to their account, contribute. This is a trend we will likely see expand to also other sectors outside retail (and airports).

Similarly, the retail experience removes the need for contact points and (human) interactions, which in a (current and post) Covid-19 era has the added benefit of reducing the risk of transmissible diseases. The camera system, as well as the 3D hand geometry scanners allow for tracking and identification without touching any surfaces.

APPENDIX B

Case Study: Denver - Daon Biometric Partnership (DEN)

Executive Summary

Covid-19 has changed passengers' needs at the airport, with a greater focus placed on health. Denver International Airport (DEN), as part of a goal is to make the passenger journey safer and more predictable, is partnering with Daon, an innovator in biometric authentication with experience developing the TSA PreCheck™ program, to develop a series of pilots at the airport. The technology solutions are based on Daon's "Glide HealthPass" platform, which is a digital health passport that allows businesses to build an authorization process to meet their unique and evolving needs (Daon, 2020). The first pilot is the VeriFLY Reservation System, which is inspired by a self-identified population of health-conscious travelers who want to maximize social distancing while using touchless technologies (DEN Talks, 2020). Using a reservation system similar to OpenTable, travelers make a reservation for access to a dedicated VeriFLY security lane, via an e-gate. Once through screening, travelers would have access to a reserved, lower capacity train car on the Automated Guideway Transit System (AGTS) to access the concourses. VeriFLY is free to passengers, but they must download an app and register with some basic personal information and a photograph, which is stored by Daon. Benefits of the program include building confidence and certainty throughout the passenger journey, flattening the arrival peaks with the reservation system, promoting a touchless and document-free travel experience by incorporating biometrics, and reducing exposure for TSA officers. A second pilot applies the same technology to a remote screening facility, to allow the family of employees to proceed through security outside the terminal area.

Key Facts

Table B-16: Key facts of case study on Daon-Denver partnership

What? (elements of Chapter 1 – Introduction to Biometrics	• Biometric authentication system for security lane reservations and off-airport premises security screening
Where?	• Denver International Airport
Customer process steps:	• Mobile app sign-up to enroll and make a reservation the security checkpoint • On day of travel, passenger self-certifies health status in app and receives QR code • Arrive at airport for designated slot, verify body temperature, and use QR code to access dedicated security checkpoint lane

Who?	• Daon • Denver International Airport • Passengers • TSA
Why?	• Speed up passenger processing of passengers • Relieve pressure on security checkpoints
How? Technology used?	• VeriFLY: Facial recognition to verify identity in the app to bring up a QR code for airport touchpoints • Remote screening: bring security checkpoint off airport premises
Enrollment / Digital Identity creation and verification	• Voluntary program with enrollment completed on the app. Appointments on the app can be booked 2-weeks in advance
Verification of identity how?	• Initial rollout utilizing QR code with future rollout of facial recognition via the mobile app
For?	• Health-conscious departing travelers who want to maximize social distancing and use of touchless technology while being able to get through checkpoint at a known time and access the concourse on a dedicated AGTS car • Remote screening for those passengers without bags traveling with airport employees

Introduction

To balance the needs of passenger health and safety, Denver International Airport has partnered with public health stakeholders and biometric technology firm Daon to develop a biometric authentication system known as VeriFLY, aimed at making passenger journeys safer and more predictable. A second pilot for remote screening takes the security checkpoint off airport premises.

How Does it Work?

Before the Passenger Journey

VeriFLY is free to passengers, but they must download an app and register with some basic personal information (non-PII) and a photograph. Daon's IdentityX® is the world's most trusted digital identity platform, delivering seamless identity establishment and verification, Multi Factor Authentication, and recovery. The technology solutions are based on Daon's "Glide HealthPass" platform, which is a digital health passport that allows businesses to build an authorization process to meet their unique and evolving needs. The database is housed and accessed entirely by Daon.

The Passenger Journey

Within two weeks of travel, the passenger uses the app to create a reservation for a checkpoint timeslot (FlyDenver, 2020). On day of travel, the passenger self-certifies their health status and receives a QR code

to access the e-gate. The QR code verifies identity and reservation time and a scanner verifies body temperature before access is granted.

Retention and Storage

Daon stores the facial biometric and personal information in their system, but customers can purge their information when they want to leave the program. The airport does not store any of the personal information.

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

Stakeholders and Responsibilities

The primary stakeholder is Daon, which is responsible for the software solution and storage of biometrics. It is also funding the current VeriFLY pilot. DEN is another key stakeholder. It is responsible for advertising, staffing, and ensuring the terminal layout and AGTS platform can accommodate the program (McLaughlin, 2020). Passengers are the third key stakeholder since passenger participation is required to make the program successful.

An indirect stakeholder is TSA since the VeriFLY program involves use of a dedicated security checkpoint lane. Early involvement was required to confirm that a dedicated lane and screening staff would be provided for the trial. Future coordination with TSA will be required to adapt the program to changes in technology such as Biometric Credential Authentication Technology, which will remove the role of the travel document checker.

Future stakeholders are expected to include airlines and medical labs as the program is expanded to provide additional functionality.

Case Study Review

Benefits

Benefits of the VeriFLY passenger screening program include building confidence and certainty throughout the passenger journey, flattening the arrival peaks with the reservation system, promoting a touchless and document-free travel experience by incorporating biometrics, and reducing exposure for TSA officers.

Benefits of the remote screening pilot include relieving pressure on the terminal checkpoints while being able to provide an enhanced, touchless experience. There is also a financial benefit of deferring construction of capacity-driven projects.

Responses from Customers

The initial response from customers has been overwhelmingly positive. More than 90 percent of users say they are likely to use it again and would recommend it to friends (Merrit, 2021). New passenger profiles are being created every day, a sign that VeriFLY is gaining in popularity.

System Specifications Review

There has not been a system specification review by a third party as this deployment is still in its early stages.

Fall Back Options

VeriFLY is a voluntary program requiring passengers to opt-in, so passengers do not have to participate. Regular security access in the terminal is still provided.

Concerns

The program is still in its early phases so one of the operational concerns is whether there will be enough passenger demand to warrant a dedicated security screening lane and AGTS train car for passengers who participate in the program. The capacity reduction from the general population would need to be sufficiently offset by passengers utilizing VeriFLY. Other concerns include appointment blocking or other attempts by participants to create a more private experience by reserving multiple timeslots.

Lessons Learnt

In the early days of the program there was a perception that the VeriFLY program was having an unintended consequence of packing more people into fewer train cars because some VeriFLY-dedicated train cars were going out empty. Through increased messaging and an increase in program popularity through the busy holiday period, this misconception was quickly corrected. Additionally, some passengers, upon seeing the success of VeriFLY, tried to download the app and join the process mid-stream. This meant that their temperatures were not checked at the start of the process.

Findings and trends

Findings

The VeriFLY program has grown at a steady pace since initial implementation and has become a program that both state and local health departments have encouraged. Since the airport has been able to prove their concept, VeriFLY will expand to a remote screening facility to allow badged employees and their co-travelers to all clear security protocols based on their specific risk factor.

Future Situation and Broader Implementation

With the initial implementation success, future phases will include incorporation of the facial biometric and ability to access third-party health information to further automate the process. At higher levels on the ladder of confidence, the facial biometric can also eventually be tied into TSA Biometric Credential Authentication Technology to eliminate the traditional role of the travel document checker. This would create a document-free travel experience through the checkpoint.

Trends Identified

The Daon VeriFLY program aligns with the key biometric trend focused on deployment of integrated and multi-stakeholder biometric solutions. While VeriFLY currently provides access only to a security checkpoint lane and the AGTS train, the system is designed to expand to other areas within the airport. This

could include areas such as concessions or ground transportation. Since VeriFLY is in early deployment, the additional functionality layers can be added as more people enroll and as the process at security is further refined and improved.

APPENDIX C

Case Study: CBP Trusted Traveler Programs at U.S. Airports (LAX and More...)

Executive Summary

Global Entry® is a CBP program that allows expedited clearance for pre-approved, low-risk travelers upon arrival in the United States using fingerprints plus passport or, more recently, facial biometric template matching. The program is open to U.S. citizens, U.S. nationals, U.S. lawful permanent residents as well as foreign nationals from 15 countries. Additionally, participants of NEXUS and SENTRI trusted traveler program are allowed use of the Global Entry® kiosks (Department of Homeland Security, 2012). As of August 2020, automatic kiosks are available at 75 U.S. POE including 15 Preclearance airports.

At airports, program members proceed to *Global Entry*® kiosks, have their fingerprints and/or picture taken and are matched against a gallery pre-compiled from a CBP database. The kiosk then issues the traveler a transaction receipt and directs the traveler to baggage claim and the exit.

Travelers must be pre-approved for the *Global Entry*® program. Applications are reviewed by CBP and information is processed through various government databases as part of a rigorous background check. Once conditionally approved, the individual goes to one of over 100 enrollment centers to provide fingerprints and facial photograph along with identity verification documents (e.g., passport, proof of residency) for review by CBP. The biometrics collected at enrollment are used for facial matching each time a passenger uses a Global Entry® Kiosk. The Global Entry® trusted traveler program benefits passengers, CBP, and airports by providing lower wait times, faster transactions, and the ability to focus government resources on higher-risk targets.

Key Facts

Table C-17: Key facts of Case study on CBP Trusted Traveler Program

What?	• Expedited clearance for pre-approved, low risk travelers entering the United States • Fingerprint and photograph utilized to confirm identify • Biometric matching 1:few as a gallery of photos of inbound passengers each day is utilized
Where?	• 75 U.S. POE, including 15 preclearance airports
Customer process steps:	• Passengers enroll online and are approved after CBP reviews information, conducts interview, and validates biometrics

	• At a kiosk in Federal Inspection Station (FIS), enrolled passengers have their fingerprints and/or picture taken at the automated border kiosk • Transaction receipt is presented to CBP Officer at exit control area
Who?	• CBP and DHS are responsible for program development and implementation • Participating airport partnerships required for facility implementation, including enrollment centers, signage and other marketing support • Enrolled passengers
Why?	• To fast track border crossing procedures for individual travelers who are deemed low risk
How? Technology used?	• Identity as a Service - Centralized - Third-party model • Global Entry® kiosks contain camera and fingerprint scanners to obtain biometric tokens to compare against • Applicant biometrics (fingerprints) are stored in the DHS Automated Biometric Identification System (IDENT); facial photographs maintained by GES
Enrollment / Digital Identity creation and verification	• Voluntary program with multi-step application process including an in-person interview
Verification of identity how?	• Facial and fingerprint biometric is collected when completing in-person interview at Global Entry® enrollment center • Fingerprints taken at Global Entry® kiosk are matched against those on file (the kiosks use four fingerprints from one hand to validate who you are) • Facial biometric is matched against a gallery compiled from CBP's Automated Targeting System (ATS) or Unified Passenger Module (UPAX) system
For?	• Pre-approved low-risk air travelers into the United States who are U.S. citizens and lawful permanent residents, and foreign nationals of certain countries

Introduction

Designed to provide quick, easy, and convenient processing, the *Global Entry*® program is a CBP program that allows for expedited clearance for pre-approved, low-risk travelers upon arrival to the United States. *Global Entry*® is designed to reduce the time required for travelers entering the United States through the passenger verification process. Similar programs include SENTRI and NEXUS.

How Does it Work?

Before the Passenger Journey

With this voluntary program, individuals submit an online application on CBP's cloud-based Trusted Traveler Program (TTP) website (formerly Global Online Enrollment System) and provide personal information such as name, address, date of birth, place of birth, country of citizenship, travel history,

employment, and other pertinent information (Department of Homeland Security, 2008). Applicants also pay a nonrefundable fee. Information collected through the online application is deposited into the GES as the system of record for CBP trusted traveler programs. Personal information is maintained in a Privacy Act system of records.

Applications are reviewed by CBP and information is run through criminal and other government databases. Once conditionally approved, the individual goes to one of over 100 enrollment centers to provide fingerprints and facial photograph along with native documents (e.g., passport, proof of residency) for review by CBP. Applicant biometrics are stored in the DHS IDENT. Alternatively, passengers are also encouraged to complete Enrollment on Arrival, launched in July 2017 and currently offered at 41 airports, to reduce the burden on enrollment centers. Enrollment in Global Entry® is valid for five years.

Applicants whose applications are rejected may seek redress under one of three methods, including via the enrollment center, DHS Traveler Redress Inquiry Program (DHS Traveler Redress Inquiry System), or CBP Trusted Traveler Ombudsman. Individuals may request information about their records in the GES/TTP System. Redress is available for U.S. citizens and lawful permanent residents through requests made under the Privacy Act.

Each trusted traveler is vetted daily through a "24-hour vetting" process against various databases, including Treasury Enforcement Communications and terrorist data sets (U.S. Government Accountability Office, 2014). Treasury Enforcement Communications is designed to be a comprehensive enforcement and communications system that enables CBP and other agencies to create or access lookout data when (1) processing persons and vehicles entering the United States; (2) communicating with other computer systems, such as the FBI's National Crime Information Center; and (3) storing case data and other enforcement reports.

The Passenger Journey

When a passenger enrolled in Global Entry® books an international trip, the passenger adds the trusted traveler membership number to the reservation. Upon reaching CBP immigration either upon arrival into the United States or at a Preclearance facility abroad, passengers are directed to a dedicated Global Entry® area. Automated kiosks are located in the FIS area of each participating airport.

In the legacy process, a passport or U.S. permanent resident card is inserted into the document reader (Department of Homeland Security, 2009). Fingerprints are scanned at the kiosk and compared to the fingerprint biometrics on file to validate identify and confirm program membership (four fingerprints are used for validation). Individuals are also prompted for a digital photograph and must answer several customs declaration questions. A transaction receipt is printed and presented to a CBP Officer at the exit control area.

Starting in June 2018 and currently active at over 15 airports, a digital photograph is taken as the only means to confirm identity (Boyd, 2020). No passport scan is required, and no customs questions are presented to the traveler. The facial biometric is matched against a gallery compiled from CBP's Automated Targeting System (ATS) or Unified Passenger Module (UPAX) system.

Retention and Storage

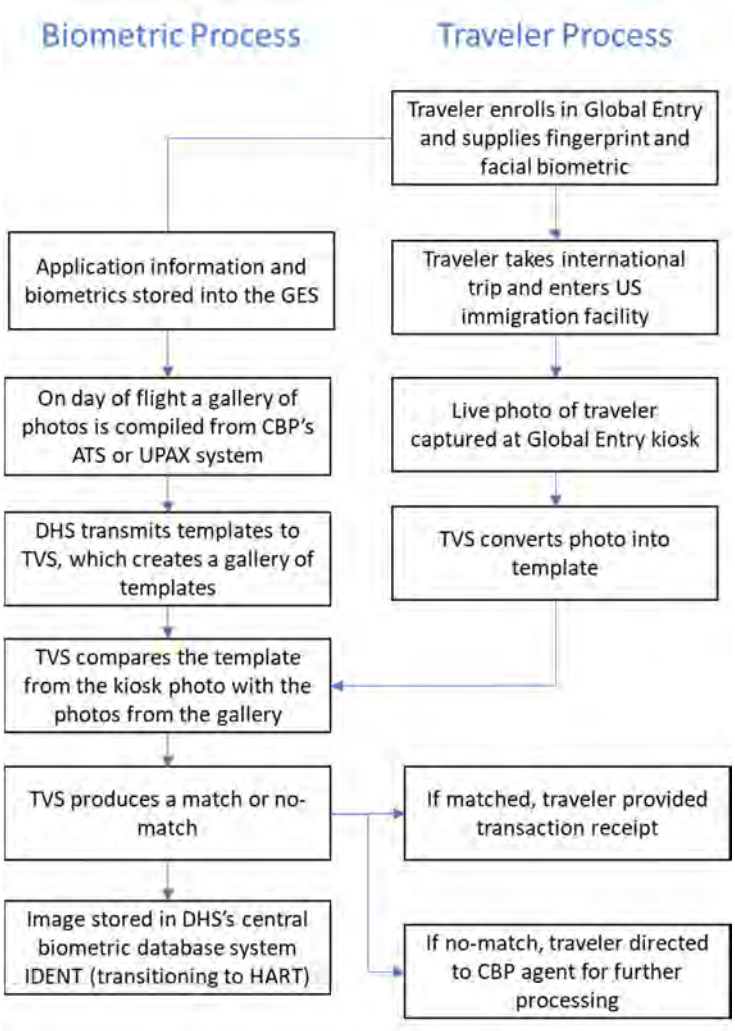
The digital photographs taken at the kiosk are saved to the DHS IDENT, which the agency is the process of transferring to a new, cloud-based Homeland Advanced Recognition Technology (HART), system (Boyd, 2019). Image data is deleted three years after a participant abandons their membership or three years after their five-year Global Entry® membership expires without being renewed.

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

System Specifications

With 1:N matching, TVS compares a live photo of a traveler against a gallery of other traveler photos (U.S. Government Accountability Office, 2020). The stepwise process aligning the traveler process with the TVS matching process is shown in Figure C-1.



Source: U.S. Department of Homeland Security

Figure C-38: Stepwise process of TVS enrollment and at an airport

Stakeholders and Responsibilities

CBP is the largest stakeholder as the agency is primarily responsible for program development and implementation. Airports and passengers also serve as important stakeholders. Passenger participation is required to make the program successful. Airport coordination with CBP is required to ensure that the FIS

facilities are designed and operated efficiently. This includes facility modifications and electrical connections required to accommodate the Global Entry® process.

Case Study Review

Benefits

Global Entry® benefits passengers, CBP, and airports. A 2018 CBP study found that Global Entry® reduced wait times by more than 70% with more than 75% of Global Entry® passengers being processed in under five minutes. This translates to an average savings of about seven minutes. Feedback from passengers has been overwhelmingly positive as on the average day, 10% of international air travelers use Global Entry® kiosks (U.S. Customs and Border Protection, 2018). In the first 10 years of Global Entry®, membership has grown to over 5.4 million members with another 2 million enrolled in either NEXUS or SENTRI. The successful growth in Global Entry® enrollments can be attributed to third party participation by airlines and credit card companies, among others. While most airlines do not offer this benefit directly to their top-tier passengers anymore, airline co-branded credit cards as well as those offered by American Express, Chase, and others include reimbursement of the Global Entry® application fee as card perk.

For CBP, Global Entry® allows the agency to identify low-risk travelers so that the focus can be placed on other unknown and higher-risk travelers. It also accomplishes CBP's strategic goal of facilitating legitimate trade and travel while securing the homeland and works toward the Title 8 USC., Section 1365b mandate which requires that DHS operate a biometric entry and exit system and that it integrates registered traveler programs into this system. From an airport perspective, Global Entry® allows for higher throughputs to be achieved in the same space and provides a customer service boost to passengers.

Responses from Customers

Global Entry® generates "overwhelmingly positive comments," John Wagner, the former Deputy Assistant Commissioner for Field Operations stated publicly. Wagner has also stated that many of the comments resonate with "Holy cow! The government did something right." Positive responses from passengers revolve around shorter lines and speed of processing. Greeley Kock, the executive director of the Association of Corporate Travel Executives, wrote, "No lines, and in less than two minutes I'm through Immigration. The longest I ever waited in line was 30 seconds."

System Specifications Review

Biometric tokens have an extremely high match rate, but occasionally issues do arise. About 3% of passengers do not have good readable fingerprints, so a match cannot be made at the kiosk. These failed matches can be processed with front-of-the line privileges with a live CBP agent, however. Additionally, the fingerprint readers and cameras occasionally fail on the kiosks, which also require manual processing by a CBP agent.

Fall Back Options

Enrollees are not required to use the facial recognition program at those airports where it is offered and can instead opt to use the passport and fingerprint method, which will remain available. Any technical or processing issues at the Global Entry® kiosk are solved with a CBP officer by giving the passenger front-of-line privileges to the next available officer. Additionally, since this is a voluntary opt-in program, passengers do not have to participate. The traditional immigration process requiring a physical document check with a CBP officer is still provided in the inspection area.

Concerns

Privacy concerns over the storing and sharing of biometric data have been expressed. To address privacy concerns, a Privacy Impact Assessment (PIA) update was completed in January 2020 (Mongin and Dansiek, 2019) to assess the privacy impacts of (1) updates to the existing Global Entry® kiosks to use cameras and facial recognition technology provided by CBP's TVS; and (2) the use of photographs collected at the Global Entry® kiosk, rather than the collection of travel documents and fingerprints, to verify traveler identity. The update addressed three risks:

- The risk that the biometrics CBP uses will be used for purposes inconsistent with the original mission is mitigated by the fact that associated photos of Global Entry® travelers are stored in IDENT and may be available to authorized IDENT users for a variety of purposes, which DHS reviews and approves prior to granting access to the system and that CBP owns and operates all Global Entry® kiosks.
- The risk that individuals may not know how CBP will use the photos is mitigated by Privacy Notices on the kiosk home screen, Global Entry® website, visible signage at the FIS, and tear sheets at the FIS.
- The risk that TVS retains user information longer than necessary is mitigated by the fact that TVS does not retain images of travelers once their identities are verified by TVS.

In 2018, an additional concern noted in an Office of Inspector General report, stated that there could be a potential exploitation of Global Entry® receipts at the exit control area due to failed authentication by the CBP officer (U.S. Customs and Border Protection, 2019). This was determined not to be a significant concern.

Lessons Learnt

In talking to stakeholders involved in Global Entry® implementations, the biggest hurdle that impacted the success of a Global Entry® implementation was the placement of the kiosks. Kiosk placement was important to ensure that access and use of the technology are self-intuitive to the user. It also required stakeholder ambassadors present to assist as necessary and to resolve kiosk issues so that the technology is properly utilized by the customer and system issues resolved or reported timely. Some airports, for example, initially placed kiosks on the jet bridge or in the sterile corridor leading to the FIS. Other airports placed kiosks in entry passages to the FIS. Each terminal design represented a different challenge regarding correct placement and flow, even with new construction.

Additionally, the backend of any technological solution needed to tie into the CBP vendor to exchange data. The initial deployment was biometric and photo-capture. CBP has since progressed with facial recognition technology and matching photograph and biometric in a "one-to-few" against the Advanced Passenger Information System (APIS) manifest.

While most of the challenges were associated with facility constraints, stakeholder willingness to invest in Global Entry® as a process was an unforeseen challenge. Some airports initially declined the opportunity to serve as a pilot site, while others like IAH and IAD quickly agreed. These initial partners helped identify and rectify some of the challenges that were experienced during the initial implementations.

Findings and Trends

Findings

The Global Entry® program provides an ability for airports to safely and securely facilitate international air travel for citizens of select countries. The process of vetting pre-approved travelers in advance of their

trips is a low-risk solution which streamlines the passenger verification and screening processes. By pre-approving low-risk travelers, CBP can focus their resources on higher-risk targets. The biometric implementation also reduces touchpoints and increases the throughput of the facility, which can be beneficial to capacity constrained airports.

Future Situation and Broader Implementation

Global Entry is in the process of upgrading the passenger verification process at airports from fingerprint biometrics to photograph biometrics at all 75 U.S. POE. Global Entry® is currently open to U.S. citizens, U.S. nationals, U.S. lawful permanent residents as well as foreign nationals from 15 countries. Additionally, participants of NEXUS and SENTRI trusted traveler program are allowed use of the Global Entry® kiosks. The program is expected to continue to expand to include additional foreign nationals and passenger subsets in order to increase the population base of low-risk travelers. Finally, Global Entry® can be expanded to include additional POEs including general aviation facilities.

Trends Identified

This case study illustrates two of the key trends in biometrics: (1) identity verification solutions, and (2) emerging global standards.

Global Entry® relies on the TVS to compare biometric images of travelers using kiosks with the database of biometrics provided at enrollment. TVS is an identity verification solution and not mass surveillance of passengers entering the United States This is especially true since these trusted travelers volunteered to provide their biometrics in exchange for travel and processing privileges.

Global standards are changing, and passport-free travel is a key example. Global Entry® contributes to the emerging global trend of passport-free travel because the immigration process at the kiosks is transitioning to a system where the facial biometrics replaces the need to scan the passenger's passport. As Global Entry® continues to evolve it is anticipated that there will be no need to show a passport during the immigration process.

APPENDIX D

Case Study: Seattle-Tacoma International Airport and Designated Aviation Channeling (SEA)

Executive Summary

Pursuant to the Aviation Transportation Security Act and implementing regulations, TSA requires all employees of airport authorities, airline carriers and other airport stakeholder employees who require unescorted access to secured areas of an airport to submit an application and be approved for a SIDA badge (Aviation Transportation Security Act). The vetting process screens an applicant's information against federal criminal and immigration databases to determine whether the applicant is a threat to transportation or national security. Starting in 2012, TSA authorized the use of DAC services by airport operators and aircraft carriers through which applicants submit their applications which include both biographic and biometric data (i.e., fingerprint records) to TSA (and the FBI) (DHS Inspector General, 2013) (Pilli, 2020).Telos ID is one of two DAC service providers authorized by TSA and offers its DAC services at Seattle-Tacoma International Airport (SEA) (Airport Technology, 2020).

Key Facts

Table D-18: Key Facts on Designated Aviation Channeling at SeaTac

What?	• DAC services are used by airport operators nationwide • Telos ID is one of two competitive "vendors" of services to airport and aircraft operators and stakeholders of DAC services for vetting of employees seeking unescorted access to secured areas of the airport (TSA requirement) (Ayers and Lucini 2012). • The application compiled by Telos includes fingerprints (straight or rolled) (matching is 1:1) and if a facial image is provided the matching for facial image is 1: many. Fingerprints are required, and occasionally photos are provided to verify identity (e.g., in the case of a name change).
Where?	• Telos DAC services are currently at 90 airports in the United States including SEA

Customer process steps:	• At the request of airport stakeholder, applicant submits biographic and biometric data (fingerprints and on occasion a photo) to Telos (Telos ID, 2020). • Telos verifies the application information (e.g., checking employment and education references), ensuring completeness, and properly formatted. • Application is electronically transmitted in an encrypted format to TSA. • TSA conducts a review of various government databases as a Security Threat Assessment and FBI runs the fingerprints for a criminal history check (otherwise known as a Next Generation Identification (NGI) check). • Results of approval or denial are provided to Telos but more detailed information is only shared with airport operator or aircraft carrier. • Badge pick-up by applicant (airport employee) but if negative results returned, airport or aircraft operator manually adjudicates the case.
Who?	• Telos under contract with SEA provides DAC services, in accordance with Airport Security Directive and pursuant to TSA requirements, to Airport staff (airlines, TSA, ground operations, airport management/ operations, other airport stakeholders/suppliers) • In the near future, Telos DAC services will also be used for CBP e-Badge applicants (Burriesci, 2020) (Hamilton, 2020).
Why?	• SIDA badge required for all employees whose duties require unescorted access to secured areas of the airport. • Use of DAC biographic and biometric process creates a more efficient and secure vetting procedure, saving airport stakeholders time and money and standardizing the TSA/FBI mandated procedure, and minimizing TSA's administrative oversight to two DAC providers.
How? Technology used?	• The main DAC service used by SEA is the secure web-based application which allows SEA to collect applicant information and packaged it according to TSA and FBI specifications. • SEA uses the DAC services by integrating it with its identity management (IdMS). SEA IdMS software is integrated with mobile/static fingerprint scanners, cameras, and software provided by Telos (Curtis, 2020). • Telos electronically transmits the application and the fingerprints in an encrypted format. No specific technology is required for transmission, but fingerprint quality must meet FBI specifications.
Enrollment / Digital Identity creation and verification?	• DAC services, while not mandatory, are provided in support of the SIDA badge application required by TSA.
Verification of identity how?	• Applicant provides two forms of government-issued identification and additional government issued authorization (e.g., immigration forms such as an I-9), if warranted. Telos conducts checks for application data pertaining to employment and education history.
For?	• DAC processing is for issuance of SIDA badge for airport employees seeking unescorted access to secured areas within the airport. (Exceptions exist for Federal, state or local government employees and for certain other

individuals, previously vetted through TSA/FAA, authorized by the airport operator due to continuous employment.)

- In the near future, applicants seeking unescorted to CBP's FIS area can apply for the e-Badge using Telos DAC services.

Introduction

In the case of an airport using DAC vendor services, the process for a SIDA badge begins when the airport employee submits the application, supported by authorized "signers" (or endorsers), to the DAC vendor. Telos as a DAC service provider takes and includes the applicant's fingerprints in the application, and in some cases additional documentation (e.g., I-9 document) (Telos ID, 2020a). The DAC vendor makes sure that the application is complete, properly formatted, and verifies the employment and education information provided. The application is accompanied by fingerprints (and a photo on occasion) which is electronically submitted to TSA for a Security Threat Assessment which TSA in turn transmits to the FBI for a Criminal History Records Check (CHRC) (Badgley, 2020). The background check compares the applicant's information against federal criminal and immigration databases to determine whether the applicant is a threat to transportation or national security. If the application is approved by TSA, the results are provided to the airport operator and a badge is issued which not only authorizes access to secured areas of an airport, but depending on the biometric technology in use at the airport and by the employer, could be scanned to record reporting for duty for timekeeping purposes or to physically enter secured entry through doors into restricted areas.

How Does it Work?

Before the Passenger Journey

The DAC service consists of various programs and systems used to collect applicant information. Primarily, SEA uses the DAC interface, which is a secure, web-based application hosted on servers managed by Telos. The backend system is a database used to house collected information for the purpose of transmitting to TSA for STA vetting and CHRC submissions to FBI.

SEA uses the DAC services by integrating it with its identity management (IdMS). SEA IdMS software is integrated with mobile/static fingerprint scanners, cameras, and software provided by Telos.

It is important to note that the DAC systems are subject to TSA MD 1400.3 IT Security, as well as Attachment 1 – TSA Information Assurance Handbook. The DACs must also comply with DHS specifications regarding the safe handling of Sensitive Security Information, personally identifiable information (PII), and sensitive personally identifiable information (SPII).

Given that the DAC systems contains SPII, the information systems and devices on which they are installed must be approved and granted authority to operate by DHS and TSA.

The Passenger Journey

At request of the airport, the applicant submits the application form with biographic and biometric data (fingerprints and if relevant a photo) to Telos for electronic transmission to TSA for SIDA badge for access to secured areas of an airport. Telos performs the following functions:

- Ensures biographic data within the application is complete and accurate and accompanied by FBI required fingerprints.
- Verifies biographic information for employment and education history (including identifying unexplained gaps) by contacting listed references, employers, educational institutes, etc.

- Verifies identity, as part of the application, of a driver's license or other identity document (e.g., passport number and country of issuance, if applicable).
- Ensures data integrity by eliminating duplicate or erroneous data.
- Automates fingerprint web capture at a designated badging office, airport operator Human Relations office or a mobile operation. Telos provides capture devices (fingerprint scanners, cameras).
- Provides capability to attach documentation, such as copies of immigration records, e.g., Permanent Resident Card, Employment Authorization Document, Form I-94, etc.
- The software allows all the information to be packaged into a format compliant with the FBI Electronic Biometric Transmission Specification.
- Encrypts the transmission and sends to TSA for its STA and background check and to FBI for a criminal history record check via a Next Generation Identity (NGI) check. Telos transmits the application via a secure connection, over secure connections utilizing Secure Sockets Layer over the Simple Object Access Protocol, or HTTPS).
- Transmits the fee to TSA.
- TSA conducts a review of various government databases for the STA and the FBI runs the fingerprints for a NGI check.
- Results of approval or denial are provided to Telos but more detailed information is only shared with the airport operator or aircraft carrier.
- The employee picks up a SIDA badge if approved, but if negative results returned, the airport operator manually adjudicates the case.

Retention and Storage

Telos saves both biometric and biographic data in the application in accordance with TSA Privacy Act System of Records Notice (SORN) requirements for STA records. It is important to note that the DAC system stores this data in accordance with TSA MD 1400.3 IT Security, as well as Attachment 1 – TSA Information Assurance Handbook. In addition, the DAC system must comply with other federal and DHS data retention policies.

The data storage process and database structure are Telos ID proprietary system designs. TSA only holds the DAC to its requirements for the input to and output from the DAC system. These requirements are embodied in the above-mentioned TSA / DHS handbooks and policies.

Per Telos, it adheres to privacy requirements set by DHS/TSA for DAC service providers in support of TSA requirements of the Privacy Act of 1974 governing the collection, storage and retention of TSA records. TSA indicated that for SEA state privacy laws may apply as well.

With respect to TSA, TSA retains information (fingerprints and biographic information) for one year after an individual's SIDA privilege is no longer valid. In addition, for those individuals who may originally have appeared to be a match to a government watch list, but are subsequently cleared as not posing a threat to transportation or national security, information will be deleted or destroyed seven years after completion of the STA, or one year after any credential or access privilege granted based on the STA is no longer valid, whichever is longer. Information contained in the subject database on individuals that are actual matches to a government watch list or otherwise pose a threat to transportation or national security, will be deleted or destroyed 99 years after completion of the STA, or seven years after TSA learns that the individual is deceased, whichever is shorter.

For airport operators, per TSA regulations, 49 CFR 1540, each operator must retain the STA application and supporting documents (verifying identity and work authorization) for 180 days following the end of the applicant's service to the operator.

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

System Specifications

There are no specifications for the DAC system design for hardware, software, encryption, cameras, etc. but fingerprint quality must meet FBI requirements.

Stakeholders

Airport operators and aircraft operators are the key stakeholders, although TSA oversees the vetting process to ensure compliance with law. In 2020, at some 78 airports nationwide, CBP began receiving from TSA those applications from applicants seeking unescorted access to the CBP FIS area, which CBP vets through its UPAX systems (a multi-record system with law enforcement information, to include criminal, civil and immigration data) (Calixte, 2020).

Case Study Review

Benefits

According to the Telos website, Telos ID's DAC services improve data integrity, increase the efficiency of credentialing operations and reduce costs. DAC services enable submissions of workers' biographic and biometric data to conduct background checks, including subscriptions to the FBI Record of Arrest and Prosecution Background (Rap Back) program, for individuals working in secured areas of U.S. commercial airports (TSA, 2018). Stakeholders have experienced a reduced administrative burden associated with operating a badging office.

Those stakeholders that sign up for the Rap Back) subscription services achieve significant savings since they no longer are required to pay for and obtain an FBI criminal history check every two years. DAC services also assist in managing insider threats with FBI’s Rap Back, which provides employers with notice of an employee's criminal and arrest records by receiving alerts in real-time from the FBI if there are any additions to an employee's FBI records.

- DAC can also integrate with other users’ workforce systems to meet additional badging, physical security and personnel administrative needs.
- DAC Rap Back subscription services allows stakeholders to manage insider threats which provides employers with notice of an employee's criminal and arrest records by receiving alerts in real-time from the FBI if there are any additions to an employee's FBI records.
- DAC services can expedite employee on-boarding with real-time and combined CHRC & STA submissions
- DAC eliminates spreadsheets that can expose PII.
- Frees up federal agency staff from data entry and accelerates processing of applications.

Responses from Airport Operators, Airlines and Stakeholders

According to the SEA representative, in an interview conducted on October 5, 2020, benefits include more efficient processing of some 12,000 applications annually and ensures greater protections for PII.

System Specifications Review (Third-Party or Other)

Telos provides capture devices (fingerprint scanners, cameras) and transmits application via a secure web portal. The scanner that transmits the fingerprints must meet FBI specifications for fingerprint quality. If approved, the applicant picks up the SIDA badge, but if there are negative results, the airport operator receives the details from TSA and manually adjudicates the case.

Fall Back Options

Applications may be submitted as a hard copy manually or by mail.

Concerns

With respect to privacy protections extended to Telos' processing of airport employee applications and related data, Telos maintains biometric and biographic data and Yes/No results of the vetting, but does not receive the actual rap sheets or details regarding a finding that the employee may have disqualifying events/offenses in his/her background. According to Telos, all information is stored in compliance with TSA requirements.

Lessons Learned

According to TSA sources, expanding the use of DAC services to multiple categories of airports has facilitated TSA's oversight role and benefited larger and smaller airports with greater efficiencies to both.

Findings and Trends

Findings

The DAC system promotes greater efficiency for pre-processing of SIDA badge applications for a large volume of workers.

"As an encrypted, web-based solution, Telos ID's DAC services …[and] [i]ts modular design supports each airport's and air carrier's needs, and users can perform multiple functions on one platform."

Both TSA and CBP acknowledged the increased efficiencies and improved speed of application processing through the use of DAC services.

During Phase 1, CBP realized additional efficiencies in the airport employee vetting process for eBadges by "piggybacking" on the DAC services in cooperation with TSA. In the future CBP intends to collect biometrics by requesting and receiving the set of fingerprints included in the application transmitted to TSA and the FBI.

Future Situation and Broader Implementation

Telos has indicated that its services could extend to Secure Flight vetting of passengers (but since Secure Flight is an assessment based on biographic data, it would not likely involve biometric data collections).

In the future, CBP intends to collect biometrics by requesting and receiving the set of fingerprints included in the application transmitted to TSA and the FBI.

Trends Identified

One emerging trend is the consolidation of the many types of background checks required by the U.S. Government into a single application and process. The result is greater efficiencies in the vetting process for airport employees requiring access to secured areas at commercial, federal, and joint-use facilities.

DAC services are exploring and implementing quality integrated solutions such as integrating with customers' workforce systems to meet additional badging, physical security and personnel administrative needs.

Currently, TSA PreCheck™ enrollment is conducted by IDEMIA. Starting in late 2020, Alclear, LLC and Telos will also conduct TSA PreCheck™ enrollments for travelers. One of the challenges to expanded use of DAC services to airport-related functions, is that most of the programs where vetting is a part, use an established enrollment entity.

APPENDIX E

Case Study: Curb-to-Gate Program by CBP and Delta Airlines at Atlanta International Airport (ATL)

Executive Summary

CBP's *Curb-to-Gate Program* is an application of facial recognition with the intent of reducing the number of times passengers must present their form of identification and boarding pass, as well as increasing the reliability and efficiency of both airport border and security officers.

The *Curb-to-Gate Program* led by CBP and Delta Airlines allows passenger to verify their identity in a reliable and more efficient manner through leveraging CBP's TVS:

- At check-in/bag-drop, a real-time photo is sent securely and encrypted to TVS.
- Incoming photo is matched to a biometric template in a pre-compiled library, based on the airline's passenger manifests.
- In case of a positive match, the passenger's ID is verified and the use of facial recognition for the rest of the journey is enabled.
- At bag-drop, security and boarding, the passengers' identity and right to entry/passage is verified using facial recognition.
- For border crossings, an entry/exit record is made in the ADIS.

The benefits of utilizing the *Curb-to-Gate* are: time savings for passengers and airport personnel; lower operational expenditures for airports; optimization of the use of space throughout the airport; and an opportunity for airports to revolutionize the passenger travel experience. Additionally, *Curb-to-Gate* significantly reduces the number of physical interactions amongst airport stakeholders, thereby lowering the probability of transmitting diseases and hazardous pathogens (e.g., Covid-19, etc.). Furthermore, this represents a significant milestone in terms of the power of end-to-end facial recognition and demonstrates the capabilities of biometric software (The Economist, 2020).

Key Facts

Table E-19: Key facts of case study on Curb-to-Gate program by Delta

What?	• Facial biometric template matching, • 1:few biometric matching • Pilot project led by CBP

Where?	• Maynard H. Jackson Jr. International Terminal and Concourse F at ATL Atlanta, • leased by Delta
Passenger process steps:	• “Curb to gate” program (to be expanded later) • Departures: • Check-in • Bag Drop • Security (TSA) • 15 departure gates • Arrivals: • CBP Immigration Checkpoint
Who?	• CBP led the trials, and found partnership with Hartsfield-Jackson Atlanta International Airport, Delta Airlines and also TSA. The DHS was involved as it manages and oversees access to the biometric information used in CBP’s system. NEC was selected as technology hardware and software provider, when it was the first vendor to meet specific technology requirements. NEC products include the NeoFace Express and NEC Enhanced Video Analytics (Beroukhim, 2018).
Why?	• CBP’s initial goal was to speed up processing using facial data of passengers who have been previously vetted by various system. It was important to not replicate re-vetting everyone, but to use an accurate and reliable system as a "verification" process for passenger identification and boarding. Stakeholders goals included being able to use the biometrics verification process for other non-CBP passenger processing steps, e.g., check-in and replacement of paper boarding passes. The four main goals of CBP are (August report): • Secure - Providing increased certainty as to the identity of travelers at multiple points in the travel continuum; • Simple - Eliminating the need for physical document and boarding pass checks, as well as the collection of fingerprints; • Facilitative - Establishing a clear and easily understood process that will reduce the potential for major “bottlenecks” within the air travel process; and • Compliant - Employing a high integrity biometric entry and exit system that not only increases CBP’s certainty as to the identity of travelers, but also more ably holds accountable those violating terms of admittance.

How?	• Cameras: tablets, mounted, on-a-stick, • Matching live pictures taken at the checkpoint with pre-loaded biometric templates • No collection of biographic data through TVS, pictures kept up to 12 hours • Systems and databases used: • TVS on Virtual Private Cloud (VPC) • Advance Passenger Information System (APIS) • Arrival and Departure Information System (ADIS) • Office of Biometric Identity Management • DHS IDENT • Automated Targeting System-Unified Passenger (ATS-UPAX)
Enrollment / Digital Identity creation and verification	• No formal enrollment, TVS already has access to a large database of foreign nationals' pictures if they have travelled to the United States / applied for VISA or other permits; • DHS Office of Biometric Identity Management
Verification of identity how?	• Facial biometric is collected when applying for a passport/visa or when entry/exit of United States, verification matches biometric template of unique IDs of the pictures on file with a picture taken at the passenger checkpoint which is sent encrypted to TVS
For?	• International flights with Delta or partners AirFrance-KLM, Aeromexico and Virgin Atlantic. • To be expanded to U.S. domestic flights in subsequent steps in the program

Introduction

In the passenger journey through an airport to an international flight the passenger has to present passport and boarding pass multiple times before getting on the plane. Burdened with carrying cabin luggage, worrying about making their flight and navigating the airport, this requirement has passengers fumbling with important documents and only adds to the often stressful experience.

This application of biometrics aims to take away the need to repeatedly present ID and the boarding pass, limiting it to one time at the start of the journey at the airport (Harper, 2018). It also aims to greatly increase the security and efficiency of border and security officers. More recently, this application also provides for a largely touchless journey, safer for all stakeholders traveling through and working at the airport.

This is achieved by CBP, which leverages their TVS to provide secure, efficient automated biometric identity verification at the checkpoints for Delta (Future Travel Experience, 2019) and the airport as well as for PreCheck™ (TSA, 2020) eligible passengers at the TSA checkpoint. Hartfield-Jackson International Airport in Atlanta also hosted one of the earlier versions of TSA's Biometric Authentication Technology trials, but this is not covered in this specific use case review. Note that an actual passport is still necessary for international travel for identification at the destination countries.

TVS is a cloud-based facial biometric matching service that utilizes U.S. government databases of pictures on file of U.S. citizens as well as foreign nationals who have in the past traveled to the United States. For new travelers, enrollment for Delta's service is done at the check-in kiosk or airline counter.

Storage and retention of pictures sent to the TVS system is minimal, although it builds on pre-existing U.S. government databases which keep records of foreigners for longer periods of time. For U.S. citizens, pictures are retained for no more than 12 hours in the TVS system before being purged. CBP temporarily

retains facial images of non-immigrant aliens and lawful permanent residents for no more than 14 days. For certain other foreign nationals, pictures after matching are sent to CBPs IDENT database update pictures on file and kept there for a maximum of 75 years. For both U.S. citizens and foreign nationals, an entry or exit record is stored, but it contains only the biographic information found in a passport, no pictures are in those records.

Furthermore, no pictures are stored on the local camera-devices themselves by NEC. Airlines and airports are prohibited to keep pictures of their passengers. The accuracy of the matching is very high (99%) and the sending of data is regarded protected due to the secured connection between the NEC systems and TVS, and due to the encryption of the pictures before they are sent.

The main benefits include significant time savings for passengers, which can lead to space and resource savings for airports and airlines, having to utilize less staff, place less counters and thus save space. The system architecture is technology agnostic, and thus allows for multiple hardware suppliers to develop specific solutions for airports.

How Does it Work?

Before the Passenger Journey

Several databases of the U.S. government are essential elements of the workings of the system behind the *Curb-to-Gate* program at Atlanta Hartfield Jackson by CBP. CBP's TVS and its API is the system that interacts with private third parties' devices. The most important databases are briefly introduced here:

- HART (follow up system for IDENT) – the HART System is a centralized DHS-wide biometric database that contains limited biographic and encounter history information. The system will replace IDENT for the storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions, and other administrative uses.
- IDENT was the DHS database for Automated Biometric Identification System has, since 2003, collected pictures, fingerprints and basic biographic data (e.g., passport information) of non-U.S. citizen photos having travelled to the United States (THALES, 2021).
- Department of State (DOS) database of passport photos and visa applications
- APIS - a collection of all passenger information flying from U.S. airports, supplied by the airlines
- ADIS – CBP's system keeps track of all entry/exits of U.S. citizens as well as foreign nationals, relating to visas
- FBI NGI - FBI's Next Generation Identification system for fingerprints, formerly known as the Integrated Automated Fingerprint Identification System (IAFIS)
- ATS-UPAX - Module system is the decision-support tool operated by DHS CBP and which combines data from numerous U.S. databases for passenger vetting
- TVS VPC – the TVS Virtual Private Cloud is the firewalled virtual network on which the TVS system runs.

The TVS database and software, is hosted in the United States on Amazon Web Services dubbed the Gov Cloud, a version of Amazon Web Services that is designed to be able to host sensitive data, regulated workloads, and address the most stringent U.S. government security and compliance requirements.

Prior to the passenger journey, CBP's TVS system uses information from passenger booking information in the APIS database to create traveler manifests (lists) of passengers that are expected to travel that day in its VPC. The TVS system pre-loads verified biometric *templates* of the passengers' pictures into the traveler manifests.

A biometric *template* is a digital representation of a biometric trait of an individual generated from a picture and processed by an algorithm. The template is usually represented as a sequence of characters and numbers comparable to a long string of letters and numbers.

The source for the biometric templates is DHS' decision-support tool called the ATS-UPAX, from which existing pictures are downloaded and converted into biometric templates. The pictures downloaded from ATS-UPAX are not stored in the TVS system.

ATS-UPAX sources pictures from multiple databases, such as the DHS' database IDENT, as well as the Department of State's database of passport and photos of both U.S. citizens and foreign nationals, but potentially from several other intelligence databases.

The Passenger Journey

1. At check-in/bag-drop: a real-time photo is made by NEC hardware (NEC, 2020) with integrated cameras and sent securely and encrypted to the TVS matching service through the API.
2. In the TVS cloud service (VPC), the incoming encrypted photo is matched to the biometric *templates* in the relevant traveler manifest.
3. If a positive match is made, the passenger is verified and the use of facial recognition for the remainder of the passenger journey is enabled (Today.com, 2020). With a positive biometric match within the right manifest, the passenger record in the manifest is updated from "reported" to "confirmed".
4. At subsequent passenger process touchpoints (bag-drop, security and boarding), the passenger's identity and right to entry/passage is verified using facial recognition and matched with the corresponding specific traveler manifest (Baran, 2020).
5. In case of the border crossing, an entry or exit record consisting of only the biographic information from the passenger's passport is created or added to the pre-existing record and retained in the ADIS.
6. In case of no match or if the passenger wishes to opt-out of this process, a manual verification of the identity is done at each checkpoint. Pursuant to CBP inspection, the manual ID check is followed by a check of eligibility to enter/exit the United States (Murph, 2018).

Retention and Storage

Storage and retention of pictures sent to the TVS system is minimal:

- No pictures are stored on any of the airports' and airlines' devices supplied by NEC. These only take the picture, encrypt the file and immediately send it to the TVS through the API over a secured connection. Airlines and airports are prohibited from keeping pictures of passengers.
- For U.S. citizens, pictures are kept up to 12 hours in the TVS system (Patterson, 2018).
- During the initial trial period, pictures of both U.S. citizens and foreign nationals were kept in the ATS-UPAX for up to 14 days, for the evaluation of the technology. This is no longer the case.
- For foreign nationals, pictures are sent to CBPs IDENT database after matching to keep the records' pictures up to date and current. These records are kept for a maximum of 75 years.
- For both U.S. citizens and foreign nationals, an entry or exit record is stored in ADIS. This record contains only the biographic information found in a passport; no pictures are in those records.

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

Stakeholders and Responsibilities

CBP took leadership of the (pilot) project, partnering with Delta, ATL, TSA (TSA, 2020a) and NEC to trial the TVS system on broader application use over multiple passenger checkpoints. This *Curb-to-Gate* trial follows several earlier pilot programs building upon CBP's earlier Departure Information System Test (DIST) pilot and Departure Verification System (DVS), both in 2016.

Stakeholders

The main stakeholders of the *Curb-to-Gate* program include Delta Airlines, Hartsfield-Jackson Atlanta International Airport, TSA, NEC and via Delta Airline; other SkyTeam partner airlines (AF-KLM, Aeromexico, Virgin Atlantic) (Mutzabaugh, 2018). CBP in an interview reiterated the importance of carrier buy-in from the onset, and throughout the development and period of the program.

Responsibilities and Governance

CBP was the main driver and the main requirements of the pilot were dictated by the CBP. After various collaborative discussions with several organizations, CBP took the lead on moving the project forward with key officials to establish a strategic pilot project. As the task and goals were outlined and agreed upon, subject matter work groups were formed (e.g., data systems and information technology) and decided on protocols. For CBP, Delta Airlines and the Atlanta Airport, officials were designated and provided guidelines and project goals.

Timeline and Planning

According to CBP, multiple timelines were based on individual workgroups task capabilities. Weekly updates were established as the working groups progressed with the pilot projects, implementations, evaluations and next steps.

Procurement and Vendor Selection: NEC

NEC was the first vendor to demonstrate the capabilities to meet the biometrics facial technical requirements for all the vested partners. Delta volunteered to pilot the biometrics process at their Atlanta airport operational hub.

Case Study Review

Benefits

For the passengers, a reduction of an average 7 to 9 minutes is accomplished when adding up all the time savings at the passenger checkpoints that utilize the facial recognition technology (Burt, 2020) (Linder, 2020). As well, passengers will not have to reach for and hand over their passport and boarding pass on several occasions, making the passenger checkpoints much less of a hassle, as well as preventing possible transmission of communicable diseases through the closer contact and interaction.

For the airport, airline, TSA and CBP, the faster processing times through checkpoints mean a possible reduction of staffing, space and other resources required with a similar throughput. This allows for expansion of throughput in the current assigned areas or freeing up of space for other uses. More specifically, CBP reported the following benefits in their August Report of 2019:

Table E-20: CBP Strategic Benefits

Improved business process	• An enhanced entry/exit business process that integrates within existing government and stakeholder business models.
Stronger relationships	• An environment that allows CBP and stakeholders to work together and that allows for further airline modernization.
A positive impact on inbound security and throughput	• Enhanced inbound security and more efficient throughput.
Improved traveler experience	• An overall enhanced traveler experience.
Improved data integrity	• Utilize DHS enterprise biometric repositories provided to ensure accurate biometric identity records.
Enhanced visa overstay enforcement	• Support the ID and tracking of visa overstays by closing information gaps associated with current exit reporting capabilities allowing for improved enforcement action.

TVS is technology-agnostic and comes with a range of tools (the API) for integration with stakeholder/partners technology for capturing facial biometrics. This means that other suppliers of the hardware and software (NEC) can be chosen or developed in parallel.

The 1:few matching greatly improves matching speed and accuracy over the use of other large U.S. databases.

With respect to privacy, the pictures are encrypted before uploading to the cloud where the picture is transformed to a biometric template: only the unique IDs are stored for a short period of time. Pictures uploaded by the airline/airport are compared to the biometric templates, and only a positive/negative match is returned. This means no actual pictures are stored in the TVS database.

The process and flow of information is well defined, for sharing of pictures for traveler verification as well as other information flows, as it is analyzed by the Office of Biometric Identity Management in their Privacy Impact Assessment (PIA). These PIA reports are available to the general public to read, greatly benefiting the digital transparency of the system.

For the CBP, the automated process lets the CBPO's (officers) focus on the high-risk travelers, or even the undocumented travelers, which adds to the border protection mandate of the CBP.

Responses From Passengers

Feedback from passengers has been very positive, only 2% opted out of the process in passenger surveys performed during the pilot project, 93% of customers had no issue usging the technology at boarding (Steele, 2019), and 72% found it more preferential than normal processes (Yamanouchi, 2019) (Yamanouchi, 2019a).

System Performance and Specifications Review

According to the CBP report of August 2019, attained online via (Department of Homeland Security, 2020), the accuracy of the facial recognition matching was in the high 90s and that improvements in the technology have led to much lower false positives and false negatives. The matching rate is running at 97 to 99 percent currently, according to CBP as can be seen in the below results table from the August Report, 2019.

Table E-21: Facial Recognition Performance Report - August 2019

Modality	Number of Locations	Flight Count	Number of Travelers	Technical Match Rate
Air Entry	11	446	34,716	99.2%
Air Exit	16	92	11,545	97.6%
Air Preclearance	4	45	6,559	99.4%

The estimated false positive rate based on the internal CBP analysis is .0103 percent, which is within the established Key Performance Indicator (KPI) target of less than 0.1 percent.

Fall Back Options

For those passengers who do not wish to take part in the *Curb-to-Gate* program, currently about 2% (Pitrelli, 2020), there are opt-out possibilities. This will mean having staff do manual verifications of identity, as well as boarding pass/passport checks along the passenger journey.

As with every computer system, power cuts or other system integrity failures can seriously hamper the operation of the passenger identity vetting system. Luckily, with the main system running in the cloud, this process can be hosted in a multitude of physical locations, thus protecting from interruption. Similarly, mobile devices in the airport used at the passenger checkpoints can run software independently and on battery power, maintaining an encrypted connection, so that in event of a loss of power, these devices can continue operation. The latest update from the traveler manifest should allow for continued operation, at least for those that are positively matched in the TVS system. Manual ID verification in the case of a negative match are more difficult at CBP as these require connection to DHS/DOS to for formal ID queries.

Concerns

Media attention has raised concerns on the implementation of biometrics in four main categories:

1. Use of technology for (mass) surveillance
2. Privacy
3. Transparency
4. Technology standards

Use of Technology for (Mass) Surveillance

The fear that the technology of facial recognition, if developed, will allow for mass surveillance of public or state, has seen media attention around the world, especially as some countries have implemented just that. The goal of the *Curb-to-Gate* program, and thus its (system) design prevents this capability. CBP specifically states that while TSA is not evaluating the use of facial comparison for law enforcement purposes, it is assessing its use for traveler identity verification as part of its mission to protect the Nation’s transportation systems to ensure freedom of movement for people and commerce. In the execution of the system, there are no means that allow in this case federal authorities to access the camera systems, and all the system does is generate automatic versions of the entry/exit reporting for which CBP already was keeping records.

Privacy

Privacy concerns (Hautala, 2019) for any system that handles biographic or biometrics personal information range from misuse or loss of that information when collected, used or stored. To counter privacy concerns, CBP in the design of the TVS has implemented a Privacy by Design approach to ensure that privacy protections are embedded into its use of facial comparison technology. CBP employs four primary safeguards to secure the data: secure storage, brief retention periods, irreversible biometric templates, and strong encryption during data storage and transfer.

On top of that, CBP has submitted and published a number of PIAs (Office of Field Operations, 2018), on related pilots and programs to the DHS Privacy Office for adjudication and publication. These use the FIPPs to assess and mitigate any impact on an individual's privacy. These principles are rooted in the Privacy Act of 1974 and govern the use of personal information.

One example of the Principles of Privacy by Design is showcased in the case of a data breach. If the TVS database were to be hacked, only the biometric templates that are stored in the database would be susceptible to theft. These are worthless as they cannot be recreated to biometric facial pictures without the software and codes used to make the template in the first place.

Transparency

CBP when interviewed, stressed the need to mitigate privacy concerns with outreach and openness. CBP provides transparency and general notification to the public through program information, such as frequently asked questions, available on the CBP website and the TVS Privacy Impact Assessments (PIAs) and SORNs published on the Department of Homeland Security website. The PIAs and SORNs for the TVS and its predecessor projects explain all aspects of CBP's biometric entry/exit programs, including policies and procedures for the collection, storage, analysis, use, dissemination, retention, and deletion of data.

Technology Standards

System performance highly depends on adequate hardware and software roll out, in which case standards for the technology can protect against malfunctioning, misinterpretation or other issues that may arise. One issue that has gained attention in the media is the reported bias in some demographic groups, as per NIST in 2018. Another worry with facial recognition technologies is that camera images are not of high enough quality, impacting the accuracy of the match.

Because data privacy, protection, and mitigation of algorithmic or operational bias are prime concerns, CBP actively makes improvements while seeking to ensure there are no signs of bias, and engages in a robust public dialogue on appropriate standards. CBP also engages in outreach with privacy advocates, the NIST, and DHS Science and Technology Directorate (S&T) to monitor performance and progress.

Lessons Learned

According to an interview with CBP, several lessons learned were key in the program development, and the continuation of it to next phases. Some key lessons are:

- Initially, there was skepticism and concern with the cost of equipment, programming and training by potential end-users and stakeholders. Through discussions and joint planning, all parties were able to establish and implement mutually beneficial goals.
- Initially, there were various levels of government and private entity scrutiny regarding government biometric and facial data collection and storage. CBP emphasized the importance of not replicating the vetting process and not storing data for privacy reasons. This proved beneficial in further privacy assessments.

- It was important to have the airline and airport approval to access relevant company data and systems.
- It was important to allow subject matter work groups to leverage expertise and focus on the immediate needs by not being too rigid in timelines and process. At times, there was the trouble of visioning the end result among stakeholders, which resulted in some inflexibility. By including willing partners at the operational decision-making table, continued progress was possible and a collaborative effort for a continuous focus on future enhancements was established.
- Ensuring that acquisition groups are in sync with implementation requirements. This expectation management was key for tracking progress and updating timelines for pilot programs.

Findings and Trends

Findings

The development of (federal) national standards (or best practices?) to govern the use of biometrics in facial recognition in verification/identification is considered beneficial for:

- Picture quality and method of sharing, to further improve matching accuracy and speed
- Method of encryption, secure connection, to ensure further protection from digital threats such as hacks
- Use of biometric (templates) regarding capture, use and storage
- Synthesis of lessons learned/recommendations from PIA to further privacy commitments enacted e.g., storage and retention durations
- Information and transparency: Informing users and passengers of system functions and how these work in a campaign to gain trust and dispel the negative media attention.

Starting in 2018, DHS S&T has performed independent biometric analyses using a sample of operational TVS probe and gallery facial images. Based on these analyses, DHS S&T made specific recommendations to CBP including:

1. To ensure that only ticketed travelers are allowed to use TVS for boarding or to increase match thresholds used for biometric exit; and
2. To carry out an exhaustive "Virtual Red Team" analysis to calculate the risk of false matches based on the demographics (age, country of origin, gender) of travelers on individual flights.

Future Situation and Broader Implementation

The successful *Curb-To-Gate* program with Delta Airlines and Hartsfield-Jackson International Airport gave rise to implementation of TVS at numerous other airports in the United States (Steele, 2020). In 2018, the entry process using facial comparison was reengineered and deployed in the air entry environment at 15 airports including four preclearance locations, with plans to expand further in 2019. From recent reports by CBP, next steps for further pilot programs/implementation of the TVS system, the following can be expected in the (near) future:

- Expanding the program to domestic flights in the United States
- Expanding the trial to transferring passengers
- By 2022, CBP's goal is to deploy biometric exit using TVS to the top 20 airports, which account for more than 97 percent of departing commercial air travelers from the United States
- Full certification/integration with Simplified Arrivals and Biometric Entry/Exit?
- Mass implementation: all passenger processes will have the option for use of facial recognition, including all transfers (rescreening and CBP immigration)
- Standard process for CBP and TSA

- Optional opt-out to stay (in separate lane?)
- The technology of TVS is potentially an enabler for the Flexible Facilitation Model (FFM), where mixing of, for instance domestic and international passengers is possible without physical separation of the two passenger flows with terminal partitions.

Beside the above, CBP is actively working to expand stakeholder partnerships and adoption, prioritizing the highest volume of international airports and carriers to achieve the biometric air exit implementation goal. CBP continues efforts to consider innovative ways to utilize TVS with mobiles phones, tablets and watches. CBP will look to expand partnerships with international airports and governments and to further expand capabilities in preclearance locations to continually improve security and facilitation of traveler processes.

Trends Identified

This specific use case has shown the possible success of a seamless passenger journey through several checkpoints, manned by different airport stakeholders (airline, customs, security)

- Touchless touchpoints going forward – reducing the risk of transmission of communicable diseases, as well as increasing speed of travel, ease of travel
- End-to-end integration of digital identity management throughout the passenger (airport) journey. This is to continue even beyond the scope of just the airport. All journey touchpoints will use biometrics, from booking to arriving at a hotel/destination, across different modes of transport, different suppliers of services (taxi, baggage pickup, airport, airline, security, taxi, hotels, etc..)
- Incentives passengers to use the system as it allows for more ease-of-use, faster processing, less hassle with official documents.

APPENDIX F

Case Study: Known Traveler Digital Identity at Aéroport International Montreal-Pierre Elliot Trudeau, Montreal, Canada (YUL)

Executive Summary

To respond to the increasing demand for a more efficient and streamlined passenger process, the World Economic Forum and several airport and industry partners launched a program for the development of a trusted digital identity based on biometric technology, named the Known Traveler Digital Identity program, or KTDI. The goal of this initiatives is to make it possible for all industry partners to use this digital identity securely and with ease of use, while protecting the passenger's privacy.

The KTDI program is still in the early development phases and relies on the "self-sovereign" concept where passengers are the owners of their personal data and can elect to share them (or not) with different parties (e.g., airport, airlines, border authority). In its current design, the program identifies that the digital identity should be created by an identity issuing authority, either a third-party or a government authority. This authority would create a biometric template of the passenger as well as a unique security feature. With the use of distributed ledger technology on a blockchain, the immutability of the digital identity can be secured.

The KTDI concept would use the distributed ledger to register every successful identity claim at various authentication touchpoints in order to build up trust through verifiable claims, a type of smart contract in the blockchain. In 2018, the Governments of Canada and The Netherlands established a pilot-group to drive the KTDI efforts. After a successful pilot, efforts for implementation are currently stalled due to the Covid-19 pandemic.

Key Facts

Table F-22: Key fact of case study on KTDI

What biometric technique is used?	• Facial recognition, • 1:1 and 1:few matching of biometrics
Where?	• Initial pilot at three International airports: • Aéroport International Montréal-Pierre Elliott Trudeau (YUL), • Toronto Pearson International Airport (YYZ) • Amsterdam Airport Schiphol (AMS)

Pax process steps:	• Enrollment first, prior to booking a flight: o KTDI digital identity enrolment, with 3rd party or government authority • Departure at airport o Passenger and bag check in follow the conventional check-in process; o Enrollment by forwarding passenger flight details to the KTDI app, on a mobile device or by enrolling at biometric kiosk in the departure hall; o Entry to security filter with biometric lane for enrolled passengers o Border control emigration checkpoint with biometric lane; o Boarding gate with biometric lane • Arrivals: o Enrollment by forwarding passenger details through mobile phone (prior to departure or from the plane) or by enrolling at biometric kiosk in the arrival hall; o Border control immigration checkpoint with biometric lane;
Who?	• The KTDI facilitation is developed by the Governments of Canada and The Netherlands, in partnership with World Economic Forum (WEF) and several other partnering organizations. The complete pilot-group consists of: o World Economic Forum o Government of Canada (Transport Canada) o Government of The Netherlands o Aéroport International Montréal-Pierre Elliott Trudeau o Toronto Pearson International Airport o Amsterdam Airport Schiphol o KLM Royal Dutch Airlines o Air Canada o Accenture (Accenture, 2018) o Vision-box o Idemia o Customs and Border Service Authority CBSA (Canada) o Immigration Refugees and Citizenship Canada (IRCC) o Koninklijke Marechaussee (Dutch Border Police) o Rijksdienst voor identiteitsgegevens (Dutch Identity authority) • The workgroup was initiated in 2018, pilot implementation in terminal was originally planned in 2020 but postponed and expected to commence in the near future
Why?	• The KTDI program is based on a platform that enables a traveler-managed digital identity for international paperless travel, to create a seamless passenger flow which is faster and more enjoyable. KTDI

	protects the passenger's privacy by giving back control over their data and who they share that with.
How? Technology used?	• KTDI is based on an interoperable digital identity, linked directly to government-issued identity documents (e.g. e-Passports) of which the verifiable claim is stored on a blockchain. The platform allows for identity verification to airports, airline and border authorities using cryptography, distributed ledger technology and biometrics (facial recognition).
Enrollment / Digital Identity creation and verification	• During the pilot, a one-time enrollment in KTDI program was achieved thus: o Airline invites a select group of passengers to participate o Passenger creates and certifies digital ID with appropriate official issuing authority: (Local Government digital identity issuing office hosted at Schiphol airport or The Canada Border Services Agency (CBSA) in Canada) o Passenger downloads mobile phone application and creates KTDI profile o The local identity issuing authority makes a photograph of the passenger with the passengers capturing device, in a controlled environment. The passenger stores the image on the KTDI app where it is encrypted, which the authority then verifies. o The passenger then tests this verified digital ID by making a selfie, which is compared to the digital ID and if a positive match is made, it is verified by the local authority and becomes the first verifiable claim of a traveler's identity data stored on the KTDI blockchain. The photos are not stored anywhere, other than on the passenger's own device. The blockchain only stores the verifiable claim. o In the mobile phone application, the passenger can then add information regarding upcoming flight, such as digital boarding cards. • Per trip online check-in for each flight: o Prior to a flight the passenger can push its biometric details, passport details as well as its boarding card to the seamless system of the airport where it is temporarily stored in a passenger data envelope (stored max 24 hours). This can be repeated for each flight without having to enroll again. • *Note:* the exact method of enrollment may still be subject of change due to the fact the project is still in development.
Verification of identity how?	• The Digital ID and other details of the passenger are temporarily stored in the Passenger Data Envelope (PDE). Directly after forwarding the data to the airport of departure or arrival, the system can perform all checks whether the passenger is authorized to pass each touchpoint. At the airport upon arrival at each biometric lane of the seamless process the passenger's face is matched with the template stored in the system and processed according to the authorizations.
For which user groups?	• Pilot group of passengers between the Netherlands and Canada with a Dutch or Canadian Passport traveling with KLM and/or Air Canada

	between AMS-YUL and AMS-YYZ in either direction. The system can potentially be used for any nationality (with an e-Passport) as long as the respective authority of the country provides the required digital ID verification and KTDI support.

Introduction

After evaluation of the Cathay pacific trial it was concluded by AMS that the passenger process could be further optimized. Biometric enrollment with the use of an e-passport is still a time-consuming procedure. If it would be possible to enroll once and then be able to fly every time regardless with which airline without additional enrollment at the airport, this would save a processing step and create a more seamless passenger experience. A potential solution for such a process was initiated by the World Economic Forum: the KTDI (KTDI, 2020). The KTDI concept (Accenture, 2018a) shifts from conventional travel documentation verification to a digital format. The concept is piloted by cross-border collaboration between Canadian and Dutch public and private partners. In 2018, the Governments of Canada and The Netherlands established a pilot-group to drive the KTDI efforts and determine the potential of the concept for international connections. The pilot-groups includes the public authorities of both countries, the airports and airlines offering a direct connection, and the technology companies involved with KTDI's development. as part of the initiative the concept is planned to be implemented at Amsterdam Airport Schiphol (AMS) for KLM and Air Canada flights from and to Montréal and Toronto.

Note that as the pilot has not started, this case study description is limited to the main concept of operation, functions, and technical aspects.

How Does it Work?

Before the Passenger Journey

The KTDI system relies on two main 'platforms'. The first platform is the KTDI supported airport system hosted by an airport, the other is the KTDI app on the mobile device of the passenger, which holds the passengers digital ID and flight information.

The airport's orchestration platforms, as it supports KTDI, can accept passenger data when they share it via the app, prior to departure or arrival. The orchestration platform creates a Passenger Data Envelope for that data and will store that for the duration of the trip. These platforms are typically hosted locally or on a cloud dedicated to the airport systems.

The KTDI app on a passenger's mobile device stores the passenger's biographic data (passport data) as well as the passenger's biometric data: the photographs of the passenger's face. These data are stored only locally on the mobile device and can be shared with airport platforms and country authorities if the passenger chooses to do so.

The touchpoints at the airports operate on the system provided by Vision-Box, based on IATA's OneID concept. The system is built up of the following components for departures:

- KTDI enrolment kiosk for post check-in
- Biometric lane with digital ID verification at security filter access
- Biometric lane with digital ID verification at border control filter
- Biometric lane with digital ID verification at boarding gate

The following components are installed for arrivals:

- KTDI enrolment kiosk at the arrival gate
- Biometric lane with digital ID verification at border control filter

The Passenger Journey

Passengers that travel with the KLM or Air Canada flight from Amsterdam Airport Schiphol to Aéroport International Montréal-Pierre Elliott Trudeau (YUL) or Toronto Pearson International Airport (YYZ) and vice-versa can be invited to participate in the pilot. During the pilot participation is for invitees only.

KTDI Enrollment and Preparation

The KTDI concept relies on a KTDI profile and a verified digital ID that is kept in a digital wallet on the mobile device of the passenger in the KTDI app. The digital ID contains biometric and biographic details of the passenger. These details are verified by an identity issuing authority and encrypted by a security certificate.

In the Netherlands, the verification of the KTDI profile on the mobile device takes place in the municipality office at the place of residence. The municipality office is designated as the organization to issue identification documents on behalf of the Rijksdienst voor Identiteitsgegevens (RVIG) (translates to: National Office for Identity Data). Verification is done at the desk of the municipality office with the passenger being present.

In Canada, passports are issued by Immigration, Refugees and Citizenship Canada (IRCC) at dedicated passport offices. Application for a digital ID and verification of the KTDI profile takes place at these IRCC offices and takes a few processing days, as the Canada Border Services Agency (CBSA) checks the application. Passengers enroll at a kiosk, after which the passenger data is vetted by the office authorities.

Once setup and verified, the KTDI profile is ready for use with the mobile device and includes the first verifiable claim of a traveler's identity data. The digital identity, being a trusted traveler (Verifiable Digital Identity - VDI), is on the mobile device and can be expanded with travel data (e.g. boarding card) but also immigration data such as VISA's or ETA's. The passenger has self-sovereignty over the data and can push data to the seamless airport/airline platform. The data remains with the passenger on the mobile device and is not centrally stored.

Airline Check-In and Airport Enrollment Per Trip

To prepare for a trip, the passenger can check-in online or at the airport to receive a mobile boarding card. The boarding card can be added to the digital KTDI app after which the passenger can forward the all the relevant data to the seamless platform of the airport. This includes passport details, a biometric template and boarding card details for the airline.

The seamless platform then creates a PDE (Passenger Data Envelope) that contains all the data required for the journey of the passenger by the airport, airline, and border control authorities, being either the Koninklijke Marechaussee (Dutch border police) or the Canada Border Services Agency (CBSA). The platform provides the interfaces with the systems of the stakeholders and organizes the data flows. It also manages the business rules and organizes the authorization that are received from the stakeholders.

The data that is provided by the passenger is pre-staged in the seamless platform. No passenger data itself is exchanged or stored at the blockchain, only transactions with pointers are provided. As long as all transactions (i.e. the verifiable claims) are without complication, the required level of trust is present, and the passengers' credibility is established.

Arrivals With the KTDI App

Upon arrival at the destination airport, a dedicated area with registration kiosks is located at the gate for the invited and enrolled passengers. These kiosks register the passengers ID as well as their biometrics to create a Passenger Data Envelope in the same way as is done at the departure airport. Again, the passenger's details will be verified against the systems of the border control agency.

At immigration, dedicated lanes for KTDI with a mantrap layout are equipped with a camera to recognize and confirm the passengers ID and a near-field communication reader for the mobile phone with the digital ID or the e-Passport when required (for redundancy). When the passenger is authorized to proceed, the exit barrier opens.

Retention and Storage

Although the process at the airport is based on a "per trip" model, enrolment to KTDI can be considered as a "for life" model. The digital identity that can be stored on the passenger's mobile phone is created for the lifetime of the passenger's e-passport and can be used for multiple journeys. Unless the passenger wants to opt-out, by deleting the KTDI app and its data from his/her mobile device.

The passenger's identity data is not stored on the blockchain. The blockchain holds the pointer to the verifiable claims (interactions) of a traveler's identity data with trusted entities. The record is expanded with every claim from every time the traveler uses the profile and thereby re-establishes the credibility of its identity. As the record expands, the credibility increases.

The mobile phone application can contain additional data related to the passenger. Prior to a trip the passenger can push this information to the seamless flow system of the airport. The passenger manages the KTDI profile and digital ID with self-control over the permissions and data pushed to the respective airport, airline, and authority per trip. The identity data itself stays with the passenger and is not saved centrally at the airport or authority. The data that is made available by the passenger, to the airport, airline, and authorities is encrypted and stored in the local databases for 24 hours and is only available for the trip (World Economic Forum, 2020a).

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

System Specifications – Digital ID and Self-Sovereign Identity

Instead of simply replacing the hardcopy ID with a softcopy digital ID derivative or alternative, the concept uses verifiable claims (interactions) of a traveler's identity data with trusted entities. The use of such claims ensures that the credibility of the traveler and its identity are established and authenticated. Blockchain technology is used to provide information of these verifiable claims as they are essentially transactions between the digital ID of the passenger and verifying entity. The use of a digital format enables optimization of the passenger process and improves risk management.

Stakeholders and Responsibilities

The KTDI program was brought together under the World Economic Forum (World Economic Forum, 2020), with many partners at the table. The three airports, the two national governments as well as Accenture and World Economic Forum lead the program through its initial forming setting the direction with innovation and the drive to organize pilot programs.

Stakeholders

The main stakeholders of the KTDI program are the three airports Aéroport International Montréal-Pierre Elliott Trudeau (YUL), Toronto Pearson International Airport (YYZ) and Amsterdam Airport Schiphol (AMS), together with the two airlines; KLM Royal Dutch Airlines and Air Canada. Also, three private companies were involved, with Accenture, Vision-Box and Idemia. As partners during the development of

the KTDI program and thus stakeholders, the Governments of Canada (being Transport Canada), CBSA, The Government of the Netherlands and the Koninklijke Marechaussee (Dutch Border Police) were closely involved to facilitate the programs first pilot. Most importantly, the stakeholder group to be most affected by the program: the passengers who were selected flying KLM or Air Canada to partake in the pilot.

Responsibilities and Governance

The consortium between the stakeholders led, at the start of the project, to the formation of multiple working groups, all made up of members of the different stakeholders to maximise working together on multiple fronts. The working groups are guided by a project management committee and a steering committee, that oversee the progress as well as guard the project goals and timelines. Working groups were formed for tasks related to legal topics, communications, the system architecture and technology, implementation and performance measurement, and for the delivery of pilot projects leading up to larger implementation. In this format, responsibilities amongst the different stakeholders were divided equally, with experts in each of the groups taking lead and informing the other members.

Case Study Review

Benefits

Benefits of the implementation of KTDI are numerous, different for each stakeholder. The main benefits are aimed at the passenger and his/her experience. KTDI allows for faster touchpoint processing, better privacy protection, a touchless journey through the airport which in current Covid-19 time is a key focus. The complete process allows the passenger to only use his/her mobile device, relieving him/her of having to fumble with a passport and/or boarding pass. Faster processing through touchpoints at the airport will smoothen the journey and be less stressful, allowing the passengers to spend more time relaxing, visiting retail shops or select offerings in food & beverage.

Furthermore, for government agencies/subcontractors such as border protection, immigration and airside security, the digitized process allows for a more efficient resource allocation, a smaller footprint in the airport and notably a safer and more secure airport operation.

Airlines will benefit from efficiency increases as automation makes room for more personal service, where needed, and more streamlined processes. Passengers will predominantly interact with the airline through the application on their phone.

For airports, the biometric solutions provide means to increase automation, decrease the necessary footprint of touchpoints, decrease staff numbers and all in all process more passengers in less space. Especially with Covid-19, the focus lies on creating a touchless and seamless travel experience, which KTDI paired with the right infrastructure offers.

Another benefit for airlines, airports and passengers alike, is the forward verification and country entry eligibility that is possible with the system, preventing passengers being rejected at the country of destination and having to fly back. Arriving at the destination, passengers present their KTDI digital identity, and being vetted prior to arrival, they only have to wait for a positive match of the picture made at the e-gate

With the system architecture including a blockchain component, which aims to store the verifiable claims of confirmed identity, rather than the digital identity itself, the passenger can choose exactly which data he/she shares with which stakeholder in the passenger journey (Kelleher, 2019). The complete identity document or credential is only stored on the passengers own mobile device. KTDI is designed to comply with both the Canadian as the European privacy protection rules, and is designed according to ‘Privacy by Design’ principles.

Responses from Passengers

For now, with the biometric solution still being under development, no passenger feedback has yet been collected. Internal feedback by members of the working group, and employees of the consortium had been used in the development of the mobile application which has now progressed to a second beta phase. Trials in a laboratory environment will aim to test all components together, linking systems of all the different stakeholders.

Fall Back Options

The KTDI program is designed to replace the current touchpoint infrastructure at the airport, but a non-biometric, non-KTDI option will for the near future still be required for passengers that wish to opt-out. The initial pilot program that was successfully rolled out, only included a limited number of selected passengers per flight, thus the standard processes were still available for passengers wishing not to use the KTDI system.

Concerns

Two points that were a concern for the consortium were 1) regarding the hosting of mobile application and 2) the legal frameworks that would need to be agreed on. On the first concern, discussion is ongoing on whether the WEF would host the application, or if a separate entity would need to be created. Development of the application by TC or CBSA (with experience in application development) or the Dutch government authority would not necessarily mean that party would host the application.

On the second, the consortium had knowledge of multiple industry providers of technology and hardware infrastructure that demonstrated the individual use and capabilities of the component, much harder would be the drafting of legal agreements between the multiple stakeholders regarding their roles in data processing, data controller, data exchange as well as how this would be impacted by privacy impact assessments that several stakeholders would go through.

Lessons Learnt

One of the main lessons learnt (so far) by the working groups of the consortium was that the creation of the legal framework was underestimated at first (Gendreau, 2020). Expertise on a wide range of matters from privacy protection for the two countries as well as the European GDPR, to data management, matters of intellectual property and the legal arrangements that are typical for collaborations between public and private companies. The drafting of these legal frameworks started slow, and expertise had to be attracted from outside the consortium, affecting budgets and project timelines.

A second lesson learnt was the switching from a detailed project approach description and plan, to a more flexible, phase by phase approach. This dynamic approach provided clearer short-term goals and deliverables that were easier to manage and attain by the project working group.

Findings and Trends

Findings

- An ongoing development of the digital credential, with international standards developing simultaneously, with ultimate goal of being interoperable with other (biometric) systems

- The multi-stakeholder (multi-country) system proves a much more complex project, although the potential benefits in the long-term (interoperability and scalability) can only be attained through this route.
- Project lessons learned on privacy of information and transmission and collaboration with foreign governments, especially regarding legal frameworks between both public and private project partners.

Future Situation and Broader Implementation

The goal is to implement the KTDI system at all airports that offer flights between the Netherlands and Canada, to offer the seamless flow option to all passengers flying with the project stakeholder airlines (Air Canada and KLM). Proof of concept might attract more interested countries/airlines/airports.

Until that time, first a pilot in a lab environment aims to test the complete system for a very small amount of simulated passengers. Pilots at actual airports with actual passengers would follow, before further implementation as the partner airports.

Scalability is another major focus for the future implementation, especially as blockchain component needs to be well designed to handle larger amounts of data traffic. Similarly, the hosting of the application on the passengers mobile devices need to be able to handle the data load, the interoperability and integration with multiple (new) airlines.

As many digital and biometric solutions are being developed around the world, the consortium is in constant contact with IATA and ICAO, to follow developments in DTC and OneID. The consortium aims to align the KTDI system with these international standards and developments, to increase the likelihood of successful interoperability with other systems.

Trends Identified

For this specific case study, all five trends identified in the second chapter make their appearance. Key in this biometric solution for the passenger is the use of a mobile device (smartphone) for storage of their digital identity and biometrics. Looking at the system architecture design, we see in this use case the trend towards a complex, multi-stakeholder system that aims to maximize long-term benefits of interoperability and scalability, by aligning to global standards for digital identity credentials as well as standards for biometrics with regard to privacy, security and ethical concerns.

With increasing global concern on the latter, it is of no surprise that the consortium in this case study has applied design principles of Privacy by Design, and is taking significant time preparing legal frameworks to mitigate potential risks.

Finally, this case study is another example of a solution that leans heavily on biometric technologies for identity verification, and takes care to distinguish itself from systems that might be used for mass-surveillance.

APPENDIX G

Case Study: The Seamless Passenger Journey at London Heathrow (LHR)

Executive Summary

The vision for a seamless passenger journey consists of the deployment of biometrically enabled touchpoints equipped with "cameras on a pole", at check-in kiosks, self-service bag drops, ticket presentation gates and self-boarding gates. This initiative targets both international and domestic customers, and encompasses all terminals of the airport, with an initial focus on T5 and T2. At a later stage other processing points will be added to the end-to-end journey, such as immigration and security screening and the ability to enroll and check-in using a mobile app. Another parallel initiative consists of biometrically enabled preclearance of passenger travelling from the U.K. to the United States on selected flights.

Upon arrival at the first touchpoint, the departing passenger consents to the digital process, scans his/her boarding pass and captures a photo of his/her face (i.e., on the day image). The automated passenger identification involves matching this on the day image with the image stored in the passenger's e-Passport chip. If there is a positive match, the passenger's ID is verified. Biometric matching and boarding pass scanning will be used at subsequent touchpoints to recognize the passenger throughout the remaining journey.

For a passenger travelling to the United States, the process also involves matching the on the day image against the CBP's TVS. For the validation to work, it is a pre-requisite that the passenger had previously visited the country, or his/her photo is otherwise accessible from a U.S. government database such as for a visa application (Heathrow, 2020a).

At the heart of the process is the Passenger Authentication Scanning System (PASS2), which was developed by Atkins on behalf of London Heathrow Airport (LHR) and currently manages passenger identity throughout the airport. The system incorporates Atkins' ID management platform (IMP), and is augmented for various tests and trials of different technologies, including those from Yoti, ICM, CEIA, Dorma Kaba, Rockwell Collins and Aurora AI (Stewart, 2019).

Passengers' biometric data are stored and retained on a "per trip" basis, and will be cleared at the end of the operational day or after 24 hours (Oliver Wyman, 2019) (and within 30 days during the live trials, which passengers were notified (Heathrow, 2020)). LHR only keeps anonymized transaction data to monitor and improve the biometric technology. Due to privacy issues and the risk of data breach, LHR prefers not to hold passenger's biographic data in their IMP and is testing a third-party provider of verification function. Booking details are not stored either, as the passenger is still required to scan a boarding pass.

The main benefits include an enhanced experience with faster processing and reduced queuing times for passengers, allowing the airport and airlines to save and optimize their resources and minimize costly terminal expansions. From a government perspective, the automated process is much more accurate, and thus more secured, than manual ID verification.

Key Facts

The table below summaries the key aspects of the seamless passenger journey at LHR.

Table G-23. Key facts of case study on the Seamless Passenger Journey

What?	• The Seamless Passenger Journey • Facial recognition • 1:1 and 1:few biometric matching
Where?	• London Heathrow Airport (LHR), the United Kingdom
Passenger process steps:	• All the processing points were tested in the lab or with live trials, but full deployment will happen either in the short-term (a date has not been set yet due to Covid-19) or at a later stage • Online and off-airport check-in (at a later stage) • Self-service kiosk and self-service bag drop (in the short-term) • Improved security (risk-based – at a later stage) • Ticket presentation gate (in the short-term) • Security risk-based screening (at a later stage) • Self-boarding gates (in the short-term) • Border (at a later stage) • U.S. bound flights – cross-validation with CBP's TVS (live on some flights and planned for the remaining flights in the short-term) • Cross-border with transit and destination airports (at a later stage)
Who?	• LHR was set to launch its first end-to-end biometric deployment, from the summer of 2019, bringing facial recognition to the key processing points of the departing passenger's journey. Atkins' PASS2 system, which incorporates Atkins' IMP and various technologies, including those provided by Yoti, ICM, CEIA, Dorma Kaba, Rockwell Collins and Aurora were tested.
Why?	• The £50 million project is part of a wider program of investments (Heathrow, 2018) to increase the speed, efficiency and security of passengers' journeys, reduce congestion in LHR's terminals, and increase capacity in the existing facilities, thus postponing costly expansions. Biometrics on the outbound passenger journey was first implemented at T5 to enable the terminal to co-locate domestic and international passengers. A face capture of the domestic passenger is performed at the ticket presentation gates when the passenger presents his/her boarding pass and then again at the boarding gates. This would ensure that domestic passengers would not board an international flight and similarly international passengers would not board a domestic flight. The program was then extended to T2. Recently after extensive testing, the program is ready for full deployment to include all passengers and additional touchpoints.
How?	• Currently, manual authentication means passengers need to present IDs and travel documents such as boarding passes and passports many times throughout the outbound journey to show that they are authorized to fly. By offering passengers the option to use facial recognition technology, the process becomes more streamlined and faster.

Enrollment / Digital Identity creation and verification	• In-person enrollment: The passenger can enroll at a biometrically-enabled self-service check-in kiosk, at a self-service bag drop or at the ticket presentation gate; the passenger scans his/her e-Passport (the machine readable zone contains the passenger's biographic and biometric data), takes a "on the day image" that is then matched to the passport's image, and scans or retrieves their travel booking; the verified biometric data is then stored in the IMP. • Mobile enrollment (at a later stage): The passenger uses a mobile device ID verification app, provided by Yoti, to scan his/her passport's Machine-Readable Zone (MRZ), gaining access to the passport's chip and biometric/biographic data. The passenger takes a lively "selfie" to authenticate the image on the passport. The verified biometric data is then stored in the IMP. This process was tested in principle, but it will be fully implemented at a later stage • Because of privacy issues and the risk of data breach, LHR would prefer not to hold passenger's biographic data in their IMP; ideally the verification function should be provided by a third party and the only data stored in the local IMP would be the biometric data; the booking details are not stored either as the passenger is still asked to scan his/her boarding pass at each touchpoint.
Verification of identity how?	• Identity verification involves matching an 'on the day image' taken of the passenger at one of the biometrically-enabled self-service touchpoints to the image recorded on the passport's chip. A single Passenger Data Envelope (PDE) is created and stored in the local IMP. Biometric matching will then be used at subsequent touchpoints to prove it is still the same passenger without the requirement to again provide documentation (i.e., by matching subsequent scans of the passenger's facial biometrics to those extracted from the first "on the day" image)
For?	• The initiative will be extended to all domestic and international flights out of T5 (British Airways), T2 and eventually to all terminals

Introduction

LHR has been using facial biometrics for the departing journey for more than 10 years (Wilcox, 2019), with the original system designed to capture the domestic passengers' faces at ticket presentation gates and later on at boarding gates. This was primarily set up to allow international and domestic passengers to mix in the combined departure lounge, while ensuring that they would board the correct flights.

In 2016, LHR developed a new business case to set out the future pathway for automation, innovation and technology at the airport. In this process, LHR quickly realized that passenger identification is key in creating a seamless passenger journey for all customers, and biometrics is the right technology to help achieve this objective (Wilcox, 2020).

LHR began a 3-year program of investments to implement automated self-services and augment the existing system for passenger identification, with the aim to increase the speed, efficiency and security of passengers' journeys, and reduce congestion inside the airport's terminals. After a series of successful trials, LHR was set to launch its first end-to-end biometric deployment from the summer of 2019, bringing facial recognition to the key processing points of the departing passenger's journey. The deployment has been postponed until further notice due to the on-going pandemic crisis.

How Does it Work?

Before the Passenger Journey

Biometrics has been adopted as a means of passenger identification at T5 first and then T2 for more than ten years. Therefore, when it was decided to extend the program to additional touchpoints and to all international and domestic passengers, the most cost-efficient and viable option was to augment the capability of the existing IMP, developed by Atkins.

The platform stores the passenger's name and biometric data captured at the first touchpoint (self-service check-in kiosk, self-service bag-drop or ticket presentation gate) by reading the e-Passport chip and taking a photo ("on the day" image). The data stored is referred to as the PDE.

The biometric data stored in the e-Passport chip is compared to the "on the day" image and, if there is a positive match, the passenger's ID is verified and from that point onwards, the "on the day" image is used to recognize the passenger throughout the remaining journey, without the need for additional paper-based identification.

While it is technically feasible to store additional passenger data, such as the PNR, in the IMP to eliminate the requirement to scan the boarding pass at each touchpoint, LHR staff made the decision to not integrate this step and therefore to not store passenger booking details in the IMP. The thinking behind this decision was that passengers will continue to hold a boarding pass (printed or on their mobile app) for the foreseeable future, as confirmed by a passenger survey. This decision eliminated the need to integrate the IMP with the airline DCS where passenger information such as the PNR is kept, significantly simplifying the IMP capabilities and shortening the validation and matching times.

The CBP TVS initiative relies on the CBP's own capabilities to almost instantaneously validate a passenger's identity by comparing his/her biometrics data ("on the day" image captured at the boarding gate) against a pre-existing CBP held database (for the validation to work, the passenger has to be a returning passenger to the United States with his/her biometric and biographic data already captured by CBP in a previous visit, or his/her photo is otherwise accessible from a U.S. government database such as for a visa application).

Mobile enrollment was tested to prove that the technology works and that the IMP could support the integration with a third-party identity app. However, this mobile enrollment capability has not gone live yet as LHR staff believe that airlines should integrate this capability within their own booking app and therefore they should take the lead in pushing this initiative forward. Considering that 60 to 70% of passengers at LHR travel for leisure and a significant number of these passengers travel only once a year, this capability would have limited value overall.

The trial was conducted in partnership with Yoti and consisted in the passenger checking in on the Yoti webpage or using the mobile app. The passenger was asked to share biometric and biographic data by having the app access the passport MRZ and by taking a photo of the day. The data was then stored in a secure Yoti-controlled database, setup specifically for this trial. At the following processing points, the passenger's face would be captured by the biometric-enabled touchpoint, translated into a specific readable format and sent to Yoti's IMP for verification of identity. Using this approach, referred to as self-sovereign ID management approach, LHR IMP would not store passport details and would therefore be less exposed to privacy concerns and/or data breeches.

The Passenger Journey

First touchpoint (self-service kiosk, self-service bag drop or ticket presentation gate)—The passenger's consent is taken to use his/her face biometrics and biographic information; the passenger scans his/her boarding pass (printed on paper or on his/her mobile app) and his/her passport; the kiosk camera capture the passenger's face (on the day image); the boarding pass is validated directly with the airline DCS; the

passenger's biometric data is accessed via the e-Passport chip and verified against the on the day image; if there is a match, the passenger's face biometrics, name, flight number and PNR information, known as PDE, is stored in the airport IMP and it will be used for identification at the other biometric-enabled processing points at the airport. The process and the technology are capable of handling group enrollments versus one on one enrollments.

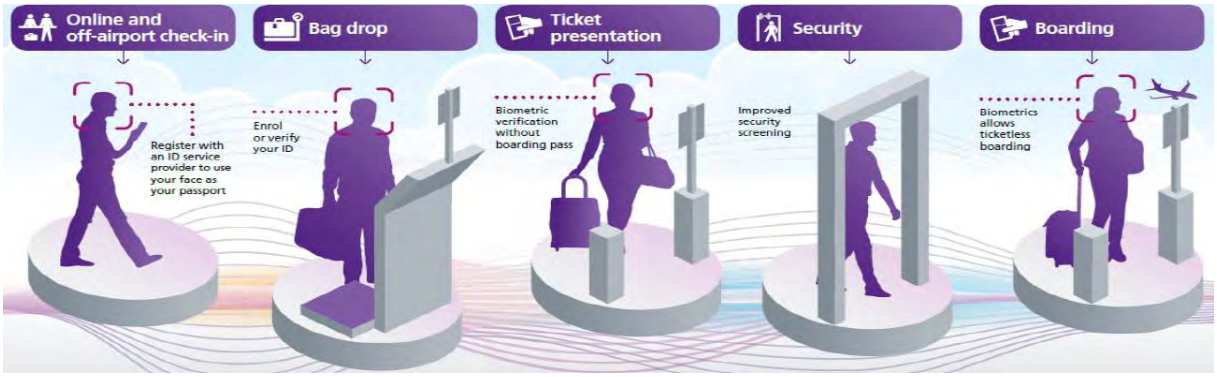
Other biometric-enabled processing points—the passenger is identified by a comparison between the camera capture at the processing point and the "on the day" image stored in the IMP.

In case of a no-match or if the passenger wishes to opt-out, he/she can proceed to staffed processing points.

In the case of selected U.S.-bound flights and for returning passengers to the United States, the passenger scans his/her boarding pass at the boarding e-gate, the passenger's identity is validated as per above and the biometric data is verified against the CBP TVS database.

Retention and Storage

The PDE storage and retention is "per trip" and all information is deleted at the end of the operational day or after 24 hours. After that, only anonymized transaction data is retained to monitor and improve the biometric technology. During live trials, the data was kept for 30 days.



Source: Heathrow (Beunardeau, 2019).

Figure G-39: Seamless Journey Vision

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

Stakeholders and Responsibilities

Stakeholders

Since the early visioning stages, airline partners (including British Airways) and suppliers (including airport system, hardware and the IMP vendors) worked collaboratively together to map the journey, define the concept of operations and test the technology.

U.K. Government's bodies were involved in different stages of the process. For example, LHR was collaborating with the UK Department for Transport (DfT) to test the prospect of risk-based differentiated-

security. In addition, LHR worked with lawyers and the Information Commissioner's Office (ICO) to look at the process from a privacy perspective.

The compatibility of the PDA data format and its integration with the Government own database was tested in principle on both inbound and outbound processes, but no live trials were implemented due to the regulatory and policy changes required to make the implementation possible.

As previously mentioned, the U.S. Government, in particular CBP also collaborated with LHR.

To gain further stakeholders' buy-in, demonstration days were held throughout the initiative. LHR also actively shared their experiences with other airports and aviation industry bodies, such as IATA and ACI.

Responsibilities and Governance

The seamless travel initiative's governance can be summarized as follows:

- Heathrow staff led the initiative and secured the necessary funding for lab testing, live trials, and any other related activities.
- Several working groups and sub-working groups were established to include all stakeholders and focus on specific subject matters such as technology, processes, regulation, etc.

This governance structure was kept in place since the beginning of the initiative in 2016.

Timeline and Planning

The vision was initiated by Heathrow staff in a series of visioning workshops to discuss the future of automation and passenger identification and how technology and innovation could shape the passenger journey. A business case to support the initiative was developed and the initiative was officially kicked off in 2016. Since then, LHR has embarked on a series of lab tests and live trials, which have provided invaluable insights on each aspects of the journey including human interaction and perception. Those tests included the following:

- Testing individual and group enrollment and biometric matching at various airport's touchpoints, such as kiosks, bag drops and entrance to security;
- Enabling off-airport enrollment using an app;
- Allowing passengers' automated access at subsequent touchpoints once they have enrolled at the first touchpoint, thus expediting their journey;
- Looking at the prospect of enabling risk-based differentiated security, in collaboration with the UK Government;
- Testing a cross-border solution in collaboration with CBP's TVS system (Heathrow, 2020a); and
- Testing a third-party provider of verification function.

The approach taken by LHR is to retrofit existing or new self-service equipment with "cameras on a pole" rather than have cameras integrated the equipment itself. This decision was made to provide a sense of consistency across the various touchpoints and the terminals so that passengers would know what to expect and where to look.

Procurement and Vendor Selection

By early 2019 lab tests and trials were successfully completed, vendor selections were finalized and an initial investment of £50 million was secured. The initial phase of the roll-out at T2 and T5 was planned to start in mid-2019. Once completed, this would be the largest rollout of biometric technology with more than 5000+ touchpoints. Due to the global pandemic and the drastic decrease in passenger numbers, the deployment has been put temporarily on hold.

Use Case Review

Benefits

The benefits for the various stakeholders are highlighted in the table below.

Table G-2. Amazon Go - Stakeholder Benefits

Stakeholder	Benefits
Passengers	Enhanced experience with a more seamless journey
	Faster processing and reduced queuing times
Airport	Increased passenger processing throughputs postponing the need of costly capital expansion programs
	More efficient use of existing infrastructure
	Co-location of international and domestic passengers in the same departure lounge with significant increase in efficiency
Government	Enhanced security: ID validation is much more accurate than manual validation (almost double the matching rate)
	Reduce staffing costs as fewer passengers have to be manually processed
Airlines	The biggest beneficiaries
	Staff reduction or redeployment where most needed
	Operational improvements such as on-time performance

Responses from Passengers

During the lab tests and live trials, it has been proven that biometric verification without boarding pass is technically feasible. However, passengers' feedback indicates that they prefer the combination of facial biometric capturing and boarding pass scanning at different gates and touchpoints. This approach seems more natural, reassures the passengers that the process is secured and that they are correctly completing the departing journey. LHR therefore assumed that the boarding pass will not be disappearing in the short to middle term.

It is noteworthy that passengers' feedback was always very positive when they were asked about identity management as a mean to deliver a secured and seamless journey. However, they were quite skeptical and negative when hearing the term "biometrics".

In addition, LHR established a focus group of 3,000 people to gauge the public's sentiment on privacy. The vast majority of the respondents said they were ok sharing their data if they received transparent information on how their personal data would be used and if they had control over their personal data (who to share it with and why).

System Performance and Specifications Review

To overcome the problem of poor ambient lighting, a decision was made early own to adopt cameras augmented with infrared technology. This technology consistently provides better quality images for matching purposes.

Some of the biggest challenges had to do with additional functions having to be performed at some of the processing points, such as visa checks (when visas are not electronic) and excess baggage payments.

Fall Back Options

The intention was never to completely eliminate manned positions. Therefore, in the case of no matching, lack of consent, or if the technology fails, staffed counters or roaming agents would be always available at each touchpoint.

Concerns

Data privacy was addressed from the beginning and the principles of Privacy by Design were incorporated in the system architecture where access to data was provided only on a "need to know" and "authorized to know" basis.

LHR engaged ICO to perform a full review of the seamless passenger journey initiative. Specifically, the ICO reviewed the role and the relationships between the different business partners (airport, airlines, suppliers) involved in the processing of biometric personal data, confirmed that data management met GDPR/DPA18 provisions and assessed LHR's proposed method for obtaining explicit passengers' consent to use their biometric data in a live environment.

Lessons Learned

The key lesson learnt was that the seamless passenger journey initiative is not about technology, but rather about human interaction with the technology. The technology exists and lab tests proved that it works. However, if the technology is not intuitive and user friendly, ultimately it won't serve its purpose and this was proved over and over during live tests.

Apparently simple things such as the distance from the camera during image capture, where the passenger was looking during image capture, crowding around cameras and tight queuing in proximity of boarding gates, would cause poor image quality and no matching. Human interaction was carefully analyzed and appropriate solutions were identified throughout the trials.

Findings and Trends

Findings:

Biometrics, combined with self-service processing, delivers tangible efficiencies in processing times, reduction in staffing requirements and a significant improvement in safety and security with a much higher matching rate than that measured in manual processes.

These benefits are significant when the deployment of biometrics and automation is on a very large scale as it will be in the case at LHR.

Future Situation and Broader Implementation:

Other initiatives such as the mobile enrollment, risk-based security, and the integration of immigration in the seamless journey are currently on-hold.

The cross-border initiative (between 3 airports, 3 governments and 2 airlines) was initiated by Heathrow with involvement from IATA and it is currently in the technical testing phase, an identity management mobile app is in the process of being developed and the function of the 3rd party broker (providing a platform to verify identity, which in the case of the United States is CBP, but it is different in other countries) has

been currently discussed and could hypothetically be provided by IATA. This solution minimizes risk to airports as they will not be responsible for holding biographic passenger data.

Trends Identified

A self-sovereign approach is the most promising form of passenger data management. Under this model the passenger would control what personal data he/she wants to share and with whom. This model is the one described above in the cross-border initiative, but could be applied more broadly to the entire passenger journey. This model is successfully been adopted in other industries, such as financial services, but the adoption of such a model in aviation is proving more challenging.

APPENDIX H

Case Study: Risk Management During Covid-19 Using Biometrics at Carrasco International Airport - Montevideo, Uruguay (MVD)

Executive Summary

Carrasco International Airport has successfully implemented biometrics at its border control and boarding checkpoints at arrivals and departures, significantly increasing processing capacity at those points. With only international flights, all of the passengers go through border control, since 2016 choosing for the new e-gates, or queueing for the control podium. At the e-gates, the passengers automatically enroll by scanning their passport, selecting their flight on a touch screen and having their picture taken. If the picture matches the biometric information on the e-Passport and no other issues are present, the passenger is allowed to exit or enter the country. With successful enrollment, for the departures process, the passenger can then complete boarding by simply approaching the e-gate at the boarding gate and having his/her face scanned. A positive match opens the gate and all personal private information is purged 30 minutes after departure. Passengers wishing not to use the biometric enabled checkpoints may opt out and use the legacy facilities.

Processing times at the border control gates have been reduced from 40-50 seconds to approximately 15 seconds, for those passengers with eligible e-Passports and boarding times have also decreased. Additionally, it has reduced passenger and ground staff interaction and contributed to a more seamless and touchless passenger journey, improving health safety at the airport.

The use of the technology also enabled early 2020 the border control authority to initiate risk profiling during the arrivals process, related to Covid-19 risks. Passengers arriving from low-risk countries were able to pass through the border e-gate quickly, while passengers from higher risk countries were easily directed to a secondary screening or additional health check. This greatly reduced the need for increased staff and other resources otherwise needed to check all passengers by their origin. This was all made possible by integrating data defined as Advanced Passenger Information and PNR into the system platform.

Key Facts

Table H-24: Key facts of case study on risk management during COVID-19 with biometrics

What?	• Border and boarding biometrics enabled, and implemented risk management for Covid-19 • 1:1 matching at border control

	• 1:few matching at boarding
Where?	• Carrasco International Airport, Montevideo Uruguay
Passenger process steps:	• Departures: o Border control o Boarding • Arrivals: o Immigration
Who?	• **Lead:** Corporacion America (Centre of Excellence) - Easy Airport Consulting Division • **Stakeholders:** Airport Authorities: Border control (immigration), Vision-Box (global vendor), Air Europe and LATAM
Why?	• Improve passenger processing speed though airport • Improved security as border officers can focus on high-risk passengers • Allow risk-based profiling for Covid-19 testing and
How?	• Two biometrically enables e-gates by Vision-Box, operating system a collaboration between Vision-Box and Corporacion America. • The placement of e-gates at border control as well as e-gates at boarding. The e-gates at border control verify the passport that is scanned (1:1 matching), let the passenger select their flight and then takes a picture of the passenger's face for the temporary biometric token. • At boarding, the scanning of the passenger's face and subsequent successful matching (1:few) allows passage through the e-gate for boarding the aircraft
Enrollment / Digital Identity creation and verification	• No prior enrollment is needed. All is done at the border control checkpoint. • Identity is verified by reading the e-Passport and comparing to the stored biometric on the e-Passport to the live picture taken of the passenger's face • TRIP model token – the biographic and biometric information used for the token is only used for one trip
Verification of identity how?	• Matching of the e-Passport's stored facial biometric with the image taken of the passenger's face at the e-gate (1:1 matching)
For?	• International passengers only (MVD airport only has international connections) • Currently limited to passengers with: o Uruguayan e-Passport or ID card o e-Passport from other countries that do not have visa requirements

Introduction

At the largest and international-only (no domestic services) airport of Montevideo in Uruguay, named Carrasco International Airport (Montevideo Carrasco Airport, 2020), the airport operator Corporacion America has made significant progress in piloting and subsequently implementing in full a biometric system

that automates most of the border crossing and boarding steps in the passenger journey. The airport has taken a leadership role in South America, as the first to implement biometric solutions (Vision-Box, 2018a).

How Does it Work?

System Architecture, Pre-Existing Systems and Databases

The biometric solutions at Carrasco airport are found at the border control e-gates and the boarding e-gates. A collaboration between Vision-Box and the Centre of Excellence team of Corporacion America – specifically the Easy Airport Consultation Division (Easy Airport, 2020) – resulted in the creation of an inhouse operating platform, based on Vision-Box's Orchestra architecture. The system is connected to API and is also linked to airline DCS systems so it has access to PNR. This tailormade system enables the operation of the e-gates, facilitates the temporary storage of the recorded biometrics and provides a portal "EasyWeb" for its users and stakeholders.

The EasyWeb portal is a unique feature, and one that required most of the custom programming in-house. The portal allows airlines to track the passengers through different checkpoints during their airport journey. This allows the airlines to have a complete picture of the passengers who are ready for boarding, or who might still be underway to the gate.

The EasyWeb portal also offers the airport Operational Control Centre (OCC) and third-party stakeholders some additional features, such as:

- Dashboards of useful information such as waiting times, passenger flow statistics
- Anonymized statistics of passenger flow; wait times, movements and dwell times through the airport passenger journey

The Passenger Journey

For the departing passengers, enrollment using biometrics prior to the arrival at the airport is not needed. With a confirmed flight booking, the passenger can check in online, or at the airport, drop off baggage and then continue to the pre-security e-gate. At this point, only a valid boarding pass is scanned allowing the passenger to continue to proceed to airport security.

After clearing security, biometric enrollment is done at the border control checkpoint, since all flights at MVD are international. At this e-gate, the passport is scanned and the passenger selects his/her flight on the touchscreen, after which a live picture is taken of the passenger. The passenger's identity is verified comparing the passport's stored biometric information to the live picture, and if verified, passage is granted through the e-gate (Vision-Box, 2018b).

The facial biometric is then stored temporarily in the system and passed to the e-gate at the correct boarding gate. When the passenger arrives at the boarding gate at the designated time, he/she will be granted passage in case of a successful match (1:few).

For the arriving passenger, he/she will only encounter the biometric enabled border control gates, that verify one's identity through facial recognition and comparison to the stored biometric information in the e-Passport or ID card, similar to the departure process.

Retention and Storage

The government of Uruguay has a fairly modern approach to personal private information (PPI) and has laid down strict rules for the capture, use, retention and deletion of the information. The highest goal is to keep the information safe, delete it when possible and make sure that if other parties want to use it, the information has to benefit the whole community.

At MVD, the stored biographic and biometric data that is linked to flight information is purged 30 mins after departure. What remains are the non-identifiable statistical data points that benefit, for example, the airport OCC, the airlines or other third parties.

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

Stakeholders and Responsibilities

Stakeholders

The project was led by Corporacion America and in collaboration with the airport (government) authorities at Montevideo, as well as the vendor Vision-Box. The main stakeholders include the two main airlines at the airport Air Europa and LATAM and several airport departments.

Responsibilities and Governance

Corporacion America, the airport authority has taken up the lead for this project and has put in place multiple working groups to make this effort a reality.

Use Case Review

Benefits

The main benefits of the implementation of the biometric enabled e-gates at MVD have proven to be:

- improved security
- improved health safety
- reduced staffing requirements
- faster border crossing and boarding times
- Covid-19 related risk profiling of passengers

The first benefit relates to the improved security, as the border control officers have more availability to focus their time on high(er)-risk passengers. Instead of having to process all the passengers and focus the majority of their time on checking low-risk passengers, the border control officers can now invest most of their time on more high value activities. This improved the border control officers' performance, as well as job satisfaction. Also the security of flights increased. When boarding 200 passengers in 20 minutes and airline ground staff often times being stressed or in a rush means that the extra time needed to accurately check each passport picture would be under pressure.

A more recent focus and benefit is the reduced number of interactions with ground staff and common touch points. The biometric enabled e-gates have made the passenger journey at MVD take a leap towards a fully touchless, seamless journey. Less touchpoints, less interaction decreases the risk of transmission of communicable diseases, for example, as Covid-19

Overall, the EasyAirport system, together with the EasyWeb portal have allowed the airport and the airlines to adopt a much more data-intensive operation, learning to better allocate resources and plan ahead. Data-driven solutions have, for example, reduced some staffing requirements at checkpoints, or reallocated the priority of their jobs. Also, with the portal, airlines have a complete picture of the passengers who are

ready for boarding, or who might still be underway to the gate, improving the effectiveness of what the ground staff could offer in their service. This was a major incentive for the airlines to join the program.

For both airlines and passengers, the faster border crossing and boarding of aircraft was a big benefit. Traditional border crossing checks would typically take 40-50 seconds and are replaced by a 15-second e-gate checkpoint. For airport capacity this is a huge improvement. For boarding, in some examples, double or even triple the boarding speed was achieved, as larger percentages of the passengers could use the facial biometric enabled e-gates. LATAM shared that it's ground staff could manage the boarding process much better and provide a better passenger experience.

The use of the technology also enabled early in 2020 the border control authority to initiate risk profiling during the arrivals process, related to Covid-19 risks (Cerri, 2020). Passengers arriving from low-risk countries were able to pass through the border e-gate quickly, while passengers from higher risk countries were easily directed to a secondary screening or additional health check. This greatly reduced the need for increase staff and other resources otherwise needed to check all passengers by their origin. This was all made possible by integrating data defined as Advanced Passenger Information and PNR into the system platform.

Responses from Passengers

Passenger reviews on the new systems, even if their knowledge on how the systems work was very basic, have been very positive. The passenger satisfaction has been very high since the installation in 2016, regarding the use of biometrics (Mujica, 2020).

Fall Back Options

For the two biometric enabled checkpoints, the normal legacy checkpoints are still available throughout the airport. The implementation of the new systems has since 2016 seen a steady rise in adoption, due to the phased availability to different nationalities and government ID cards. As adoption keeps rising, resource allocation for the legacy checkpoints will likely decrease.

Concerns

A primary concern of the government authorities was the correct and proper use of data, minding the privacy of the passengers. The design of the system followed stringent requirements to protect private information (biographic and biometric) and for stakeholders that wanted to use the EasyWeb portal, information had to be given to all stakeholders about how they would use the anonymized data, and explain to what purpose. For several third-party stakeholders, the wealth of information was used for making the airport better in terms of passenger services, less waiting times, and improvements across the entire airport system. If stakeholders shared their intended use of the non-PPI information, then they are allowed to join and have access to the portal. In this instance, the government agencies maintained control over the admissions.

No real other concerns were voiced by the airport authority, neither regarding the communication or education of passengers, nor about violations of privacy rights of passengers.

Lessons Learned

The main lessons learned can be grouped to the following:

- Leveraging security improvements in the business case with stakeholders for collaboration
- Iteration of improving the capturing of facial biometrics: influenced by lighting, time of day, face masks and user feedback

- Not all airlines were initially rushing to implement and collaborate, but Covid-19 and the new focus on health measures changed that
- Limited eligibility of passports causes slow increase in passenger adoption

A lesson learned from the discussions with potential airline stakeholders was that rather than just the ROI, also the improved security proved of high importance convincing participation in the collaboration (Cabrera, 2020). Government agencies noted the improvement in security was a major driver.

The capturing of facial biometrics with cameras installed in the e-gates was improved several times after learning the influence of lighting (time of day, light conditions outside, added lighting in the e-gates) as well as the sudden mandatory use of masks to prevent the spread of Covid-19 in the airport. In the latter case, the actual algorithm for comparing and matching the biometrics was changed, to meet the required standards today. To add to that, due to communication with airport staff and passengers, the e-gate went through several iterations of design. This changed the method of capture of the facial images, as well as the interaction of the passenger with the e-gate. Examples were changes to the messaging, layout of the touchscreen and the overall lighting conditions at the e-gate.

Initially, not all airlines were in the same hurry to implement. Air Europa and LATAM wanted to introduce the new systems primarily to reduce staff, increase efficiencies, and improvement in safety, security. These airlines already had a strong digital and online presence, so facilitating online check-in and such was already part of their process. For smaller and more local airlines, participation with the project would cause they have to upgrade their back-end systems. This meant these airlines would first have to invest in their own systems. With developments around Covid-19 and the move towards touchless passenger facilitation, many more airlines have joined the project. Only in the last month (due to touchless) are these airlines also interested.

The use of the e-gates was first limited to Uruguayan e-Passports, counting for about 15%-20% of the passengers, followed by Brazilian and Argentinian e-Passports, another 10-15%. In time, also Uruguayan ID cards were allowed, as travel within South America does not require passengers to have a passport. Thereafter, e-Passports of passengers from countries not requiring visas were also allowed to use the e-gates. The above caused a slow increase in the technology adoption. Theoretical coverage of users is 97% but a very large percentage of the Brazilian population traveling to Uruguay does not have a passport, only an ID card but one that is not updated. In this case, the policy of a foreign country to not have up-to-date identification documents influenced the adoption rate in Montevideo. Real user adoption rates are currently closer to 50%.

Findings and Trends

Findings

Easy Airport presented the ability to meet different airline business cases and strategic objectives, including resource and time savings. It also presents the opportunity to install state of the art technology and infrastructure to meet the airports future demand. The added data portals for airlines and other stakeholders is a bonus, which delivers anonymized data streams. More interestingly, *Easy Airport*, was used during the Covid-19 pandemic in risk-profiling passengers into specific categories, automatically, and notifying border agents of passengers entering the country from specific origins. Those passengers underwent a different (health) screening process.

Some key lessons learned for the airport authority and implementing teams were around the protection of passenger privacy and information, transmission of such information to foreign governments, especially regarding legal frameworks between the project stakeholders.

Future Situation and Broader Implementation

One of the future considerations, according to MVD, is looking into including children in the program, as currently e-Passports are only available for citizens 18 year or older. This would greatly improve the passenger experience, as currently travelers with children have to utilize the legacy system, and verify the identity with regular identity cards or passports.

The use of facial recognition has also been opted for the pre-security check currently only requiring a valid boarding pass. This would shift the location for the enrollment possible to earlier in the passenger journey. The aim is to allow all touchpoints in the passenger journey to be facilitates with the EasyAirport biometrics solutions.

Trends Identified

The main trend identified in this Case Study is the increasing utilization of biometric solutions to improve the passenger experience, create a seamless journey, and allow for less physical interaction with ground staff and touchpoints. The EasyAirport the passenger journey in Montevideo well in the directino of becoming completely touchless, althgouh several points of interaction still exist. Integration with other airport authorities and possibly the increased use of mobile devices will see this move forward.

APPENDIX I

Case Study: Digi Yatra and the Seamless Passenger Journey at Kempegowda International Airport, Bengaluru, India (BLR)

Executive Summary

In 2016, as part of the new terminal development program, BLR staff conducted a series of workshops to discuss the future of the passenger journey and how this could be facilitated by a single biometric token. The BLR Innovation Lab further developed the concept of operations and explored different types of biometrics, including face, fingers and iris. In January 2017, BLR rolled out its first Digi Yatra trial, which went live on a Vistara Airlines flight (Airport Technology, 2019) (Bureau ET, 2019). The initiative was then quickly expanded to AirAsia India and Spice Jet, and is now set to include all domestic airlines. International flights will be involved at a later stage (Future Travel Experience, 2019a).

At the heart of the initiative is the Common Digi Yatra ID Platform, an interface platform between the country-wide biometrics database owned by the Unique Identification Authority of India (UIDAI) and the local airport ID Management platform (IMP).

To partake in the Digi Yatra seamless journey, the departing passenger can create a Digi Yatra ID any time prior to his/her trip. This is a one-time process which can be done online or in-person at one of the airport's registration kiosks, using a government-approved ID number (including a unique identifier if the passenger has previously been registered in UIDAI database) or a manual ID card. In case a manual ID card is used, an additional physical check by an officer is required at the registration kiosk. Once completed, the Digi Yatra ID is activated and will be permanently valid.

The passenger can enter his/her Digi Yatra ID number at the time of ticket booking, which is then transmitted by the airline Departure Control System (DCS) to the airport IMP.

On the day of the travel, the passenger arrives at the airport registration kiosk, scans his/her boarding pass and has his/her iris and face captured by the kiosk's camera. The passenger's consent is taken to use his/her face biometrics for the journey. The Digi Yatra ID platform performs boarding pass validation with the airline DCS and a real-time biometric validation to verify the passenger's ID. At this point, a digital template of the passenger's face biometrics is activated in the airport IMP, and a single token combining this digital template with the PNR is created. This single token, also called the "passenger dataset", grants the passenger seamless and paper-free accessibility through the rest of the biometric-enabled processing points. In case of no-match or if the passenger wishes to opt-out, a manual verification of the travel document and identity is performed at each processing point.

A passenger's data storage and retention vary by each database. On the one hand, the Digi Yatra ID will exist indefinitely after activation. The passenger can update his/her profile if necessary, and can choose to opt-out at any time he/she wishes. On the other hand, the "passenger dataset" stored and retained in the airport IMP will be deleted one hour after the corresponding flight departs.

The Digi Yatra trial at BLR showed promising results, as passenger processing times at biometric-enabled processing points considerably decreased compared to the manual process. The airport is aiming

towards having 60 to 70% of passengers using the biometric-enabled journey. Once this goal is reached the true magnitude of the reduction in processing times and staff count will be fully visible and measurable.

At the moment, due to the Covid-19 pandemic, the Digi Yatra ID platform's deployment has been delayed and a manual validation process is in place. BLR is currently exploring the possibility of trialing another option, referred as a "self-sovereign" approach. Under this model the passenger would control what personal data he/she wants to share and with whom. The passenger would complete the enrollment process using government-issued validation number; would then take a selfie, unlock the e-Passport chip (via the same app) and combine this information into a digital token that he/she can share with the airline and with the airport. BLR is in the process of exploring and potentially trialing this option in the near future.

Key Facts

The table below summaries the key aspects of the seamless passenger journey at BLR.

Table I-25: Key facts of the case study on Digi Yatra

What?	• Digi Yatra: seamless, biometric-enabled, paperless journey
Where?	• Kempegowda International Airport Bengaluru, India (BLR)
Passenger process steps:	• Outbound domestic passenger journey (curb to gate) (to be expanded to international flights at a later stage) • Enrollment kiosk • Airport entry e-gate • Check-in/bag drop • Security entry • Emigration (at a later stage) • Boarding e-gates • In the aircraft (tablets with biometric identification) (at a later stage) • Immigration (at a later stage)
Who?	• The Digi Yatra is a Ministry of Civil Aviation's initiative in partnership with the major privatized Indian airports and the IAA. The common Digi Yatra ID platform, once operational, would enable the automated validation of the passenger's identity. The platform has not been implemented yet (due to Covid-19), but BLR has biometrically enabled several of the touchpoints listed above and linked them into their own localize ID management platform. The ID validation process is still performed manually until the Digi Yatra platform is operational or a different approach such as the self-sovereign ID management approach is implemented. • The initial BLR trial was launched in partnership with Vistara Airlines. The selected vendor was Vision-Box who provided the airport ID biometric platform technology (Orchestra). After Vistara Airlines, AirAsia India and SpiceJet were added. The program is now on a full roll-out stage to include all domestic airlines (IndiGo is the last remaining domestic carrier to be included). The program will be expanded to international flights at a later stage.
Why?	• The Ministry set several goals for Digi Yatra:

	○ Delay costly airport capital expansions by looking at innovation and digitalization to improve efficiencies and reduce costs ○ Provide a better and easier passenger experience ○ Enhance security standards ○ Back up the program with a strong, verifiable government-issued identity ○ Provide a common identity management system that would work across all domestic airports in India and that could be used by all domestic and international passengers ○ Use Digi Yatra as a mean of communication with all enrolled passengers
How?	• The Common Digi Yatra ID platform was conceptualized by a joint venture between the Government (with majority stake), the AAI (with minority stake) and all private airport operators. The Common Digi Yatra ID platform offers core passenger services such as enrollment, authentication, consented profile sharing. Passengers have to enroll once using a valid Government issued ID. The local airport identity management system uses the face biometrics data provided by the Digi Yatra ID platform to identify the passenger for all the processes inside the airport. The face biometrics data is purged out of the airport system one hour after the passenger's flight takes off. • In the interim, until the Digi Yatra platform becomes operational, the identity check is manually performed.
Enrollment / Digital Identity creation and verification	• Passengers can enroll in the Digi Yatra online by providing a valid Government ID (preferably the Aadhaar number, which is a 12-digit unique identifier that the Government issues to all its citizens after biometrically enrolling them into this country-wide program). Passenger obtain a personal Digi Yatra that has permanent validity. The activation (validation) process is performed once online or at an airport registration kiosk (where a photo-of-the-day is taken and the identity is validated against the Government database accessible through the Aadhaar number). In all subsequent trips this step is no longer needed if the passenger, at the time of booking, includes his/her personal Digi Yatra number to his/her reservation.
Verification of identity how?	• If the passenger uses his/her Government-issued Aadhaar number, the verification and activation is performed once by matching the "photo-of-the-day" with the Government-held biometrics data, accessible through the Digi Yatra ID platform. If another form of Government issued ID is used (other than the Aadhaar number), the ID has to be manually checked at the airport to complete the activation process.
For?	• All domestic flights on Vistara Airlines, AirAsia India and SpiceJet. To be expanded to IndiGo and all international flights. (ET Government, 2020) (Business Traveller India, 2020) (Press Trust of India, 2020)

Introduction

Aviation in India has been growing at a considerable pace and India is expected to become the world's largest domestic civil aviation market in the next 10 to 15 years. More and more emphasis has been placed on investing in innovation and digitalization to keep up with this tremendous growth.

To this effect, the Ministry of Civil Aviation has started Digi Yatra in partnership with the privatized Indian airports and the Airports Authority of India (AAI). This major initiative aims at transforming the passenger experience at all Indian airports and re-inventing its airport terminals, explicitly rejecting the conventional "build a bigger Airport to manage more Passengers" approach.

Specifically, Digi Yatra makes use of biometrics and identity management technologies to allow a seamless, paper-free journey (Awtaney, 2019). As one of Digi Yatra's stakeholders, BLR became one of the first Indian airports that trialed the concept: passengers only need to show their face to gain access to all terminal processing checkpoints, eliminating the requirement to repeatedly show travel and identification documents. (Devaiah, 2019)

How Does it Work?

Before the Passenger Journey

The Common Digi Yatra ID platform is an interface platform between the country-wide biometrics database owned by the Unique Identification Authority of India (UIDAI), under the Ministry of Electronics and Information Technology and the local airport ID Management platform (Bhavan, 2018).

Specifically, the three platforms are:

- UIDAI platform—Country-wide database where Indian residents' demographic and biometric data is held; UIDAI is responsible for enrollment, updates and authentication; any Indian resident can enroll by providing a proof of identity and a proof of address; as part of the enrollment process, at the enrollment center, a photo, finger-prints and iris scans are taken; once the authentication is performed (within 60 to 90 days), a unique number, the Aadhaar number, is issued; the number has indefinite validity and can be used to validate identity; obtaining an Aadhaar number is not mandatory.
- Digi Yatra ID platform—Country-wide airport system database, where the demographic and biometric identity data are linked to travel bookings; the enrollment is completed on-line and it is valid indefinitely; the activation is done once, at an airport registration kiosk (if the Aadhaar number is used, that constitute a valid proof of identity; if there is no Aadhaar number, the activation process is performed by a manual validation of a Government-issued ID document); the validation is valid for 5 years; at the time of booking, the booking reservation number is linked to the Digi Yatra number and to the demographic and biometric data in a single ID token; this is possible because of the integration of the airline's DCS with the Digi Yatra ID platform. (Government of India, 2020)
- Airport ID management platform—BLR uses Vision-Box's Orchestra ID management system to validate identity at the biometric-enabled passenger processing points (entry e-gates and all other downstream processing points); only the photo capture (biometric data) and the PNR is shared between Digi Yatra and the airport platform. (Burt 2019)

Due to Covid-19, the Digi Yatra ID platform is not operational and therefore automated identification validation is not possible and the PNR is not automatically shared with the airport own platform. Therefore, the identity validation is currently performed manually at the registration kiosk and the PNR data capture is done at the airport e-gate by having the passenger scan his/her boarding pass.

BLR is exploring another option that would empower the passenger to digitally share his/her biographical and biometric data when required via an app. This approach is broadly known as sovereign ID management approach. The passenger would complete the enrollment process using his/her Aarhaad number; would then take a selfie, unlock the e-Passport chip (via the same app) and combine this information into a digital token that he/she can share with the airline (during the booking process) and with the airport (to access the

biometric-enabled processing points). BLR is in the process of exploring and potentially trialing this option in the near future.

The passengers completes the on-line Digi Yatra enrollment process and are issued a Digi Yatra number. As mentioned before, the enrollment has to be completed only once. At the time of booking, passengers are asked to include their personal Digi Yatra number in their booking reservation which is then transmitted by the airline DCS to the airport ID management platform; the PNR number on the boarding pass is used as the key to extract the passenger's Digi Yatra ID number from the airport ID Management platform at the time of validation at the airport entry e-gate. (Khadakbhavi, 2020)

Note: *The immigration and "in the aircraft" processing points will be incorporated in the journey at a future stage.*
Source: Digi Yatra Biometric Boarding System Report, Ministry of Civil Aviation, Rajiv Gandhi Bhavan, New Delhi- 110003.

Figure I-2: The Digit Yatra Journey Concept

The Passenger Journey

Registration kiosk—The passenger scans his/her boarding pass (printed on paper or on his/her mobile app); the kiosk camera captures the passenger's biometrics (face and iris for Aadhaar validation); the passenger's consent is given to use his/her face biometrics for other airport processing points; the Digi Yatra ID platform validates the boarding pass with the airline DCS and verifies the identity of the passenger with real-time biometric validation within the Digi Yatra ID Platform (or, if this the first time, the Digi Yatra ID platform performs a one-time validation of the passenger with the Aadhaar system using face and iris biometrics data); the passenger's face biometrics digital template is activated in the airport ID management platform with the creation of the "passenger dataset" which includes the face biometrics digital template and the PNR for identification at the other biometric-enabled processing points at the airport; the "passenger dataset" is associated to a unique identifier; the face biometric digital template is updated to the Digi Yatra ID platform .

Airport entry e-gate—The passenger having completed the registration process can now access the airport entry e-gate; the passenger is identified by the "passenger dataset" and the e-gate opens.

Other biometric-enabled processing points—as per above, the passenger is identified by the "passenger dataset".

In the of a no-match or if the passenger wishes to opt-out, a manual verification of the travel document and identity is performed at each processing points.

Retention and Storage

Storage and retention of the passenger data varies by database:

- Digi Yatra—the passenger data is retained indefinitely or until the passenger elects to do so; the passenger can update and modified the information in his Digi Yatra profile, if necessary.
- The passenger dataset (photo and PNR) is stored and retained in the airport ID management platform only until one hour after the flight departs. After that, all data has to be deleted.

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

Stakeholders and Responsibilities

The following paragraphs summarize the various stakeholder and their responsibilities.

Stakeholders

This initiative is a partnership among the Ministry of Civil Aviation, the privatized Indian airports and the Indian Airports Authority. BLR is one of the first airports that started trialing the concept in 2017. The launch airline was Vistara Airlines, but the program was quickly expanded to include other domestic airlines, AirAsia India and SpiceJet. Other airlines, including international carriers, will continue to progressively join the program.

Responsibilities and Governance

The Digi Yatra program's governance can be summarized as follows (Khadakbhavi, 2019):

- The Secretary of Ministry of Civil Aviation is in charge of the overall initiative
- A Steering committee (Digital Cell) comprising of the CEOs of major Indian Public Private Partnership airports (including BLR executives), Airports Authority of India (AAI), Bureau of Civil Aviation and Security (BCAS) and Central Industrial Security Force (CISF)
- A technical working committee (TWC) which comprises of subject matter experts from the participating airports, including staff from BLR, and the BLR Innovation Lab.
- The TWC conducted a series of workshops with all stakeholders including airlines, on-line travel agents, regulators, airports and the UIDAI, to explain the concept of Digi Yatra and gather consensus among all stakeholders.

Timeline and Planning

In 2016, as part of the new terminal development program, BLR staff conducted a series of workshops to discuss the future of the passenger journey and how this could be facilitated by a single biometric token. The BLR Innovation Lab further developed the concept and explored different types of biometrics, including face, fingers and iris.

Procurement and Vendor Selection

Once BLR developed the concept of operations, a selection process involving several leading biometric service providers, was conducted and the preferred vendor, Vision-Box, was selected. The trial went live on a Vistara Airlines flight in January 2017. (Mayhew, 2018) (Vision-Box, 2018) (Vision-Box, 2019)

Case Study Review

Benefits

The benefits for the various stakeholders are highlighted in the table below (Khan, 2020).

Table I-26: Digi Yatra and the Seamless Passenger Journey - Stakeholders benefits

Stakeholder	Benefits
Passengers	Enhanced experience with a more seamless journey; no need to show boarding pass or ID at multiple processing points
	Faster processing and reduced queue times
	Same program across Indian airports
Airport	Increased passenger processing throughputs postponing the need of costly capital expansion programs
	Enhanced passenger experience and simplified processes, accessible to all including less tech-savvy passengers
	Better resource planning by knowing passenger loads and locations
	Reduce staffing costs as fewer passengers have to be manually processed
Government	Enhanced security: minimize ID fraud, reduce the risk of allowing non travelers into the terminal
	Scalability of the program to all airports across India
	Leverage of the country-wide UIDAI Aadhaar database to make identification more secured and streamlined
	Reduce staffing costs as fewer passengers have to be manually processed
Airlines	Better resource planning
	Improved on-time departures, by knowing where passengers are within the terminal
	Redeployment of staff where most needed

Responses from Passengers

The feedback from passengers was very positive. The majority found the process easy to understand and they appreciated the convenience of not having to show multiple times the same documents. Passengers also noticed that queues were shorter and the processing times faster than before. Non-tech savvy passengers could also successfully use the system, given its simplicity.

System Performance and Specifications Review

One of the main challenges had to do with the ambient lighting that impacted the cameras, resulting in bad quality images at some of the processing points. These images could not be used for matching purposes. This problem was addressed with manual intervention. As image capture technology and image enhancement algorithms continue to improve this challenge should be overcome.

Fall Back Options

If the passenger is not enrolled in the Digi Yatra program or if the authentication process for some reason does not work (no match), the passenger is processed manually at each processing point (valid Government-issued ID and boarding pass are checked at each checkpoint). The passenger is still processed through the airport entry e-gates, albeit manually. Today some of the terminal entry points do not have entry e-gates and passengers with disabilities or others requiring assistance can use these staffed entry points.

Concerns

To respond to privacy concerns, privacy considerations were addressed and incorporated early on into the concept development process. The techniques implemented to achieve data Privacy by Design included authentication protocols, verification of credentials, encryption, data minimization, privacy enablers in databases, data masking, secure data storage and transparency enhancing techniques.

The system is fully GDPR compliant and all passenger data and travel records are purged from the airport ID management platform one hour after the flight departs.

In addition, the Digi Yatra policy prevents airports from creating a profile of users and using that for marketing purposes without passenger's consent. Once enrolled, Digi Yatra users can opt-out of the system and, at any time, they can delete their profile.

Lessons Learned

Understanding how passengers interact with the cameras and the equipment is fundamental to achieving positive outcomes. For example, passengers travelling in groups would be crowding around the device preventing the system from properly working. At BLR the processing of passengers, even if travelling in groups, is done one by one and therefore, having more than one person standing in front of the camera creates matching issues. This was resolved by signage and by deploying adequate staff to coach the passengers along the journey. As passengers become more familiar with the technology, some of these challenges will be overcome.

The current Covid-19 pandemic is accelerating the need to implement touchless technology and minimize the manual handling of IDs and travel documents. Touchless technology was not until now the focus of the effort as some of the touchpoints still require some interaction (e.g., registration kiosk, bag tag printer). Going forward touchless solutions at all processing points will be further explored and implemented.

Findings and Trends

Findings

The decrease in passenger processing times is considerable, especially at the airport entry e-gates with a decrease of approximately 50% if compared with the manual process. The boarding e-gates are also registering faster processing times. The airport goal is to have 60 to 70% of passengers using the biometric-

enable journey. Once this goal is reached the true magnitude of the reduction in processing times and staff count will be fully visible and measurable.

Future Situation and Broader Implementation

By the end of 2020 it is anticipated that all passengers travelling on domestic flights will be able to use all the biometric-enable touchpoints. The program will be extended to international flights, airline by airline, starting in Q2 2021, assuming the inherent complications associated with immigration processes can be resolved. (Lakshman, 2020) (OT Staff, 2019)

The Digi Yatra common ID platform implementation has been delayed due to the global Covid pandemic. As Indian airports re-prioritize their investments during these uncertain times, it is unclear as to when the program will resume in the future. Before the crisis hit, the design phase was completed and the RFP to select the vendor had been prepared. Therefore, the reactivation of the program, once the decision is made, should be quite straightforward.

In the meantime, BLR has been exploring another identity verification solution that would not require the Digi Yatra platform and it is based on the concept of self-management of digital personal data, to empower each passenger on what personal data to share and with whom. The passenger would enroll by using an identity app on his/her phone to take a selfie to verify biometric and biographic information, by reading the chip on the e-Passport or by using the Aadhaar number and the user-specific password generated by the UIDAI. At the time of booking, this app interfaces with the airline app to combine the biometric and biographic data with the PNR and generate travel credential that can be shared with other parties, such as the airport and the Government (if, in the future, border processing is included in the seamless journey). At the airport entry e-gate, the passenger, by showing his/her face and scanning his/her boarding pass, gains access if there is a positive match in the local airport IMP (the PNR is valid and the passenger is who she/he say they are). The remaining processes are the same as before. This concept is still in an exploratory phase and more work has to be done to make it a reality.

Trends Identified

BLR staff have identified several learning and trends during the planning and implementation of the seamless journey:

- The vast majority of passengers have embraces this technology and appreciate the benefits that it provides; this trend is in-line with the latest IATA Global Passenger Survey
- The success of this initiative is due to the adoption of a very collaborative approach as all key stakeholder were invited to participate from the very early conceptual stages

The self-sovereign ID management is probably the best way forward as it empowers individuals to decide with whom and how to share their personal data

Sources

Future Travel Experience. “Bengaluru International Airport Introduces Kerb-to-Gate Biometric Journey.” Future Travel Experience, July 25, 2019. https://www.futuretravelexperience.com/2019/07/bengaluru-airport-kerb-to-gate-biometric-journey/.

APPENDIX J

Case Study: Happy Flow at Aruba's Queen Beatrix International Airport

Executive Summary

Happy Flow is aimed at improving the departure process at Aruba's Queen Beatrix International Airport (AUA), by smoothening the flow, and creating a unique and seamless passenger experience. The program adopted protocols and standards that would benefit authorities, the airport and airlines.

Using facial recognition at multiple passenger touchpoints, passenger identity and right to travel are verified more securely. Plans are underway to include off-airport elements in the passenger journey (hotel check-in and car rental). In the initial launch of Happy Flow, there were also ideas to pre-clear into European Schengen.

In the process, travel documents are only required at the enrollment station. There, the passenger's identity is securely checked, and a virtual identity is created. After enrollment, the passenger goes through self-service passenger touch points (bag drop, security, border control and boarding) where the passenger's face is matched to a secured database, only allowing authorized passengers to pass.

As with other facial recognition initiatives and programs, the intent of Happy Flow was designed to promote a more streamlined departure process while improving overall security. Enrollment is the most time-consuming step, while processing is very efficient after the biometric token is created. The system can be further optimized by introducing one-time enrollment such as Digital Travel Credential, as well as measures to counter identity fraud from off-site/mobile enrollment.

Key Facts

Table J-27: Key facts of case study on Happy Flow in Aruba

What?	• Seamless passenger process using facial biometric matching
Where?	• Queen Beatrix International Airport, Aruba
Customer process steps:	• Process as the predecessor of IATA Seamless flow (OneID) • Departures: o Biometric enrollment per flight (verify passenger ID + boarding card) o Baggage drop-off with biometric assistance (counter with camera for walking pace facial recognition that pulls up PNR o Biometric self-service border control checkpoint (exit check) combined functionality with airside check (reservation and travel document)

	○ Duty free and airside terminal area (conventional, no applications of Happy Flow) ○ Boarding gate with separate Happy Flow lane (with camera for facial recognition)
Who?	• Aruba Airport Authority N.V. (AAA) together with KLM Royal Dutch Airlines and the Government of Aruba. Supported by the Ministry of Justice in the Netherlands, KMAR (Dutch border police), Royal Schiphol Group, Vision-Box
Why?	• To improve the passenger experience, save time and make the passenger process more efficient for airline and airport
How? Technology used	• Verification of the ID and facial imagery takes place at the biometric kiosk. Therefore, front-loading and splitting the border control process: • Identity verification at the kiosk by authentication of the e-Passport and biometric verification of the holder and the biometric on the e-Passport under government control • Biometric ID verification and exit control at border control • Privacy by Design principles/GDPR were adhered to from the start of the project
Enrollment / Digital Identity creation and verification	• Enrollment per departing flight at the self-service biometric kiosks when entering the Terminal: • Check-in through airline's systems conducted online or via CUSS kiosks. • At the seamless flow kiosk: ○ step1: verify identity with biometric data on passport and authenticate passport ○ step 2: scan boarding card at kiosk ○ step 3: create a Digital ID is created and temporarily stored in a passenger data envelope together with boarding card details
Verification of identity how?	• First by machine check of the authenticity of the passport in accordance with Frontex ABC standards. Then by comparing the image stored on the passport with the person in front of the enrollment kiosk.
For?	• KLM departing passengers to AMS (16+) with e-Passport valid for participation (EU/EER nationals, United States, Canada)

Introduction

In 2012, the Government of Aruba, Ministry of Justice in the Netherlands, Queen Beatrix International Airport, KLM and the Schiphol Group agreed on starting up an innovation project aimed at improving the passengers' experience, smoothen the flow, and facilitate the process at Queen Beatrix International Airport. The program was to adopt such protocols and standards that it would benefit the authorities, the airport and the airline, and potentially even bring relief to the immigration process at Amsterdam Airport Schiphol for the arriving flights from Aruba, but most of all that it would create a unique and seamless passenger experience.

The improved passenger experience has been the shared driver of the workgroup throughout the years and turned out to be the vital element in innovation and realization. This shared goal, independent from

individual stakes and interests, created a shared sense of responsibility and motivation. Along the passenger process, each stakeholder benefitted directly or indirectly from these improvements due to improved bilateral ties, increased passenger satisfaction, reduced queues and inefficiencies, and relieved pressure from authorities' operations. This resulted in the fitting "Happy Flow" process which hints at the Islands slogan, "One Happy Island" and the natural flow that was created. With the introduction of Happy Flow, the world's first biometric seamless passenger process was introduced. In the future, the concept is to be broadened to include mobile enrollment, the arrivals process of more airlines and off-airport services like hotels and car rentals.

How Does it work?

Before the Passenger Journey

Upon arrival at the airport the passenger can decide to participate in the Happy Flow program (Aruba Happy Flow, 2020). Upon enrollment at the airport at a biometric kiosk, the biometric data of the passenger including PNR and boarding card details are stored in the PDE. All PDE's are stored in a database located at the airport. The Aruban border police will receive all passport data for verification. The airline's DCS will receive the boarding card details to register boarding.

The Passenger Journey

Passengers that are over 16 years old, holding an e-Passport and travel with the daily KLM flight from Aruba to Amsterdam, are allowed to use the biometric systems provided at Aruba International Airport in the Non-U.S. departures area. Participation is optional, passengers can also follow the conventional passenger process.

Biometric Enrollment

Upon entering the main terminal building, passengers on the KLM flight get the choice to opt for the Happy Flow process. Provided that the passenger has passed online check-in, the passenger can enroll at the Happy Flow biometric kiosks for that day's flight.

The passenger needs to insert its e-Passport in the Happy Flow kiosk where the authenticity of the passport is verified, and the digital image of the passport holder is read from the passport chip by the machine. The built-in camera of the kiosk captures an image of the person in front of the camera, and confirms his/her identity by matching it with the image from the passport. The verification of the passenger's identity is done in the same manner as at an automated border control gate, in accordance with the European Frontex standards. This requirement is the foundation for the federated identity management system and an important part of the arrangement between the stakeholders on which the concept is based.

After confirmation of the passenger's ID, its details are matched against the law enforcement databases to verify if the passenger is eligible to leave the country. This is checked within seconds after enrollment, and the status is recorded in the system. In the passenger process this is well in advance of the actual border control checkpoint leaving ample time for border control agents to respond to passengers of interest. In fact, the border control procedure is now divided in two stages, creating potential new use cases for border control operations.

At the enrollment kiosk the passenger also has to scan the boarding card. When the time and date (of the flight reservation) are right, its boarding card details are stored in in the PDE of the seamless flow database together with its biometric template. When both verifications are positive and the document is authenticated, the biometric image that is captured of the passenger's face is stored in the seamless flow database and serves as the single token for the successive steps in the Happy Flow process.

Facial recognition cameras are used for every next step in the passenger process, essentially digitalizing and replacing the need for hardcopy documents (ID and boarding card). The passenger's face serves as a single token. At every biometric checkpoint only the minimum information from the PDE that is required for that specific process step will be shared with the system and stakeholder according to the Privacy by Design principles. As a result, passengers are no longer required to show their travel documents as is the case with the conventional passenger process. This leads to a quick and hassle-free process where at every step the passenger only needs to show his/her face.

The passenger's data stored in the seamless flow database includes the passport details, boarding card, and biometric template of the passenger's face. The data required for the passenger journey is stored by the seamless platform less than 24 hours and then deleted. The passenger needs to enroll for every new trip. The passport details and facial images are saved in a separate database of the immigration authorities for a longer term.

Source: Aruba Airport

Figure J-40: Image of a biometric enrolment kiosk for Happy Flow

Baggage Drop-off Based on Biometric match

After enrollment, the passenger proceeds to one of the separate hold baggage counters dedicated to Happy Flow. A camera integrated in the desk is directed to the passenger approach flow situated in front of the desk. When a passenger comes in view, facial recognition software will recognize the passenger's face and confirm the corresponding digital ID.

As the passenger will be recognized while approaching the desk, the staff at the desk already gets the PNR presented with the required travel documents on their workstation. Once the passenger is at the desk, they simply handover the baggage and can continue to the next step in the passenger process. The airline staff at the desk can insert the number of bags, print the label(s), and tag the bags.

Border Control Checkpoint (Emigration/Exit Check)

As the passengers make their way through the terminal, they arrive at the border control checkpoint where separate Happy Flow lanes are present. These lanes are designed as a mantrap, with barriers upon entry and upon exit. Inside, the lanes are equipped with cameras situated at the end of the lane that can move vertically inside a console to find the right camera angle to recognize and confirm the passenger's ID. When a passenger is recognized and authorized, the exit barrier will open. The lanes are fully automated and able to process passengers within approximately three seconds. Ultimately, the lanes at AUA should be able to speed up the biometric identification and authentication process to the time required for the passenger to pass through the lane at walking speed. This would eliminate the static moment between the barriers (therefore avoiding queues and retaining the seamless flow).

In case the camera is unable to recognize and confirm the passenger's ID, the passenger is requested to step out and follow the regular facilitation process next to the Happy Flow lanes. In case a passenger was flagged with a law enforcement or immigration issue, the immigration office will have been notified through their Happy Flow dashboard. The immigration officers will intercept this passenger at the border control exit check point and take the appropriate action depending on the issue. If the issue is resolved the border police will change the flagged status of the passenger, and the passenger can continue.

For this step the border control checkpoint is also combined with the entry to the security filter. To enter the security filter (or airside access, as the actual security filter is not directly annex, but a short walk away) a valid boarding card is required. Which is confirmed already upon enrollment.

Source: Aruba Airport

Figure J-41: Biometric e-gates in the Happy Flow passenger journey

Boarding Gate with Biometric Lane

At the gate serving the KLM flight to Amsterdam a dedicated Happy Flow biometric lane is provided with similar and recognizable features as the previous checkpoints, and much like the border control checkpoint but without the mantrap feature. The lane is fully automated and equipped with a moveable camera and access barrier at the end. As with the security checkpoint, the recognition and identification processing take place within a few seconds where after the barrier opens and the passenger can board. The processing speed of the biometric lane is deliberately reduced to avoid queues in the boarding bridge.

In addition to these features, the device has an interface with the airline's DCS in order to register actual boarding of the passenger. The automated boarding lane is considerably faster compared to the conventional manual actions, thereby keeping queuing and standstills to a minimum.

Retention and Storage

Because KLM is a European company and EU citizens' data is processed, the EU privacy regulations (GDPR rules) need to be adhered to. This means the entire platform is developed, based on the concept of Privacy by Design. The digital ID that is created during enrollment is encrypted and stored in a local database for temporary use by the airport, airline, and authorities. The data is stored for less than 24 hours and deleted directly after. When the data is shared between stakeholders each stakeholder only receives the fields of data that they are authorized to have, and which are required for the purpose of that specific task only:

- the Aruban Immigration Authority – receives all data that is incorporated in the embedded chip of the e-Passport for the task of the border control process;
- the airline – receives only the data that is required to be registered in the flight manifest via the DCS or to pull up the PNR at baggage check-in;
- the airport – receives only data that is de-personalized as they are not allowed to register any Personally Identifiable Information (GDPR).

The data relevant to the Aruban Immigration Authority and law enforcement agencies (facial biometric details captured and passport data) is encrypted and saved permanently on a dedicated database.

System Architecture Flow Diagram

The flow diagram of this case study can be found in CHAPTER 2: U.S. and Worldwide Lessons From Deployments.

System Specifications

The pilot with KLM Royal Dutch Airlines is based on a "per trip" model. The system as installed at Aruba International Airport is built up of the following components

- Biometric enrollment kiosk
- Biometric baggage drop-off desk
- Biometric border control lane
- Biometric boarding control lane
- Biometric template database
- (Biometric) Data management system orchestration via business rules
- Facial data recognition software
- External database interfaces (like the connection with authorities' databases that have long term storage of person's details)
- Local database for temporary storage (less than 24 hours)

The overall system consists of physical passenger processing devices which are connected through a dedicated and secure IP network with the databases and systems. The operating system and hardware are supplied by Vision-Box. The operating system is at the center of the hardware and software components and manages all data flows. The operating system of Vision-Box also manages the business rules for decision making at the various checkpoints.

The operating system uses cameras at each part of the process (check-in/enrollment, baggage drop-off, border checkpoint, boarding) where identification of the passenger is required. Wayfinding and routing of the Happy Flow throughout the terminal in between these parts is passive and provided by signage and wayfinding.

Biometric Boarding Lane & DCS Interface

The biometric lane at the gate operates as a standard CUTE e-gate and has a data connection with the biometric database. As soon as the passenger's identity is recognized the boarding card details are sent to the airline host DCS. When the passenger and its boarding card are verified and approved, the airline host sends a signal to the gate that it can open and the passenger is registered as boarded.

The lane also contains a standard boarding card reading device and through the link with the DCS which makes it possible that non-enrolled passengers can also be processed.

Stakeholders and Responsibilities

The Aruba Airport Authority N.V. (AAA) is responsible for the biometric facilities at the airport and the availability and reliability of the equipment.

KLM Royal Dutch Airlines is responsible for the use and operation of the enrollment kiosks, the biometric check-in system and the biometric boarding lanes.

The Aruban Immigration Authority is responsible for the use and operation of the biometric immigration lanes.

Case Study Review

Benefits

The Happy Flow pilot was introduced on the daily KLM flight with an Airbus A330 that uses two circle routes depending on the day. The first is a round trip from Amsterdam to Bonaire to Aruba and back. The other is opposite and flies to Aruba first and back to Amsterdam via Bonaire. Consequently, about half of the passengers originate from Aruba, making up 150 passengers on average per day.

On this daily flight, between 100 to 130 passengers enroll and utilize Happy Flow, with an average participation of approximately 80%. Enrollment was open to all age groups but during alter implementation limited to adolescent and adults (16 year +) only due to the fact that in accordance with Aruban law it needs to be verified by the immigration authorities that minors are leaving the country with the permission of both parents.

The ultimate goal to improve the passenger's experience was met and, in the process, the implementation of Happy Flow using biometrics improved passenger satisfaction, reduced queues and inefficiencies, and relieved pressure from authorities' operations where realized.

Responses from Customers

Passenger feedback research conducted by KLM, passengers indicated that they:

- Experienced less stress
- Liked to be in control over their journey (rather than having to join the queue)
- Enjoyed the usability and decreased passenger processing times
- Still felt some concern over privacy, data storage, and data ownership

KLM indicated that although passengers are concerned about their privacy, they perceive KLM as a reliable airline, and also expect they will deal with their data in a reliable way.

Some passengers indicated that instead of privacy concerns they perceive the biometric process as extra secure. Only people who have something to hide would not want to enroll. Passengers from countries with stronger privacy concerns were more reluctant to enroll.

Systems Specifications Review

The system is designed according to the Frontex automated border control standards (EU). No actual information is available regarding the performance of the system (false rejection rates). The processing speed of gates at boarding is approximately 6 Seconds.

Fall Back Options

The passengers that did not enroll in Happy Flow traveled only with hand baggage and were checked-in online or were families with children under 16 years old. The first group would simply pass by the enrollment kiosk as they headed directly to the first touch point in their passenger journey: border control. Therefore, they pass through the terminal as quickly as possible. Families with children under 16 years old simply could not enroll and needed to check in together.

There was also a group of passengers that often travels with considerable baggage. They spend more time at the baggage drop-off and check-in desks and the efficiency savings with Happy Flow are more limited. The conventional passenger processing facilities are still in place, so the passengers that do not enroll in Happy Flow are able to use that process.

Concerns

One of the obstacles experienced during pilot was that the passport image quality stored on the e-Passport chip varies per nationality. Some of which are of inadequate quality to perform a reliable match with the person at the enrollment kiosk. As a result, the identity verification for such passengers cannot be performed at the required level of accuracy. These passengers will have to use the conventional passenger process.

Another challenge is the sensitivity and calibration of the touchpoint equipment at enrollment, baggage drop-off, border control, and boarding. The cameras for facial recognition require consistent lighting (with certain margins) on the passenger's face across the day. This may pose challenges at some gates due to the terminal design in terms of natural light. This is solved with artificial lighting and adjustments of the camera view angle.

Lessons Learned

Many lessons are learned from the Aruba Happy Flow project, but the most important one is the proof that a cross-border public-private data sharing endeavor is possible, even when including border authorities. This would not have been accomplished without the trust that the international stakeholders have placed in each other, and the openness of sharing each other's business interests. This has led to a joint definition of the requirements and operational goals for the pilot and the development of a trust framework between parties. Ultimately this resulted in a system that is designed in accordance with Privacy by Design, EU GDPR and Frontex requirements. This paved the way for cross-border interoperability and developments of international program such as OneID and ICAO DTC (Steenbergen, 2020).

The project proved that it is much more than just an access control device at an airport. Multiple stakeholders can benefit from efficiency gains and offer more and better service to passengers, with the same system. KLM for example, likes to have its passenger check-in process via its own user interface so

it can still make last minute adjustments or ancillary sales (Knoppers, 2020). At the time of the pilot it was not yet possible to incorporate check-in with biometric enrollment in one kiosk. It is expected this can be incorporated in the next generation. This passenger centric thinking also sparked initiatives to include hotels and car rental companies in the program in the next generation of the system. And in the same line of thinking, online health registration of test results for Covid-19 or proof of vaccination may well be incorporated.

Findings and Trends

As a world's first, Happy Flow catalyzed developments for automation and the use of biometrics in airport passenger processes. These developments range from international standards and recommended practices, professional associations and working groups, legislation, politics, technology, and research and innovation. Aruba has not stood still since and moved to the forefront of these developments and is planning to continue to do so in the future.

Future Situation and Broader Implementation

The Happy Flow concept has developed into a 2.0 version that is ready to be rolled out in the near future. This new version aims to process all airlines and be able to interface with any airline booking and departure control system. It is also the intention to add non-air stakeholders like hotels and rental car companies to the Happy Flow platform. The use of a (self-sovereign) trusted digital identity will be key to these future developments that will be in line with international standards, like ICAO DTC and IATA OneID. This would enable home enrollment and would reduce the required enrolment time at the airport.

Aruba International Airport has been one of the first airports to establish U.S. Preclearance facilities. With large volumes of traffic to the United States and CBP now also opting in to biometric passenger processing, AUA also has ambitions to facilitate biometric processing for U.S. bound traffic.

Trends Identified

Process facilitation: The airline and airport are seeking to have single (multiple trip) enrollment that supports international interoperability, such as ICAO DTC or KTDI. This to avoid the need for (time consuming) enrollment facilities at the airport, and to increase overall efficiency.

Commercial services: The airport and airline are also seeking to introduce more stakeholders in the program that can provide services with the use of the passenger's biometric token. The trend is to provide more biometric enabled services during the passenger journey, improve the passenger experience and non-aero revenues.

Fraud and risk management: The protection of a passenger's data is considered a basic requirement. It is expected by the passenger and a passenger trusts the data with the airline in relation to the brand image. This means that secure data protection is very important to help establish the brand value. In addition, passengers feel more secure knowing that a trusted system is in place that verifies the background of all passengers on a flight.

APPENDIX K

Legal, Policy, and Privacy Review

The Supreme Court has recognized the common law root of the right to privacy. [cl] There are four well-established common law privacy torts: (1) unreasonable intrusion upon someone's seclusion; (2) appropriation of a person's name or likeness; (3) unreasonable disclosure of private facts; and (4) publicity that unreasonably places the other in a false light.[cli] The factual scenario most likely implicated is the unreasonable intrusion upon someone's privacy, but even this is unlikely unless facial recognition technology is deployed in circumstances where the intrusion is "especially private" (e.g., a bathroom).[clii]

The Supreme Court has decided that while not expressly set out in the Constitution, privacy protections are implicit or within the "penumbra" of several provisions of the Constitution, to include the prohibition of unreasonable searches and seizures under the Fourth Amendment; and other amendments under the Bill of Rights.[cliii] In addition, while beyond the scope of this report, use of facial recognition combined with public surveillance can implicate First Amendment considerations.[cliv]

With respect to the issue of identification, the Self-Incrimination Clause in particular is implicated, but it does not protect against the compelled collection of physical evidence, such as blood, DNA, or fingerprints, and its introduction at trial.[clv] Rather, the evidence sought must be testimonial, incriminating, and the Supreme Court has held that the disclosure of one's identity "is likely to be so insignificant in the scheme of things as to be incriminating only in unusual circumstances." [clvi] Thus, even without an individual's consent, the collection and disclosure of biometric data, which is neither testimonial nor incriminating, arguably does not violate the Self- Incrimination Clause, but recently lower courts have been split on the issue.[clvii]

Although the Supreme Court has not considered whether the specific use of facial recognition technology might violate provisions of the Constitution, it has rendered decisions on the use of technology.[clviii] For example, in Kyllo v. United States, the Supreme Court held that the use of thermal imaging technology to determine the amount of heat within a person's house (presumed to be associated with marijuana cultivation) was an unreasonable search, given the heightened privacy expectation associated with one's home.[clix] It may be argued, however, that the Court was more concerned with where the search occurred rather than the technology used to conduct the search.[clx]

In subsequent decisions where the facts focused on the use of technology for the collection of location data or cell phone information, the Supreme Court rendered decisions that eroded in part the doctrine that Fourth Amendment protections did not extend to public spaces or information received from third parties. For example, in 2012, the Court decided that the installation of a GPS tracking device, without a warrant, violated the defendant's Fourth Amendment rights, holding that the physical installation of the device constituted an unlawful interference with the suspect's property interests in the vehicle.[clxi] Six years later, the Supreme Court decided that the government's acquisition of information from a third party on the defendant's cell-site location was a search under the Fourth Amendment for which a warrant supported by probable cause was required.[clxii]

Private Parties

As noted in Ch. 3, where a private party acts as an agent of the government, that conduct may implicate Fourth Amendment principles pertaining to searches. Examples where the courts have found that a search by a private party was conducted as an instrument of the government include: where an airline employee, who had been an informant in the past and financially rewarded for his assistance, performed a luggage search[clxiii]; or where an airline employee conducted a search of luggage pursuant to airline and FAA procedures.[clxiv] The fact that the federal government has not compelled a private party to take a particular action does not, by itself, establish that such action is a private one.[72] For example, encouragement or endorsement of a certain action by authorizing it and removing all legal barriers to it "suffice[s] to implicate the [Constitution]."[clxv]

The issue of whether a company that sells facial recognition technology to the government can be considered a state actor (and subject to Fourth Amendment rules to protect privacy) has arisen in a number of cases brought against Clearview AI.[clxvi] In essence, the complaints filed against Clearview AI contend the company was acting as an agent of the federal government for:

- allegedly scraping billions of facial images from the Internet;
- performing facial scans of those images; and
- creating a biometric database that allows users of the database to immediately identify a member of the public merely by uploading a person's image to the database.[clxvii]

DNA Identification as a Case Study

Although courts have not yet had the opportunity to examine the governmental use of *facial recognition technology*[clxviii], recent case law on the collection of DNA and creation of DNA profiles provide a useful framework for understanding how courts will likely address such conduct in the future. Ultimately, the similarities and differences between DNA profiling and the use of facial recognition technology arguably demonstrate the latter's legality.

This caselaw is the product of disputes arising from the DNA Analysis Backlog Elimination Act of 2000 (DNA Act), which created the Combined DNA Index System (CODIS).[clxix] CODIS, which is supervised by the FBI, connects DNA laboratories at the local, state, and national level, collects DNA profiles from arrestees, convicted offenders, and forensic evidence found at crime scenes, and sets uniform standards for DNA matching.[clxx] Although the DNA used for such matching is often referred to as a "genetic fingerprint," it does not have any association with a genetic disease or any other genetic disposition.[clxxi] Thus, while it is functionally equivalent to a fingerprint, the information in the database is only useful for "human identity testing."[clxxii]

However, that is not to say that the Supreme Court has not been divided over the government's asserted purpose for DNA identification. In Maryland v. King, a close 5-4 decision from 2013, the Court held that the use of a cheek swab to obtain an arrestee's DNA sample and DNA identification of the same arrestee as the perpetrator of an unsolved crime from six years earlier was reasonable under the Fourth

Amendment.[clxxiii] Justice Kennedy reasoned that the fact that the DNA identification search as part of a routine booking procedure precluded any need for a warrant.[clxxiv]

Next, Justice Kennedy balanced the government's legitimate interests against the degree to which the search intrudes upon an individual's privacy, finding that the former's interest in verifying the identity of a

person in detention, determining the risks such person presents to facility staff, the existing detainee population, and new detainees, ensuring the accused person's availability for trial, deciding whether the individual can safely be released on bail, and preventing the detention of innocent people outweigh privacy intrusions from DNA identification.[clxxv] Specifically, Justice Kennedy noted that the intrusion of a cheek swab to obtain a DNA sample is a minimal one because its context, police custody, diminishes privacy expectations; it is brief, painless, and does not break the skin; and the sample only reveals an individual's identity, not any genetic traits.[clxxvi] Thus, he concluded that the search in this case, unsupported by any individualized suspicion beyond that which supported the arrest, was reasonable.[clxxvii]

In his dissent, Justice Scalia responded the Court's assertion that "DNA is being taken, not to solve crimes, but to identify those in the State's custody, "taxes the credulity of the credulous."[clxxviii] He maintained that the majority uses "identify" to mean finding out what unsolved crimes the arrestee has committed, since, in this case, what the DNA match identified was a previously-taken sample from an earlier crime.[clxxix] In fact, King's identity was already known when he was charged—before the DNA database returned a match.[clxxx] Consequently, because suspicionless searches have only been permitted when the primary purpose of the search was not to detect evidence of ordinary criminal wrongdoing, DNA identification searches must, Justice Scalia contended, require some level of individualized suspicion.[clxxxi]

It is well-established that suspicionless searches of all persons—such as fingerprinting—for ordinary law-enforcement purposes would violate the Fourth Amendment. [clxxxii]

Extrapolating from both *King* opinions, arguably the use of facial recognition technology to identify air passengers is even more safely within the ambit of Fourth Amendment reasonableness than DNA identification. Unlike DNA identification, identification via facial recognition would be for non-law enforcement investigatory purposes, including verifying that the passenger may lawfully enter or exit the country and ensuring the safety and security of other passengers, the airplane crew, and society at large. Moreover, if suspicionless searches of passengers' persons and properties can already be lawfully conducted at airports as lawful border searches or administrative searches, a search that is more limited in scope, not physically intrusive, and functionally equivalent to the current practice of examining a passenger's passport is consistent with the Fourth Amendment.

Survey of Federal Privacy Laws Relevant to Airport Operators and Stakeholders

Generally, federal privacy laws: (1) govern a federal agency's collection and use of biometric data; and/or, (2) protect consumers' privacy with respect to the collection and use of their biometric data and provide them a cause of action. There are a number of federal privacy laws applicable to the collection and use of biometric data *by federal agencies* as well as specific activities by various industries in distinct business sectors, some of which are relevant to airport operators and stakeholders. Interestingly, a 2015 GAO report observes that there are no federal laws restricting the *capture* of facial images except with respect to matters associated with minors.[clxxxiii]

With respect to legal protections pertaining to *commercial uses* of biometric data, including facial recognition technology, federal laws can be divided into three broad categories: those that address privacy and consumer protection for: "(1) the capture of facial images; (2) the collection, use, and sharing of personal data; and (3) unfair or deceptive acts or practices, such as failure to comply with a company's stated privacy policies."[clxxxiv]

The overarching federal law governing federal agencies' collection, use and disclosure of personal identifying information (PII), such as biometric data, is the Privacy Act of 1974.[clxxxv]

Privacy Act of 1974

The Privacy Act of 1974 governs what information is collected, maintained and used by federal agencies.[clxxxvi] Where a federal agency creates records retrievable by personally identifying information to satisfy requirements required by law,[clxxxvii] legal requirements governing the collection, use, retention, dissemination, disclosure, and maintenance of individuals' personal information are set out in the Privacy Act of 1974. When seeking personal information from an individual, the Act requires agencies to provide a Privacy Act Statement that informs the person about the authority for the collection, the purpose, the routine uses of such information, and the consequences should the individual decline to provide the information.[clxxxviii] In addition to controls imposed on federal agencies, the Act creates rights for persons on whom the records are maintained.[clxxxix]

Generally, an agency must publish public notice in the Federal Register about the collection, maintenance, use, and dissemination of information about individuals maintained in a system of records (referred to as a System of Records Notice or SORN) and must conduct a Privacy Impact Assessment (PIA) analyzing how the data is used and determining whether it meets applicable legal and policy privacy requirements[cxc]. Further, agencies may not disclose records on individuals without their consent unless one of twelve exceptions apply (such as for law enforcement and national security purposes)[cxci]. The Act imposes recordkeeping, retention, and destruction requirements, as well.[cxcii] There are civil and criminal penalties applicable to violations of the Act.[cxciii]

In addition to the application of the Privacy Act, federal agencies' collection of biometric data, particularly facial recognition data, is authorized and/or governed by laws, regulations, and policies pertaining to:

- requirements on airport operators to establish airport security programs;[cxciv]
- requirements for anyone, including airport and air carrier employees, requiring unescorted access to aircraft and secure areas to obtain a SIDA badge;[cxcv]
- the issuance of airman certificates;[cxcvi]
- the collection of biometric data from travelers for border control purposes;[cxcvii]
- the establishment of an improved visa issuance system, Electronic System for Traveler Authorization (ESTA);[cxcviii]
- the creation of trusted traveler programs;[cxcix] and
- travel security, defense, counterterrorism, and law enforcement.[cc]

Even where federal agencies are using biometric and/or facial recognition technology linked to sector specific activities, there are gaps in the coverage of the law for the regulation of substantive and procedural protections for subjects' data.

For example, CBP implemented a biometric exit system required by law, but has not mandated cooperation from carriers or other authorities.[cci] After almost a decade of collecting biometrics (fingerprints) from arriving aliens[ccii], in 2017, CBP launched the Traveler Verification Service (TVS) to capture facial images from passengers departing the U.S..[cciii] Under TVS, information from a passenger's check-in for a flight is used to compile a "gallery" of pre-existing photographs of the passenger, such as from visas or passports and may include photographs from previous encounters with CBP or other DHS components. Prior to boarding, the camera takes a photograph of the passenger and TVS compares it to the photos in the gallery to verify the passenger's identity. In essence, TVS uses an algorithm to "perform both 1:N and 1:1 facial recognition matching." [cciv]Once confirmed, after a matter of seconds, the passenger is free to board and CBP creates an exit record for the passenger. [ccv]

Photographs of U.S. citizens and exempt aliens are deleted by CBP within 12 hours of verification.[ccvi] CBP has indicated that U.S. citizens entering or departing the United States may opt out of having their picture taken and that the verification will be done manually by a CBP officer or airline/airport representative.[ccvii] Further, according to a 2020 GAO report, foreign nationals may also opt out if an air carrier or third party conducts the facial recognition verification.[ccviii] CBP, however, stores photographs of non-immigrant aliens and lawful permanent residents for up to 14 days in a database, and photos of "in-scope" travelers[ccix] are stored for 75 years in another database. CBP stores *biographic* exit records for every traveler, regardless of their citizenship or status. CBP stores *biographic* exit records of U.S. citizens and lawful permanent residents for 15 years and exit records of non-immigrant aliens for 75 years.[ccx] No photos are shared with travel stakeholders, only the results of the biometric match (or no match).[ccxi]

In an effort to assess and address CBP's use of TVS, the DHS Privacy Office sought a review and recommendations from the DHS Data Privacy and Integrity Advisory Committee (DPIAC).[ccxii] The DPIAC made a number of recommendations to: improve transparency with respect to notice (both substantive and procedural); consult with the scientific community to determine length of years of reliability/accuracy of facial images; data minimization; steps to ensure greater data accuracy (including training partner airlines on use of the technology); and accountability and auditing.[ccxiii]

While CBP's TVS has not been free from criticism, as of July, 2020, only two lawsuits had been filed in connection with the use of its facial recognition technology for border entry/exit purposes. Both complaints were filed in connection with requests filed under the Freedom of Information Act for records pertaining to CBP's TVS.[ccxiv]

Similarly, TSA has been developing biometric solutions to perform travel document checks for passengers proceeding through security checkpoints. In 2018, the agency released its TSA Biometrics Roadmap for Aviation Security & the Passenger Experience.[ccxv] The Biometrics Roadmap outlines four goals:

- Partnering with CBP on biometrics for international travelers;
- Operationalizing biometrics for TSA Pre✓® travelers;
- Expanding biometrics to additional domestic travelers; and
- Developing support infrastructure for biometric solutions.[ccxvi]

In collaboration with CBP, TSA is deploying Credential Authentication Technology (CAT) which is to be used to authenticate the ID credential presented by the passenger.[ccxvii]

Lastly, we note that even in the absence of any lawsuit challenging FBI's direct use of facial recognition technology, there are numerous cases reporting challenges to the use, reliability, or introduction into evidence, of the results of the agency's matches during criminal proceedings.[ccxviii]

FTCA and Deceptive and Unfair Practices

A core mission of the Federal Trade Commission (FTC) is consumer protection. The Federal Trade Commission Act of 1914 (FTCA), as amended, authorizes the Federal Trade Commission to, among other things:

- prevent and address unfair or deceptive acts or practices;
- seek monetary damages and other relief for conduct injurious to consumers;
- prescribe rules defining with specificity acts or practices that are unfair or deceptive, including the ability to establish requirements designed to prevent such acts or practices;
- conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and
- make reports and recommendations to Congress and the public.[ccxix]

Within the scope of the FTCA is the authority to combat unfair and deceptive practices regarding the collection and use of biometric data.[ccxx] The FTC's authority, however, is limited. For example, it may not require retailers to *have* privacy policies, only that if they do, they may not engage in unfair or deceptive practices.[ccxxi] Under the FTCA, the FTC can determine that an act is "unfair" if it includes such acts or practices involving foreign commerce that:

1. cause or are likely to cause reasonably foreseeable injury within the United States; or
2. involve material conduct occurring within the United States.[ccxxii]

The FTCA further provides that:

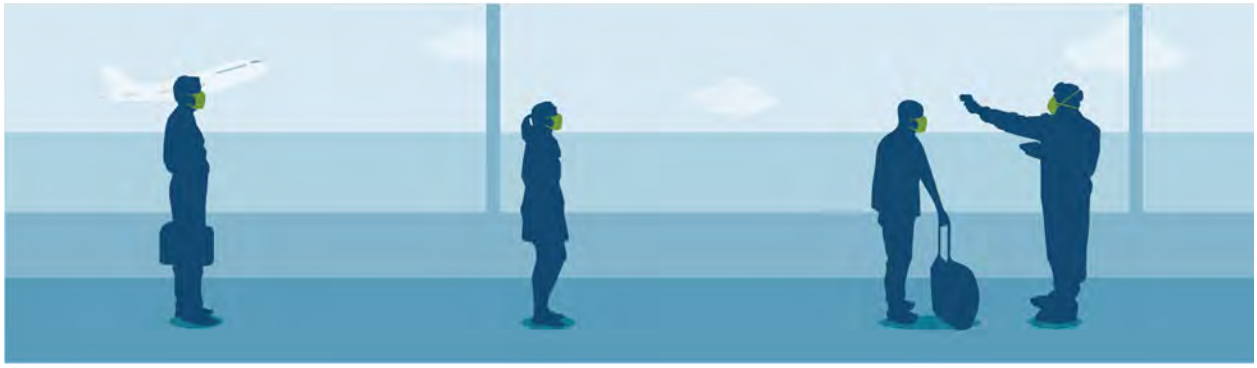
> The Commission shall have no authority …to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[ccxxiii]

As an example of the exercise of its enforcement authority, the FTC recently amended a 2012 settlement order involving Facebook's alleged deceptive practice concerning consumers' control the privacy of their personal information (i.e., sharing of users' personal data with third parties without their knowledge or consent). On April 28, 2020, the FTC formally approved an order to revise the settlement to where Facebook now agrees to pay $5 billion in penalties, make changes in Facebook's approach to privacy management, and be subject to FTC monitoring.[ccxxiv]

Finally, as discussed *infra*, while the FTC has not issued specific regulations governing the use of biometric data technology,[ccxxv] the FTC has undertaken to issue guidance, interpretive statements and other similar public pronouncements to attempt to advise employers on privacy protections and best practices.[ccxxvi],[ccxxvii]

Authorities to Control Travel During a Pandemic

Federal law authorizes the Center for Disease Control and Prevention (CDC) to exercise broad powers to conduct or require cooperative efforts to prevent the introduction, transmission, and spread of quarantinable and serious communicable diseases, such as COVID-19.[ccxxviii] The CDC may require the assistance of Customs and Coast Guard officers as well.[ccxxix]



Source: Inter*VISTAS* Consulting Inc.

Generally, this authority extends to screening, isolating and quarantining, and "plac[ing] a person under surveillance" if the CDC Director "has reason to believe" that the "arriving person" is infected with or has been exposed to" a communicable disease listed under Executive Order 13295.[ccxxx] Subject to certain limitations precluding the denial of *entry* of U.S. citizens and legal permanent residents, the scope of CDC's authority and ability to screen arriving persons at ports of entry and engaged in interstate travel is clear.[ccxxxi]

CDC surveils and/or quarantines persons believed to have been exposed to a disease but not yet ill and isolates persons infected with a communicable disease.[ccxxxii] Of note, TSA may assist CDC by screening passengers in the interest of aviation safety, maintaining a Do Not Board list (identifying persons identified by CDC as public health threats)[ccxxxiii], and canceling flights (if the CDC has determined that a person aboard the aircraft has been exposed or infected with a pandemic disease).[ccxxxiv] Similarly, airlines may refuse to board passengers infected with communicable diseases in accordance with DOT regulations (i.e., when the decision is based on "reasonable judgment that relies on current medical knowledge or on the best available evidence" that the person poses a "direct threat" to the health and safety of others).[ccxxxv]

The law is less clear with respect to *exit* screening for outbound international flights. Although untested in the courts, arguably the authority to prevent the introduction, transmission, and spread of quarantinable and serious communicable diseases would support screening of departing persons, including contact tracing, of infected travelers who have been in contact with other persons in the U.S. or who might be on a return trip to the U.S. shortly or to comply with WHO regulations.[ccxxxvi]

In late May, the CDC issued a checklist for states' health departments to design a contact tracing plan.[ccxxxvii] Also, the CDC website on contact tracing is frequently updated to provide links to resources, tools, and guidance for public health staff and others.[ccxxxviii] Note that health data is heavily regulated under federal and state law with extensive privacy protections.[ccxxxix]

U.S. Congress Legislative Activity

In this most recent session, Congress took up a number of bills proposing to legislate the use of biometric data and there is every expectation that the next Congress will entertain similar legislation. Two bills merit monitoring. The bill that most clearly implicates the use of facial recognition and interests of airport

stakeholders, is the Commercial Facial Recognition Privacy Act (S. 847). The bill would, subject to certain important exceptions, generally prohibit the commercial use of facial recognition technology to identify and track consumers without the end users' consent. As proposed, the bill would place limitations on the third-party sharing of collected facial biometric data, as well as require certain entities to meet minimum data security standards (to be published by FTC in consultation with NIST), treat violations as unfair or deceptive acts or practices under the FTCA. The bill which includes several exemptions would except "security applications" that use the technology for loss prevention or to detect and prevent criminal activity.[ccxl]

U.S. Congress Legislative Activity

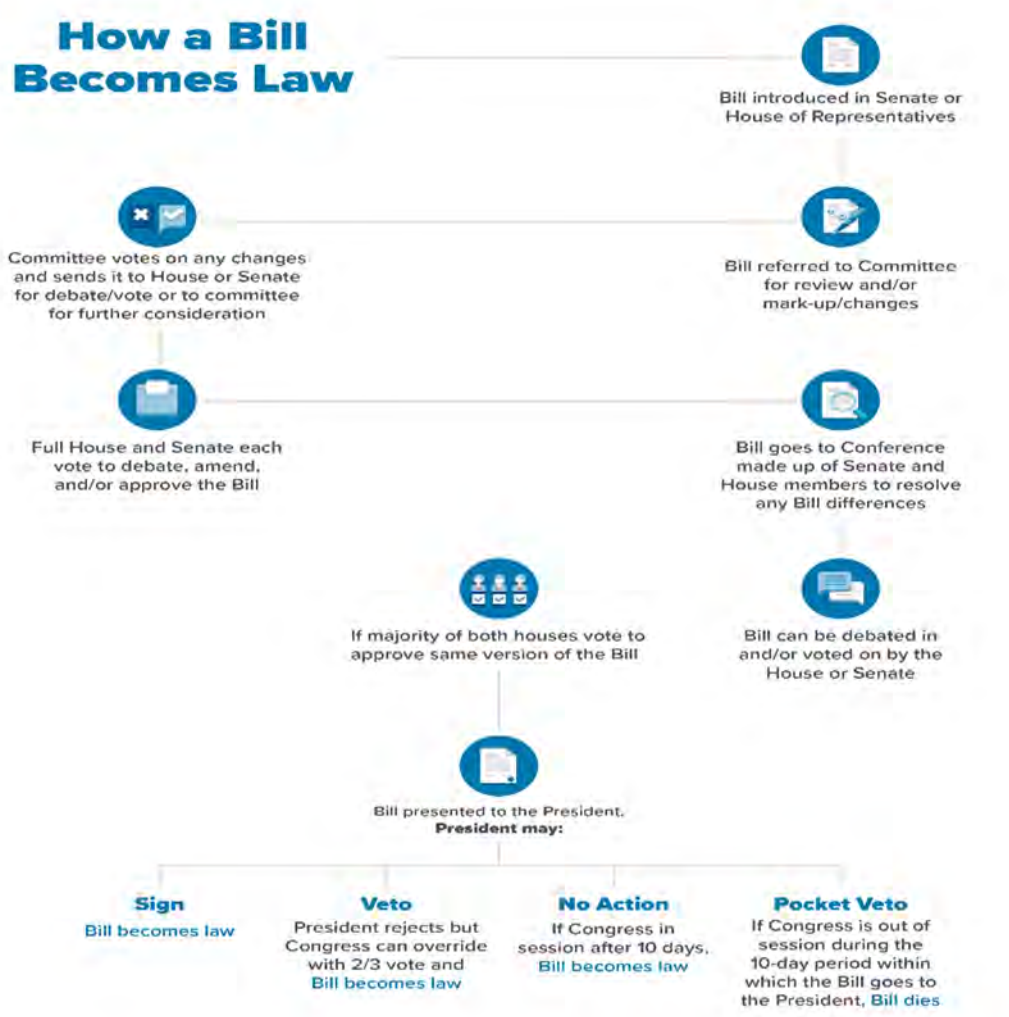


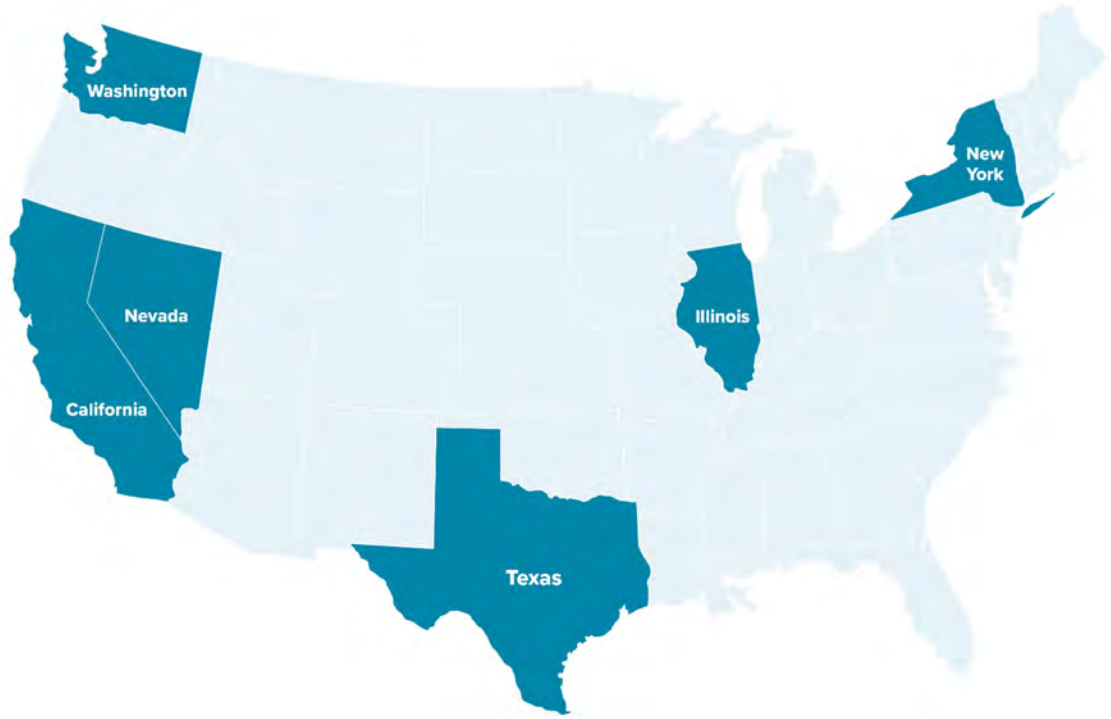
Figure K-1 How a Bill Becomes Law

Another significant development includes Senator Sherrod Brown's announcement on June 18, 2020 that he intends to introduce the Data Accountability and Transparency Act of 2020, a comprehensive privacy and data protection bill. The bill would not only create a privacy agency, but prohibit both private companies and government agencies from collecting personal data unless it is "strictly necessary" to carry out one of a few specified purposes, but more significantly, *ban the use of facial surveillance technology*.[ccxli] The impacts on the use of facial recognition technology could be enormous. This broad sweeping bill would appear to prohibit any data aggregator (which includes federal agencies) from using facial recognition technology; or collecting, using, or sharing any personal data obtained from facial recognition technology.

The topic of facial recognition has also received attention in several Congressional hearings. The House Committee on Oversight and Reform has held three hearings on facial recognition.[ccxlii] Three key concerns were identified: accuracy, transparency and protection of civil liberties.[ccxliii]

Survey of State Laws

Set forth below is a survey and description of state laws that specifically govern the collection and use of biometric data, including facial recognition technology.



Illinois

Over a two year period, 2018-2019, over 200 lawsuits were filed for alleged violations of BIPA and reportedly this is on the rise.[ccxliv] In 2019, the Illinois Supreme Court issued a decision in Rosenbach v. Six Flags Entertainment Corporation that a plaintiff need not allege an actual injury to establish that he qualified as an ”aggrieved” person under specific provisions of BIPA and allowed the suit for penalties and damages to proceed.[ccxlv] In this case, Six Flags theme park took a minor’s thumbprint, without his consent and without informing him about the purpose of data collection, for a season’s pass and future re-entry to the theme park.[ccxlvi] The reason this decision is significant is not only because it recognizes technical violations as sufficient to show harm under BIPA, but also potentially lowers the bar for litigants to bring lawsuits in federal courts which rely on satisfying a “case or controversy” showing to establish standing to bring a lawsuit. [ccxlvii]

In 2016, the plaintiff sued Google claiming in its photo-tagging that the company scanned her facial features from a photograph and created a facial template from the photograph, in violation of BIPA.[ccxlviii] The court held that biometric information obtained from a photograph qualified as a biometric identifier under BIPA, rejecting Google’s argument that only face scans taken in person would qualify as biometric identifiers under the statute.[ccxlix] Subsequently, the case was dismissed on grounds relating to a lack of proof of concrete injuries.[ccl]

Following on the heels of Rosenbach, users of Facebook living in Illinois brought suit in *California* for violations of BIPA associated with Facebook's use of facial recognition technology to "tag" persons in users' pictures.[ccli] The Ninth Circuit Court of Appeals determined that Facebook's collection, use, and storage of biometric identifiers without a written release, violated the procedural protections provided under BIPA, emphasizing that this was the type of harm targeted by the Act, and thus found the plaintiffs had articulated "a concrete and particularized harm, sufficient to confer …standing."[cclii] Even potentially more impactful was the Appellate Court's rejection of Facebook's argument that there should be no extraterritorial application of BIPA for actions Facebook failed to undertake in another state. The Court opined: "it is reasonable to infer that the [Illinois] General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state."[ccliii]

The general rule with respect to application of a state's law outside the state is that absent a clear intent expressed in the provisions of the statute, courts will generally not find extraterritorial application of the law and generally limits the scope of the law to things or persons within the state. [ccliv] Not only are the courts wrestling with the extraterritorial application of BIPA, they are considering lawsuits against third parties that have derived facial "geometries" from photographs, despite BIPA specifically excluding photographs from the definition of a biometric identifier subject to the law's provisions.[cclv]

In addition to litigation over the specific terms in BIPA, two decisions subsequent to Rosenbach are worth mentioning as well as bearing on prerequisites to the ability to bring suit: Miller v. Southwest Airlines[*cclvi*]; and, Crooms v. Southwest Airlines Co.[cclvii] In both cases, airline ramp agents from Midway Airport alleged that Southwest Airlines' practice of scanning and using their fingerprints for timekeeping purposes violated BIPA. The Seventh Circuit in Miller and the District Court in Crooms, pointing to the fact that unions represented the plaintiffs' interests under a collective bargaining agreement, Illinois could not divest the union of its role. Ultimately, the courts decided that federal law[cclviii] required the plaintiffs to bring their claims before an adjustment board (and not in federal court), and thus affirmed dismissal of their claims.[cclix]

As these cases illustrate, there are many unsettled questions, particularly with respect to the interplay of federal and state law, to include the degree of harm a plaintiff needs to show to have standing to pursue a case in federal courts versus technical violations under state law to bring a case under BIPA. As one court recently noted, federal courts and state courts define injury differently for purposes of determining standing to bring a suit in the respective courts.[cclx]

To date most of the cases under BIPA have been class actions targeting employers' use of biometric technology at work. These lawsuits are not only on the rise, but expensive and difficult to defend against. For example, recently in 2020, Facebook offered to settle a class action lawsuit (in California) for alleged violations of BIPA for $650 million (after the trial judge initially rejected the proposed $550 million settlement).[cclxi] In May, plaintiffs filed lawsuits against Facebook in Texas and Arizona, adding to the many other suits pending nationwide and the company is reportedly facing billions in damages.[cclxii]

There is also uncertainty with respect to application of BIPA (and other states' biometric privacy laws) under circumstances where airport stakeholders are partnering with government agencies, such as CBP under the TVS program. Factors bearing on applicability, compliance, and potential liability include whether the state law addresses only commercial uses of biometric data and excludes government agencies from its scope, as do all of the biometric state laws discussed in this section (with the exception of the recent Washington law); whether the airport stakeholder's partnership can be viewed as acting as an agent of the government by collecting facial images and transmitting them to CBP (and not retaining them), but this becomes complicated if the stakeholder collects the data for a dual business purpose as well, such as facilitating the boarding process.

Texas

Texas biometric privacy law, like Illinois, requires persons or entities that collect biometric data to inform individuals before capturing the biometric data and to obtain the individual's consent.[cclxiii] Unlike the Illinois law, the Texas statute does not require a written release. The Texas law, however, like the Illinois law, does prohibit the sale of biometric information, and it similarly sets restrictions on the storage of such information.[cclxiv] Lastly, although modeled after BIPA, it lacks any private cause of action, relying on each state's attorney general to enforce and, as appropriate, impose sanctions.[cclxv]

Washington

Washington state's biometric privacy statute entered into effect in 2017, regulating *commercial* uses of biometric data to require notice, consent, and a limited ability to sell biometric data.[cclxvi] Washington's law also does not include photographs, video or audio recordings or facial geometry as biometric identifiers.[cclxvii] Unlike the Texas law, it does not require that consent to collection of biometric data be in writing. Further, a significant departure from its Illinois and Texas counterparts, the Washington state law carves out an exemption to biometric data collection and storage; businesses *may* collect and store such information without providing notice and obtaining consent so long as the information is collection for "security purposes."[cclxviii] The latter is defined to include collection, storage and use of the information for purposes of preventing shoplifting, fraud and theft. [cclxix] As with Texas, there is no private cause of action and enforcement is delegated to the state attorney general.[cclxx]

In a recent development, on March 12, 2020, the Governor signed into law a new facial biometric law, backed by Microsoft, the purpose of which is to limit the ability of state and local government authorities' use of facial recognition technology.[cclxxi] Reportedly, Microsoft, Amazon, and Comcast met with state legislative members to address their concerns from earlier versions of the bill and Microsoft issued a statement endorsing the bill. [cclxxii] The Act will go into effect in 2021.

California

California's California Consumer Privacy Act (CCPA), which entered into effect on January 1, 2020,[cclxxiii] provides consumer and employee rights and regulates commercial uses of biometric data by including it in the definition of personal information.[cclxxiv] California's law applies on a somewhat more limited scale than the Illinois, Texas and Washington laws. The California law targets any company that both (1) operates in California and (2) either makes at least $25 million in annual revenue, gathers data on more than 50,000 users or makes more than half its money from user data.[cclxxv] The law treats biometric information, including images of one's face, as personal information, and provides rights to consumers to protect their personal information.

The CCPA provides the right to know what the company is collecting and why, including information about the sale of their personal information, the right to opt out of the sale of their personal information to third parties, the right to have their data deleted, with some exceptions, and the right to equal service and pricing even if they exercise their privacy rights.[cclxxvi] The law provides a limited private cause of action against businesses that fail to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." [cclxxvii] The CCPA provides a unique provision that requires consumers to provide notice to the company before initiating any legal action. This period of 30 days is to allow the company time to cure the violation and if this is done, no action may be pursued.[cclxxviii]

In sum, with respect to privacy laws enacted in Texas, Washington, and California, there are variances with respect to:

- the definition of biometric data (e.g., application to the image/data collected, but not to the analysis of the data);[cclxxix] and

- the scope of coverage (commercial purpose but not extending to data collected for security purposes, arguably excluding timekeeping uses).[cclxxx]

New York

New York amended its existing data-breach notification laws with its 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which went into effect in March 2020. The SHIELD Act broadens the definition of private information to include biometric information to protect the private information of state residents by requiring businesses to implement and maintain information security protocols.[cclxxxi] Earlier, New York had passed a limited biometric legislation, §201-a, which applies specifically in the employment context. It prohibits fingerprinting "as a condition of securing employment or of continuing employment."[cclxxxii] The SHIELD Act extends protections to any state resident and extends the obligation to provide notification of a data breach under New York's breach notification law beyond the more previously limited protected class of impacted by persons or businesses that conducted business in New York. The law, as amended, does not expressly provide for a private right of action but authorizes the state's attorney general to pursue a maximum fine for failing to notify those affected from $150,000 to $250,000.[cclxxxiii]

Nevada

Effective last October, Nevada enacted SB 220 which amended existing state law to require operators of websites and online services to post privacy notices on their websites and became the first state to provide consumers with the ability to opt out of the sale of their personal information.[cclxxxiv] Although similar to the California Consumer Privacy Act (CCPA), SB 220 is narrower in scope.[cclxxxv]

Most recently similar legislation introduced in several other states (e.g., Arizona, Florida, and Massachusetts).[cclxxxvi] Also states have enacted laws to protect the privacy of minors and students.[cclxxxvii] It is anticipated that this trend will only continue as privacy concerns increase.

Municipalities

Recently municipal bans on the use of facial recognition technology have sprung up in cities across the country. Those cities with such bans include San Francisco, Oakland, Boston (MA), Somerville (MA), Cambridge City (MA), Northampton (MA), Portland (ME), and Brookline (MA).[cclxxxviii] Other cities are considering similar measures and California, New Hampshire and Oregon have already passed state laws that ban the use of facial recognition technology in police body cameras and New York and New Jersey appeared poised to do the same.[cclxxxix] As a general rule, municipal governments have cited concerns about: potential abuses from the use of facial recognition technology, particularly with respect to surveillance activities; impacts on minorities' freedom of association; and imperfections in, and invasiveness of, the technology, citing bias.[ccxc]

International Organization Activities

There are a number of international organizations working on, coordinating, and collaborating with others to support initiatives to achieve a more seamless travel experience in the air environment. Significantly, most advocate for global standards in an obvious effort to incorporate uniformity in international aviation.[ccxci]

Beginning in the late 1960's, the International Civil Aviation Organization (ICAO) begin work on developing a machine readable travel document (MRTD) and in 1980 produced Doc 9303 setting specifications for passports and other travel documents.[ccxcii] Over the next couple of decades, ICAO adopted

and incorporated facial recognition technology as a core concept for MTRD and leading to the promotion of its use for e-Passports.[ccxciii] ICAO initiated an on-going project operating the ICAO Public Key Directory (PKD) which is a central repository for exchanging the information required to authenticate e-Passports. Overall, the objective is to advocate for, and assist in, creating a globally interoperable system.[ccxciv] Specifically, ICAO is focused on the Digital Travel Credential (DTC) which could serve as an e-Passport (i.e., extracted data) and/or issued in parallel to or in replacement of a physical e-Passport.[ccxcv] Recently ICAO published guidelines pertaining to DTC.[ccxcvi]

In an example of an alternate use of biometrics for an identity purpose, the UN High Commissioner for Refugees (UNHCR) in 2018 issued its Strategy on Digital Identity and Inclusion, a global effort to encourage and support countries' "giving everybody access to a legal and digital identity."[ccxcvii] The UNHCR indicated that refugees and other displaced persons represent a "marginalized" sector of a population in greatest need of an identity to benefit, for example, from the receipt of basic assistance, protection, and relief services. States in turn benefit from the registration of stateless persons, refugees, and displaced persons with a clearer picture on those residing in their territory. "UNHCR assists member states in ensuring that refugees and asylum seekers, stateless persons, and other forcibly displaced are – digitally speaking - not left behind." In furtherance of this effort, UNHCR began rolling out Population Registration and Identity Management EcoSystem (PRIMES), which using biometrics provides a platform for all UNHCR registration and identity management tools. A consolidated global database is in place. Many of the pilots testing PRIMES are being conducted in partnership with governments, academic institutions, international organizations and private sector companies for proof of concepts, establish use cases and processes, and test IT infrastructure.

In the 1990's, the International Air Transport Association (IATA) and the Airports Council International (ACI) launched a joint initiative, "Smart Security," focused on improving the passenger flow process, particularly through security checkpoints. Smart Security sought to address anticipated growth in passenger traffic by focusing on strengthening security, increasing operational efficiencies, and improving the passenger experience with a more seamless approach. [ccxcviii] Over the years the initiative evolved to combine IATA's Checkpoint of the Future and ACI's Better Security parallel programs to seek to achieve a roadmap for streamlining the passenger flow process, a key component of which is the integration of innovative biometric technology. As of 2018, more than 100 airports worldwide had implemented a variation of Smart Security.[ccxcix]

In December 2006, the Simplifying Passenger Travel Interest Group (SPTIG), of which ACI is a founding member, comprised of airlines, airports and others published its recommendations for the Ideal Process Flow (IPF) for the travel of passengers through an airport. It proposed that many of the processes be automated using biometrics, incorporating ICAO standard biometrics for the passenger identification process in the IPF and at all airports.[ccc]

Building on earlier efforts such as Smart Security and digital identity management, in 2018, IATA announced the One ID initiative which proposed the use of biometric technology to establish a "secure, seamless and efficient journey"[ccci] to facilitate the passenger experience through security touchpoints by "sharing a single set of passenger identity information among authorized stakeholders in accordance with data privacy rules." [cccii] The initiative includes the concept of a Digital Travel Credential (DTC), the global policy and technical specifications of which are being shaped and developed by the ICAO. Generally, the concept has been described as a "virtual credential, derived from and linked to an issuing document, securely stored on a mobile device or in the cloud and accessed via biometric authentication, essentially enabling document-free travel".[ccciii] Significantly, the initiative recognizes that a globally coordinated "horizontal" approach is needed to replace a disjointed fragmented response to date.[ccciv] One ID expressly includes within its desired end state, a plan to have One ID coincide with IATA's New Experience in Travel and Technologies (NEXTT) vision, described below.[cccv]

IATA and ACI are pursuing jointly the New Experience Travel Technologies (NEXTT) initiative, the goal of which is to make the most of the latest technological advances to transform airports, improve the

travel experience from check-in to boarding, including the cargo transport experience, and develop a "common vision to enhance the on-ground transport experience, guide industry investments and help governments improve the regulatory framework"[cccvi] Again, in response to concerns about siloed sector developments, IATA and ACI broadened the focus of the initiative to "business and cultural change as well as how airports and airlines can develop their operations to achieve additional efficiencies and ultimately increase the capacity."[cccvii] The initiative highlights the benefits of "off-airport" processes, use of city centers, and interconnected systems, and includes incorporation of biometric technology without necessarily advocating any single option or solution. Per IATA, "[t]he concept involves the use of a trusted digital identity, biometric recognition technology and a collaborative identity management platform."[cccviii]

Similarly, the World Economic Forum (WEF) has promoted the Known Traveller Digital Identity (KTDI) and in March, 2020, published a white paper offering guidance and recommendations on specifications and a facial recognition framework for industry.[cccix] To promote "responsible use" of facial recognition resources, WEF developed among a diverse group of stakeholders a set of principles (and best practices) designed to inform decision-makers and product teams on issues pertaining to bias mitigation, proportional use of the technology, privacy, accountability, consent, right to accessibility, children's rights and alternative options, to name a few.[cccx] Specifically, The Netherlands and Canada are conducting an on-going pilot to test KDTI aspects in a "real-life, cross-border context"[cccxi] and to further inform future pilots and implementation.

The white paper is intended to document the standards, open specifications, capabilities, functionalities, and industry best practices captured by the initial pilot and "provide guiding principles for the KTDI concept and any related future pilots towards the end-state vision of global interoperability."[cccxii]

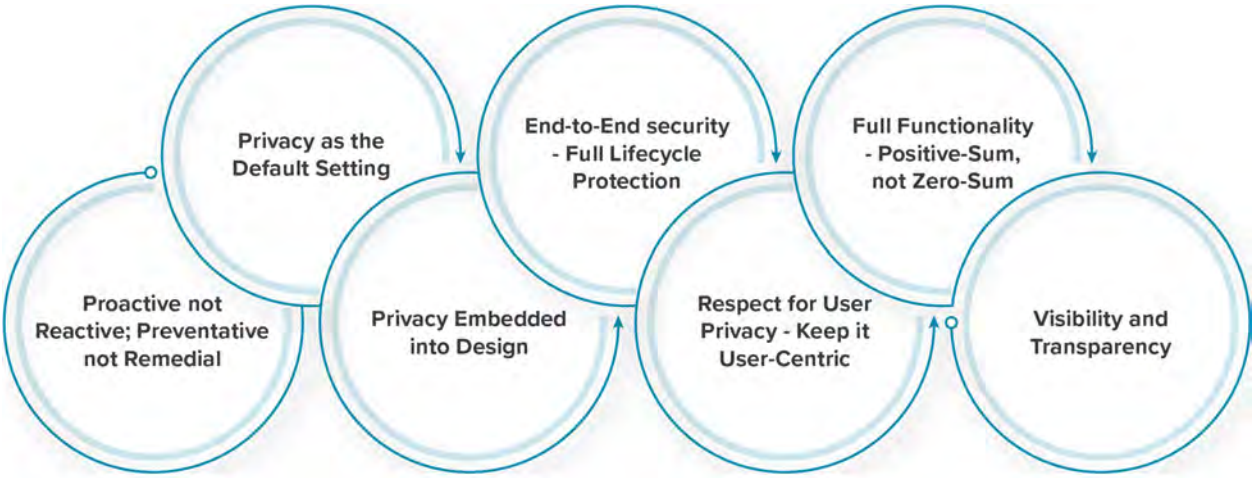
The synopsis above illustrates how various initiatives have evolved. More importantly, the organizations pursuing initiatives to design biometric identity and authentication and air transport process improvements have clearly made substantial efforts to produce not only coordinated but pilots and strategies (e.g., NEXTT) integrated and incorporating efforts of multiple stakeholders and we expect that trend will continue.

APPENDIX L

Best Practices and Privacy by Design

Included herein are additional examples of best practices, checklists, and guiding privacy principles. The FIPPs core principles include:

1. The Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. The Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. The Purpose Specification Principle. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. The Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except a) with the consent of the data subject, or b) by the authority of law.
5. The Security Safeguards Principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. The Openness Principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. The Individual Participation Principle. An individual should have the right:
   a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b. to have data relating to him communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to him;
   c. to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and
   d. to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended;
8. The Accountability Principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.cccxiii



Source: Inter*VISTAS* Consulting Inc.

Figure** Error! No text of specified style in document.**-2: Privacy by Design Principles

The 2012 FTC Report elaborated on those recommended practices as follows:

- Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.
- Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.
- Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law.
- For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.
- Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.
- Companies should provide reasonable access to the consumer data they maintain; and the extent of access should be proportionate to the sensitivity of the data and the nature of its use.
- All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.[cccxiv]
- The bulk of these recommendations mirror provisions in BIPA and other state laws regulating the collection, use, retention, and sharing of biometric data.[cccxv]
- Another useful checklist was compiled in connection with the U.K. 2019 legislation to implement Article 25 of the GDPR.[cccxvi]

Privacy by Design Checklist[cccxvii]

- We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- We make data protection an essential component of the core functionality of our processing systems and services.
- We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.

- We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
- We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- We provide the identity and contact information of those responsible for data protection both within our organization and to individuals.
- We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.
- We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
- We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- We only use data processors that provide sufficient guarantees of their technical and organizational measures for data protection by design.
- When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.
- We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

Several recent EU developments include the 2019 EU Data Protection Guidelines (4/2019) on the GDPR requirements for Data Protection by Design and by Default.[cccxviii] The draft Guidelines (which were open for comment until January 2020) proposed measures and guidance addressing: data protection by design; data protection by default; data subjects' rights; safeguard requirements; practical guidance on the application of the principles; and certification. Thus, the guidelines propose guidance on what data protection obligations meanin practice and how to implement the data protection principles effectively. Similarly, the EU published guidelines on consent describing the elements of valid consent (i.e., under GDPR article 4(11)).[cccxix]

The EU also published Guidelines (2/2020) on GDPR provisions on transfers of personal data between EU and non-EU *public* authorities and bodies.[cccxx]

APPENDIX M

IATA OneID and Seamless Flow

IATA OneID or Seamless Flow

The concept of this use case is that the passenger enrolls with his/her biometric details prior to each journey and is then able to pass several processing steps at the airport by just showing his/her face, e.g., check in, bag drop, security, border control, boarding or even airline lounge entry and duty-free purchases by using biometric verification touchpoints. The processing steps can also include the arrival process at the destination airport or the arrival process upon return at the origin airport. In addition to smooth processing of the passenger, the system can also recognize and differentiate passenger personas and provide services tailored to the persona on its journey (for example for priority or disabled passengers).

The biometric enrollment takes place at kiosks located at the airport that are capable of reading e-Passports. As part of identity proofing, the passenger's identity is verified based on the e-Passport or other biometric identity card and the image of the passenger that is stored on the chip (1:1 matching). After positive identification the system takes a new photo of the passenger and stores this as the biometric credential in the database of the biometric system for a set period. The database will not contain more data than the daily throughput at the airport. This way the 1:1 search time to match the face of the passenger with the stored image will be limited. As opposed to TVS, the database will only be populated with images of passengers that actively enroll and give their consent to use their biometrics.

Before each trip, the passenger enrolls with its biometric details, or when DTC is used, pushes its biometric credentials from its mobile device to the database of the seamless system, where the data is stored in a Passenger Data Envelope (PDE). Besides the passenger's digital identity credentials, the PDE can also contain personal information that can be of use for the process at the airport, such as loyalty program status or disabilities. Other information such as age, sex and nationality may be of special interest for border authorities to use for targeting passengers that have a higher risk profile. In the post Covid-19 era also medical information related to the passenger, such as proof of vaccination may be stored in the PDE and used for a frictionless journey.

After enrollment, based on the information in the PDE, the data management platform verifies whether the passenger is authorized to pass through all steps of the passenger process. This authentication is performed based on business rules that are programmed in the data management platform. As a result, just after enrollment the system knows exactly what to do with the passenger for each touchpoint.

The biometric touchpoints are all connected with and managed by the data management platform through a local area network. The data management platform and biometric database can either run from a server located at the airport or from a server in the cloud. This data management platform also manages the interfaces with third party databases such as airline DCS, border police systems and databases and watchlists and potentially other airport systems such as and point of sales. The business rules for decision making related to the identified person are determined by information retrieved from third party systems. These business rules can potentially be dynamic for border control agencies for targeting specific groups of passengers.

Fifteen years of driving this initiative, IATA hopes its solution can at first be adopted in markets that are struggling with capacity. “OneID is going to be possible in the coming years in 2 or 3 countries, however, a rollout of the project and wider adoption will be limited until a digital ID specification is in place.

Stakeholders in the Biometric System

Because the Seamless Flow system covers multiple steps in the passenger process there are multiple stakeholders. The border authorities are the responsible party for the border control process and as such a core stakeholder, whereas the responsibility for the passenger checks at boarding lies with the airlines. The airport is responsible for access control to the security area, so the airport also has an important stake.

Required IT Infrastructure or Facilities

The Seamless Flow system extends to multiple verification touchpoints at airports. More extensive network infrastructure will be required compared to the earlier biometric systems, depending on the number of touchpoints that are connected and the scale. A seamless system typically contains the following components:

- Biometric enrollment stations.
- Biometric touchpoints that support self-service access.
- Biometric touchpoints for other processes such as bag drop, dynamic wayfinding, point of sale.
- A secure Local Area Network
- Data management platform and face recognition algorithm
- Biometric template database (either in the cloud or in a local database)

The concept of Seamless Flow requires interfaces with other systems as it attempts to ease the passenger journey between multiple stakeholders. The seamless data management platform requires an interface with the airlines DCS at check-in when a combined CUSS/biometric device is used. And again, an interface with the DCS upon boarding. For the border control checkpoint, an interface is required with the systems and search list databases of the border authorities.

Note: When the biometric system needs to interface with Common Use Terminal Equipment (CUTE) / Common Use Passenger Processing System (CUPPS), the equipment will require certification – the vendor of the hardware needs to pay for this certification and will forward the cost to the owner(s). In case the CUTE/CUPPS is owned by multiple airlines in a so-called CUTE Local User Board (CLUB), this will require approval of the CLUB members.

Passenger Groups That can use the System

All passengers that are holding an e-Passport and are traveling by airlines that participate in the seamless travel service that is provided at the airport.

APPENDIX N

ICAO Digital Travel Credential

ICAO DTC Guiding principles

The DTC must be at least as secure as an eMRTD. The information contained in the DTC must be derived from the Travel Document Issuing Authority's data from the eMRTD. Life cycle management of the DTC may not be dependent of the lifecycle management of the eMRTD. Changes must not be needed in current eMRTD standards or issuing process for authorities not intending to issue DTC's. Revocation of a DTC must not result in the automatic withdrawal of the eMRTD associated with the DTC. Revocation of the eMRDT must automatically revoke all underlying DTC's. A DTC must always be issued by a Travel Document Issuing Authority.

Implementation of DTC

There are 3 types of DTC:

- Type 1 - eMRTD bound: consisting of a virtual credential only, with the eMRTD as a physical authenticator.
- Type 2 – eMRTD + physical credential bound: consists of a virtual credential and a physical credential in addition to the eMRTD.
- Type 3 – physical credential bound: consists of a virtual credential and a physical credential but no eMRTD.

Life cycle of a DTC

An overview of the creation, of the three types of DTC, their validity, unique identifier, use by a traveller, invalidation and revocation.

Best Practices in the use of DTC

As DTC and eMRTD are similar except for their form factor, verification of a DTC by a receiving entity requires the same procedures and same levels of scrutiny as for the eMRTD. The potential risks resulting from the use of the DTC are similar or identical to those of the eMRTD. The suggested best practices include: preventing unauthorized access to the virtual component of the DTC during transmission or when stored; use of passive authentication and verifying the issuing authority is a trusted entity (state); and checking that the virtual component is not an unauthorized copy by verifying the physical component.

Risk analysis

Many of the risks associated with DTC are shared with eMRTD's. Some core risks are unique to the DTC. The paper differentiates between risks that are shared with the eMRTD and those that are unique to DTC's and suggests some mitigation strategies.

Other considerations, such as the use of Diplomatic, Official and other passports, involve recognizing the potential impacts or lack of standardization. Visas due to the use of a Logical Data Structure 1 (identity and document information only) the absence of other data, namely visas and travel history could have an affect on traditional risk management activities performed by border and other authorities when deciding whether to board or admit a traveler. Logical Data Structure 2 can support the additional information, but first-generation DTC's will not support this functionality. The storing of multiple DTC's on a single device needs to be carefully considered to ensure that all the potential exploitations of vulnerable groups are addressed.

APPENDIX O

Accuracy of Facial Recognition

With the application of facial recognition systems in aviation it is important that all stakeholders are aware how accurate these systems are. It should be avoided that passengers that are not allowed to pass a border control touchpoint or enter a plane. Contrary, the algorithm should not be too strict so that almost every person that approaches a touchpoint is rejected, nor should the time to render the decision be too long. There needs to be a balance between security and facilitation.

The matching algorithm analyzes the features stored in the biometric template upon enrollment with the features derived from the image made of the live person upon verification to produce a similarity score. If the score reaches a certain threshold the algorithm decides that it is a match. A biometric system will never result in a 100% match. This is because it depends on the quality and amount of useful information that can be extracted from the image. The quality of useful information depends on varying conditions between enrollment and verification but also on the difference in appearance of the person that needs to be identified (e.g., aging, glasses, face mask, etc.).

Accuracy relates to the number of times that the system gives the correct response. For the response, two variables are most important in operation, namely False Acceptance Rate (FAR) and the False Rejection Rate (FRR). The FAR is the relative number of passengers that can pass through to the system who should not be allowed to do so. The FRR is the relative amount of passengers that are rejected by the system whilst they had the right to pass. An increase in the size of the database will lead to a lower accuracy, with higher false acceptances because there will be more similar biometric templates. Raising the threshold too high will lead to a low FAR but may also lead to longer processing times.

Which rates are acceptable are to be determined by the authorities and other stakeholders. The performance of different face recognition algorithms from different vendors is reported on a frequent basis by NIST . This organization has been testing the performance of face match algorithms since 2017, by using a standard measuring method against large image databases. Although the accuracy depends on many other factors of the system as well, the performance of facial recognition algorithm is the basis of a reliable face recognition system.

In the facial match algorithm, the similarity threshold can be adjusted, which will affect the FRR and FAR. After installation of the biometric verification touchpoints at the location, the system needs to be tested and commissioned. When the system is accepted and operational, the system can be load tested, by having live people enrolled and passing through the biometric touchpoints. The fine-tuning may include, for example, adjusting the uniform illumination level of the touchpoint or protecting the camera view from backlight. After some time, the system can be checked for the FRR .

In the passenger facilitation process, it is also possible that the face that is presented for verification does not exist in the database. A passenger that did not enroll in the program will not have a biometric template in the database. The system will give a rejection, but it is not false. After a series of attempts the system should raise an alarm and manual intervention will be needed.

Notes

[1] Wong, Kelly A., *The Face-ID Revolution: The Balance between Pro-Market and Pro-Consumer Biometric Privacy Regulation*, 20 J. High Tech. L. 229 (2020).

[2] Kugler, Matthew B., *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. Irvine L. Rev. 107 (October 2019).

[3] *See, e.g.*, Singer, Natasha & Metz, Cade, *Many Facial Recognition Systems are Biased, Says U.S. Study* Singer, N. and Metz, C., N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html#:~:text=By%20Natasha%20Singer%20and%20Cade%20Metz%20Dec.%2019%2C,departments%20and%20federal%20agencies%20to%20identify%20suspected%20criminals.; Harwell, Drew, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding U*se, Wash. Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[4] *Id*. (reporting on the National Institute of Standards and Technology (NIST) report issued 12/2019); Nat'l Inst. Of Standards & Tech., NISTIR 8280, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (2019).

[5] Greene, Jay, *Microsoft Won't Sell Police its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, Wash. Post (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

[8] Carrero, Angelica, *Biometrics and Federal Databases; Could You Be In It?*, 51 J. Marshall L. Rev. 589 (Spring 2018).

[15] 1 Data Privacy, Protection, and Security Law § 1.02 (2020).

[16] Intille, Amy M., *Video Surveillance and Privacy: Implications for Wearable Computing*, 32 Suffolk U. L. Rev. 729 (1999).

[8] *See Katz v. United States*, 389 U.S. 347, 350-51 (1967).

[9] *Id.*

[10] *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965).

[11] *See Griswold*, 381 U.S. at 484 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)) (describing the Fourth and Fifth Amendments as "protection against all governmental invasions 'of the sanctity of a man's home and the privacies of life.'").

[12] *United States v. Dionisio*, 410 U.S. 1, 14 (1973) (""No person . . . can reasonably expect that his face will be a mystery to the world."); *see also Maryland v. King*, 569 U.S. 435, 476 (2013) (Scalia, J., dissenting) (noting that taking a person's photograph is a not a Fourth Amendment search).

[13] *See, e.g., Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (recognizing a concrete privacy interest in one's biometric face template), *cert. denied*, 140 S. Ct. 937 (2020). Although *Patel* does not squarely address the reasonableness of the use of facial recognition technology under the Fourth Amendment, its Article III standing analysis necessarily involves an examination of the privacy interests of persons subject to facial recognition technology, and such interests logically reflect those same persons' expectations of privacy.

[14] Note that there is no Fourth Amendment right to expunge government records of one's identity. *Johnson v. Quander*, 440 F.3d 489 (D.C. Cir. 2006), *cert. denied*, 549 U.S. 945 (2006). Although indefinite retention of data deeply concerns other countries, U.S. courts have generally not shown the same level of concern. *See, e.g., Gubala*

v. Time Warner Cable, Inc., 846 F.3d 909, 912 (7th Cir. 2017) (holding that the mere retention of data does not in itself cause an injury-in-fact absent a substantial risk of disclosure); *United States v. Hasbajrami*. 945 F.3d 641, 670, 670 n.20 (2d Cir. 2019) (noting that "[s]torage has little significance in its own right," but caveating that "[t]he considerations might be different if the storage involved data responsive to a warrant and retained for the purpose of a domestic criminal prosecution").

[15] *INS v. Delgado*, 466 U.S. 210, 216 (1984).

[16] *Quander*, 440 F.3d at 498 (citing *Arizona v. Hicks*, 480 U.S. 321 (1987)); *see also King*, 569 U.S. at 465 ("[O]nce respondent's DNA was lawfully collected the STR analysis of respondent's DNA . . . did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment.")

[17] *Riley v. California*, 573 U.S. 373, 381 (2014) (quoting *Brigham City v. Stuart*, 547 U. S. 398, 403 (2006).

[18] *Id.* at 382.

[19]*United States v. Moore*, 381 F. Supp. 3d 139 (D. Mass. 2019) (citing *United States v. Bain*, 874 F.3d 1, 11-12 (1st Cir. 2017)) (law enforcement's use of a pole camera to record the homeowners' comings and goings constituted a search)

[20] *Florida v. Jardines*, 569 U.S. 1, 5 (2013).

[21] *Katz v. United States*, 389 U.S. 347, 360 (1967).

[22] Later cases analyzing *Katz* and drawing on Justice Harlan's concurrence in the case have explained that, under this approach, the Fourth Amendment protects legitimate or reasonable expectations of privacy where: (1) "the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy," and (2) "the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (internal quotation marks omitted) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)); Mariko H., *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 Conn. L. Rev. 1591 (2017).

[23] *See* Howick, J. L., The Fourth Amendment and Airports (2016), ACRP 1101, https://www.nap.edu/catalog/23500/the-fourth-amendment-and-airports

[24] *Kowalski v. Scott*, No. Civ.A.02-7197, 2004 WL 1240658, at *1 (E.D. Pa. May 26, 2004), *aff'd*, 126 Fed. App'x 558 (3d Cir. 2005).

[25] *United States v. Knotts*, 460 U.S. 276, 281 (1983); *United States v. Jones*, 565 U.S. 400, 4430 (2012) (noting that monitoring of a person's movements is reasonable where short-term).

[26] *Hudson v. Palmer*, 468 U.S. 517 (1984) (no reasonable expectation of privacy).

[27] *United* States *v. Ramsey*, 431 U.S. 606, 619 (1977).

[28] *Terry v. Ohio*, 392 U.S. 1 (1968).

[29] *Florida v Rodriguez*, 469 U.S. 1 (1984).

[30] *Id.*

[31] *Kyllo v. United States*, 533 U.S. 27, 34 (2001); *United States v. Jones*, 565 U.S. 400, 416, 428 (2012) (GPS monitoring for extended periods of time); *Carpenter v. United States*, 138 S. Ct. 2206, 2215 (2018) (technological advances in tracking cell-site location information); *Riley v. California*, 573 U.S. 373, 386 (2014) (modern cell phone storage of "vast quantities of personal information).

[32] *Carpenter*, 138 S. Ct. at 2218.

[33] *Riley*, 573 U.S. at 393.

[34] *But see United States v. Moore-Bush*, 963 F.3d 29 (1st Cir. 2020) (affirming the *Katz* principle held use of pole camera comports with rule that "a person does not have a reasonable expectation of privacy in the actions he or she exposes to the public view"); Koops, Bert-Jaap, et al, *Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance'*, 9 U.C. Irvine L. Rev. 635 (March 2019) (Suggesting that factors such as duration, intensity, use, active generation of data, etc. are relevant to an assessment of privacy intrusion by police tracking).

[35] *United States v. Ramsey*, 431 U.S. 606 (1977)

[36] *See Almeida-Sanchez v. United States*, 413 U.S. 266, 272-273 (1973); *Ramsey*, 431 U.S. at 606, 610 n.2.

[37] *Cassidy v. Chertoff*, 471 F. 3d 67, 76 (2d Cir 2006) (noting that "society has long accepted a heightened level of security and privacy intrusion with regard to air travel"); *United States v. Herzbrun*, 723 F.2d 773, 775 (11th Cir. 1984); *United States v. Albarado*, 495 F.2d 799, 805 (2d Cir. 1974); *United States v. Skipwith*, 482 F.2d 1272, 1275 (5th Cir. 1973*); United States v. Davis*, 482 F.2d 893, 910 (9th Cir. 1973); *United States v. Hartwell*, 296 F. Supp. 2d 596, 602-05 (E.D. Pa. 2003); *People v. Hyde*, 524 P.2d 830 (Cal. 1974).

[38] *United States v. Aukai*, 497 F. 3d 955, 960 (9th Cir. 2007) ("The constitutionality of an airport screening search, however, does not depend on consent…Rather, where an airport screening search is otherwise reasonable and conducted pursuant to statutory authority, 49 U.S.C. § 44901, all that is required is the passenger's election to attempt entry into the secured area of an airport."); *United States v. Marquez*, 410 F.3d 612, 617 (9th Cir. 2005) (noting that airport searches are conducted for the parallel purposes of "prevent[ing] passengers from carrying weapons or explosives onto the aircraft" and "deter[ring] passengers from even attempting to do so").

[39] Although there is no Supreme Court holding directly on point, Supreme Court *dicta* and lower courts are all in general agreement. *See, e.g., Chandler v. Miller*, 520 U.S. 305, 323 (1997) ("We reiterate, too, that where the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as 'reasonable'—for example, searches now routine at airports and at entrances to courts and other official buildings."); *see also Corbett v. TSA*, 767 F.3d 1171, 1179 (11th Cir. 2014) (holding that suspicionless scans for explosives and pat-downs are reasonable administrative searches); *Ruskai v. Pistole*, 775 F.3d 61, 77 (1st Cir. 2014) (same, for just pat-downs); *Electronic Privacy Information Center v. DHS*, 653 F.3d 1 (D.C. Cir. 2011) (same, for just scans for explosives).

[40] *Cassidy*, 471 F.3d at 75.

[41] *Harlow v. Fitzgerald*, 457 U.S. 800 (1982).

[42] *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 389 (1971).

[43] *See, e.g., United States v. Jacobsen*, 466 U.S. 109, 115 (1984) (explaining that private searches do not trigger the Fourth Amendment unless the private actor was operating as an agent or instrument of law enforcement at the time of the disputed conduct); *Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 614 (1989)*; *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971).

[44] *See, United States v. Momoh*, 427 F.3d 137 (1st Cir. 2005) (Court noting that even if private party was acting as a government agent, her search of defendant's package would have been permissible under the "border search" exception); *United States v. Rodriquez*, 596 F.2d 169 (6th Cir. 1979) (private search of package and subsequent examination of contents valid under plain view); *see, also Gonzales v. FedEx Ground Package Sys*., No. 12-CV-80125-RYSKAMP/HOPKINS, 2013 WL 12080223, at *1 (S. D. Fla. Aug. 1, 2013) (holding that 19 U.S.C. § 507 protected Fed Ex acting reasonably to assist CBP officers).

[45] *Cassidy v. Chertoff*, 471 F.3d 67, 74 (2d Cir. 2006); *Brees v. HMS Global Mar. Inc.*, 431 F. Supp. 3d 1207 (W. D. Wash. 2020)

[46] The Supreme Court has not directly addressed the application of the a special needs exception to airport administrative searches, but, in dicta, the Court signaled the likely validity of its reasonableness in two cases: *See Chandler v. Miller*, 520 U.S. 305, 323 (1997) (suspicionless searches "may rank as 'reasonable' -- for example, searches now routine at airports"); *City of Indianapolis v. Edmond*, 531 U.S. 32, 47-48 (2000) ("holding also does not affect the validity of border searches or searches at places like airports and government buildings, where the need for such measures to ensure public safety can be particularly acute.").

[47] Brennan-Marquez, K., *The Constitutional Limits of Private Surveillance*, 66 U. Kan. L. Rev. 485 (Feb. 2018).

[48] *See supra* note 81, at 517.

[49] A review of caselaw to determine any suits filed against the FBI, CBP, or TSA regarding the use of facial recognition, the only cases located to date concerned actions filed under the Freedom of Information Act for agency records pertaining to CBP's use of facial recognition technology. *See, e.g., ACLU v. DHS*, Case 1:20-cv-02213 (S.D.N.Y, March 12, 2020); *EPIC v. CBP*, No. 19-cv-689 (D.D.C. March 12, 2019) (settled on April 24, 2020).

[50] U.S. Gov't Accountability Office, GAO-15-621, Facial Recognition Technology (2015), at 28 (referencing the Video Voyeurism Prevention Act of 2004, codified at 18 U.S.C. § 1801)); but also would include the Children's Online Privacy Protection Act in that list (15 U.S.C. §§ 6501-6506).

[51] *Id.*

[52] 5 U.S.C. § 552a (2018).

[53] Constitutional Topic: How a Bill Becomes a Law, https://www.usconstitution.net/consttop_law.html (last visited Aug. 3, 2020).

[54] *See* www.congress.gov (last visited July 24, 2020). *See, e.g.*, Privacy Bill of Rights, S. 1214, 116th Cong. (2019); Consumer Data Privacy and Security Act, S. 3456, 116th Cong. (2020); American Data Dissemination Act, S. 142, 116th Cong. (2019); Data Care Act of 2019, S. 2961, 116th Cong. (2019); Digital Accountability and Transparency to Advance Privacy Act, S. 583, 116th Cong. (2019); H.R. 3900, 116th Cong. (2019); Privacy Score Act of 2020, H.R. 6227, 116th Cong. (2020); Office of Biometric Identity Management Authorization Act of 2019, H.R. 1729, 116th Cong. (2019).

[55] Shubert, Aaron, Not All Those Who Wander Are Lost: The Pathway Towards American Data Privacy Law, 48 Hofstra L. Rev. 835 (Spring, 2020); Cunningham, McKay, ARTICLE: EXPOSED, 2019 Mich. St. L. Rev. 375 (2019).

[56] www.congress.gov. (last visited 03/21/2021).

[57] Mandler, T. Y., Bernstein, M.S. & Roache, J.T., *Biometrics in the Workplace: Best Practices For Compliance*, Law360 Expert Analysis (Dec. 2017).

[58] *Mini-Symposium on Comprehensive Data Privacy Reform Legislation in the United States*: *Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection*, 24 N.C. Banking Inst. 527 (March 2020); General Data Protection Regulation (GDPR), Commission Regulation 2016/679, 2016 O.J. (L 119) 1, Arts. 4 and 9.

[59] *Id.*, at fn. 4.

[60] National Conference of State Legislatures, *Facial Recognition and Biometrics* (Nov. 2015), https://www.ncsl.org/research/civil-and-criminal-justice/facial-recognition-and-biometrics.aspx

[61] *See* National Conference of State Legislatures, *Security Breach Notification Laws*, http://www.ncsl.org/research/telecommunications-andinformation-technology/security-breach-notification-laws.aspx (last visited May 27, 2020); Noah Ramirez, *The Great Big List of Data Privacy Laws by State*, Osano (Dec. 18, 2019), available at https://www.osano.com/articles/data-privacy-laws-by-state; *see also* Oregon's Consumer Information Protection Act (OCIPA, ORS 646A-600, *et seq*.) effective 01/01/2020.

[62] National Conference of State Legislatures, *Data Disposal Laws* (Jan. 4, 2019) https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

[63] *Id.*

[64] For list of state laws, see Ramirez, *supra* note 164.

[65] Biometric Data and Data Protection Regulations (GDPR and CCPA)(June 27, 2020) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data

[66] *See, e.g*., Ark. Code Ann. §4-110-103(7) (effective July 2019, Arkansas revised its breach notification law to include biometric data within its definition of personal information); Louisiana Revised Statutes 51:3071, *et seq*. (2018) (amending its definition of personal information under its breach law to extend protections to biometric data and include a private cause of action); N.C. Gen. Stat. §14-113.20(B); Iowa Code Ann. § 715C.1(11)(a)(5) (West 2014) (defining personal information to include "unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data"); Neb. Rev. Stat. Ann. § 87-802(5)(a)(v) (West 2016) (defining personal information as including "unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation"); Wis. Stat. Ann. § 943.201(1)(b)(13) (West 2017) (defining biometric data as "including fingerprint, voice print, retina or iris image, or any other unique physical representation").

[67] *See* National Conference of State Legislatures, *2019 Consumer Data Privacy Protection*, https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx (last visited May 27, 2020). List of state bills introduced including where proposed amendments to definition of personal information failed to pass, e.g., Florida FL HB 1153.

[68] *Supra* note 164.

[69] 740 Ill. Comp. Stat. 14/15 (2013) (BIPA).

[70] The Varying Laws Governing Facial Recognition Technology, https://www.ipwatchdog.com/2020/01/28/varying-laws-governing-facial-recognition-technology/id=118240/.

[71] 740 Ill. Comp. Stat. 14/15 (2013) (BIPA).

[72] *Id.*

[73] The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020, The National Law Review, Wednesday, January 15, 2020.

[74] *See*, *Bryant v. Compass Grp. USA, Inc*., 958 F. 3d 617 (7th Cir. May 5, 2020) for a discussion of standing requirements and decisions (Standing found in case where plaintiff alleged violation of BIPA for the failure to comply with statutory requirements associated with an account to biometrically access a vending machine).

[75] Facebook Closes in on $650 Million Settlement of a Lawsuit Claiming it Illegally Gathered Biometric Data, https://www.businessinsider.com/facebook-wins-preliminary-approval-to-settle-facial-recognition-lawsuit-2020-8 (August, 20, 2020).

[76] Facebook Federal Litigation Filings, https://companyprofiles.justia.com/company/facebook/dockets/case (last visited Aug. 4, 2020).

[77] H.R. 2478, 50th Leg., Second Reg. Sess. (Ariz. 2012); H.R. 1153, 2019 Sess. (Fla. 2019); S. 120, 191st General Court (Mass. 2019).

[78] *See, e.g.*, *2019 Consumer Data Privacy Legislation*, National Conference of State Legislatures (Jan. 3, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

[79] Hudgins, Victoria, *Why 4 Local Governments Banned Facial Recognition Tech*, Law.com (Nov. 25, 2019 11:45 AM), https://www.law.com/legaltechnews/2019/11/25/why-4-local-governments-banned-facial-recognition-tech/?.

[80] *Gibbons v. Ogden*, 22 U.S. 1, 211 (1824)

[81] Vogel, Nate, *Game of Drones: The Uses and Potential Abuses of Unmanned Aerial Vehicles in the U.S. and Abroad*: *Drones at Home: The Debate Over Unmanned Aircraft in State Legislatures*, 8 Alb. Gov't L. Rev. 204 (2015)

[82] *See English v. Gen. Elec. Co.*, 496 U.S. 72, 78-79 (1990*).*

[83] *Id*. at 79.

[84] *Id.* (citing *Fla. Lime & Avocado Growers, Inc. v. Paul*, 373 U.S. 132, 142-43 (1963)).

[85] For an extensive discussion of the supremacy Clause and the doctrine of preemptions, see *State v. Martinez*, 896 N.W.2d 737 (Iowa 2017)

[86] McCauley, Megan, *Interaction Between State and Federal Law Enforcement: Reversing the ICE Age: Immigration Reform in California*, 49 The U. Of Pac. L. Rev. 481 (Jan 01, 2018).

[87] *Palomino v. Facebook*, 2017 U.S. LEXIS 2971 (N. D. Cal. 2017) (quoting from *Atl. Marine Const. Co. v. U.S. Dist. Court for W. Dist. of Texas*, 134 S. Ct. 568, 582, 187 L. Ed. 2d 487 (2013).

[88] *Id.*, at 7-8.

[89] *Id.*, at 7-8. *Palomino v. Facebook*, 2017 U.S. LEXIS 2971 (N. D. Cal. 2017) (quoting from *Atl. Marine Const. Co. v. U.S. Dist. Court for W. Dist. of Texas*, 134 S. Ct. 568, 582, 187 L. Ed. 2d 487 (2013).

[90] *Supra* note 63.

[91] *See, e.g.*, Iraola, Roberto, *Lights, Camera, Action! - Surveillance Cameras, Facial Recognition Systems and the Constitution*, 49 Loy. L. Rev. 773 (2003)

[92] *Commonwealth v. McCarthy*, 142 N.E.3d 1090, 1106 (Mass. 2020) (determining that it could not say precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections).

[93] *Id.*; *see also* Blitz, Marc J., *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 Tex. L. Rev. 1349 (2004) (comprehensive discussion of the evolution of privacy protections in the law).

[94] *Bah v. Apple Inc.*, No. 19-cv-3539 (PKC), 2020 WL 614932, at *1 (S.D.N.Y. Feb. 10, 2020). In a nightmare of a case, Ousmane Bah, a teenager, lost his learner's permit which was subsequently used by person/persons unknown to commit thefts from Apple stores in four states. Bah was arrested for the thefts based on facial recognition misidentification information from Apple "linking" him to the thefts provided to law enforcement by Apple. Bah has sued for false arrest, defamation, and malicious prosecution.

[95] *Id.; see, e.g.*, Hamann, Kristine & Smith, Rachel, *Feature, Facial Recognition Technology Where Will It Take Us?*, 34-SPG Crim. Just. 9 (Spring 2019).

[96] Bickel, Robert D., et al, *Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?*, 33 Stetson L. Rev. 299 (Fall 2003)

[97] Grother, P., Ngan, M., and Hanaoka, K., Face recognition vendor test (frvt) part 1: Verification. Interagency Report DRAFT, National Institute of Standards and Technology, October 2019. https://nist.gov/programs-projects/frvt-11-verification.

[98] *Id.*; Grother, P., Ngan, M., and Hanaoka, K., Face recognition vendor test (frvt) part 2: Identification. Interagency Report 8271, National Institute of Standards and Technology, September 2019. https://doi.org/10.6028/NIST.IR.8271; and, Grother, P., Ngan, M., and Hanaoka, K., Face recognition vendor test (frvt) part 3: Demographic Effects, National Institute of Standards and Technology, Interagency Report 8280, December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[99] *Id.* at 4-5.

[100] *Id.*

[101] NIST.IR 8271, at 2.

[102] https://www.biometricupdate.com/202002/nist-rolls-up-its-sleeves-to-test-facial-recognition-used-for-biometric-entry-and-exit-program

[103] *See, e.g.*, *EEOC v. Consol. Energy, Inc.*, 860 F.3d 131 (4th Cir. 2017), *cert. denied*, 138 S. Ct. 976 (2018).

[104] *Id.* at 143.

[105] *Nat'l Fed'n. of the Blind v. United Airlines, Inc.*, 813 F.3d 718 (9th Cir. 2016) (referencing 14 CFR § 382.57 providing that generally biometrics may not be the only means of user identification or control); *see also EEOC v. Orion Energy Systems*, 208 F. Supp. 3d 989 (E.D. Wis. 2016) (no violation of the ADA since biometric health screening assessment was voluntary).

[106] *See* Countries Applying Biometrics, https://en.wikipedia.org/wiki/Countries_applying_biometrics (last visited Aug. 4, 2020) (list of various countries' biometric laws); Carrero, Angelica, *Biometrics and Federal Databases: Could You Be In It?*, 51 J. Marshall L. Rev. 589, 598 (citing examples involving Canada, Brazil, Australia, and Argentina); World Economic Forum, *Digital Borders: Enabling a Secure, Seamless and Personalized Journey* (Jan. 2017) (detailing various country programs using biometrics), available at http://www3.weforum.org/docs/IP/2017/MO/WEF_ATT_DigitalBorders_WhitePaper.pdf

[107] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1, Art. 3.

[108] Lord, Nate, *What is the Data Protection Directive? The Predecessor to the GDPR*, DataInsider (Sept. 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.

[109] Cunningham, McKay, *Exposed*, 2019 Mich. St. L. Rev. 375 (2019). *See* Commission Regulation 2016/679, 2016 O.J. (L 119) 1, Art. 3.

[110] Cunningham, McKay, *Exposed*, 2019 Mich. St. L. Rev. 375 (2019).

[111] GDPR, art. 3(1)-(3); Recital 25; Determann, *supra* note 148, at 236-237; GDPR, Art. 3.

[112] GDPR, art. 23

[113] Heward-Mills, Dyann, California and the European Union Take the Lead in Data Protection, 43 Hastings Int'l & Comp. L. Rev. 319 (summer, 2020).

[114] GDPR, arts. 2 and 4; *see also* art. 5 (setting out the principles governing the processing of personal data).

[115] GDPR, art. 9(2)-(4).

[116] GDPR, art.4(2) (Processing means collecting, recording, organizing, structuring, storing, adapting, using, sharing, etc.); *Id*., art. 33; *Id.*, art. 15; *Id.*, art. 7; *Id*., art. 20; *Id.*, art. 25; *Id.*, arts. 37-39; *Biometric data and data protection regulations (GDPR and CCPA)*, Thales (June 27, 2020), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data.

[117] *See* GDPR, art. 45(1).

[118] European Commission, Commission Implementing Decision (EU) 2016/1250, 2016 O.J. (L 207) 11. *See also* Determann, *supra* note 156, at 238.

[119] Court of Justice of the European Union Press Release No. 91/20 (July 16, 2020), https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[120] */d.*

[121] *Id.*

[122] Shyy, Sarah, The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business, 20 U.C. Davis Bus. L. J. 137, 151 (Spring, 2020) (Concluding that "the GDPR is both *ineffective* in protecting consumer privacy and *burdensome* on businesses of all sizes", at 157).

[123] Restatement (Third) of the Foreign Relations Law of the United States, §483 (Am. Law. Inst. 1987); See Wallace, Patrick A., The Long Arm of the EU: The Reach of Brussels' Data Protection Regime into the United States, 26 Geo. Mason L. Rev. 1331, 1349-1354 (2019), for an extensive discussion of comity and the principles associated with the enforcement of the GDPR in the United States.

[124] Macaulay, Thomas, *Automated facial recognition breaches GDPR, says EU digital chief*, TheNextWeb (Feb. 17, 2020), https://thenextweb.com/neural/2020/02/17/automated-facial-recognition-breaches-gdpr-says-eu-digital-chief/

[125] Stupp, Catherine, EU Plans Rules for Facial Recognition Technology, Wall Street J. (Feb. 20, 2020), https://www.wsj.com/articles/eu-plans-rules-for-facial-recognition-technology-11582219726.

[126] See Parliament and Council Regulation 2018/1725, 2018 O.J. (L 295) 39, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN.

[127] https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data; For comprehensive list of foreign data privacy laws, see Greenleaf, Graham, *2019 Global Tables of Data Privacy Laws and Bills*, 157 Privacy Laws & Bus. Int'l Report 2 (6th ed. Supp. Jan. 2019), available at https://ssrn.com/abstract=3380794.

[128] *See, e.g.*, ICAO Public Key Directory, https://www.icao.int/Security/FAL/PKD/BVRT/Pages/default.aspx (last visited Aug. 4, 2020).

[129] *See, e.g.*, NIST, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* (Jan. 16, 2020), https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf; U.S. Dep't of Homeland Security, Privacy Policy Guidance Mem. 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (2008), available at https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf; Mandler,

T. Y., *Biometrics in the Workplace: Best Practices for Compliance*, LAW360 (Dec. 14, 2017). Amelung, C., *Biometric Data Collection and What Employers Need to Know About It*, Labor & Employment, 2019 Emerging Issues 8713 (Feb. 15, 2019).

[130] Cate, Fred H., *The Failure of Fair Information Practice Principles*, *in* Consumer Protection in the Age of the Information Economy 343 (Jane K. Winn ed., 2006), available at https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0036-163372.pdf.

[131]Cavoukian, Ann, Information and Privacy Commissioner of Ontario, is credited with developing this approach which was eventually published in 2009. *See* Privacy by Design – The 7 Foundational Principles, iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/ (last visited Aug. 4, 2020).

[132] 32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel 27-29 October, 2010 Resolution on Privacy by Design, https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

[133] *See* Cavoukian, Ann, *Privacy by Design: The 7 Foundational Principles* (Aug. 2009), archived at https://perma.cc/8QJF-7FKX; Wong, Kelly A., *The Face ID Revolution: The Balance Between Pro-market and Pro-Consumer Biometric Privacy Regulation,* 20 J. High Tech. L. 229 (2020).

[134] Cavoukian, Ann, *Privacy by Design, The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*, Ontario, Canada (2008), available at https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf.

[135] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid change: Recommendations for Businesses and Policymakers* (Washington D.C.: March 2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; *see also Facing Facts*, *supra* note 143.

[136] Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), available at http://www.ftc.gov/speeches/rosch/101201privacyreport.pdf.

[137] Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), available at http://www.ftc.gov/speeches/rosch/101201privacyreport.pdf.

[137] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid change: Recommendations for Businesses and Policymakers* (Washington D.C.: March 2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; *see also Facing Facts*, *supra* note 143.

[138] European Data Protection Board, Guidelines 04/2019 on Article 25: Data Protection by Design and by Default (2019), available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf; *see also* European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (2020) (providing guidance on consent under GDPR), available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. For a comprehensive summary of the elements of Data Protection by Design and by Default, see www.twobirds.com/en/news/articles/2019/global/edpb-publishes-guidelines-on-data-protection-by-design-and-by-default .

[139] Guidelines 05/2020, *supra* note 307.

[140] European Data Protection Board, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies (2020), available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v1.pdf.

[150] See Designing for Digital Transparency in the Public Realm, https://sidewalklabs.com/dtpr/

[141] *Id.*

[142] *Id.*

[143] *Id.*

[144] WEF_Responsible_Limits_on_Facial_Recognition_2020.pdf (weforum.org)

[145] *Id.*

[146] Those 10 principles for action are: 1) Proportional use of facial recognition systems; 2) Risk assessment; 3) Bias and discrimination; 4) Privacy by design; 5) Performance; 6) Right to information; 7) Consent; 8) Information display; 9) Right of access to vulnerable groups; and 10) Alternative option and human presence. Id., at 16.

[147] *Id.*, at 26 and 28.

[148] *Id.*

[149] For examples of other checklists, *see, e.g.*, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, The National Law Review (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020; Data protection by design and default, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (last visited Aug. 4, 2020).

[cl] *See U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 & n. 15 (1989) (recognizing the common law's protection of a privacy right).

[cli] *Restatement (Second) of Torts*, § 652A (Am. Law. Inst. 1977).

[clii] *Rivera v. Google, Inc.*, 366 F. Supp. 3d 998 (N.D. Ill. 2018); *Jacobson v. CBS Broad., Inc.*, 19 N.E.3d 1165, 1180 (Ill. App. Ct. 2014).

[cliii] *See Katz v. United States*, 389 U.S. 347, 350-51 (1967).

[cliv] Zick, Timothy, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 Fla. L. Rev. 1 (2007).

[clv] *Schmerber v. California*, 384 U.S. 757, 764 (1966).

[clvi] *Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 191 (2004).

[clvii] *Compare, e.g., United States v. Wright*, 431 F. Supp. 3d 1175 (Nev. D. Ct. 2020) (Forcing the defendant to unlock his phone with his face violated the Fifth Amendment) with *State v. Andrews*, 2020 N.J. LEXIS 898 (Aug. 10, 2020) (Court held compelled disclosure of cell phone passcode did not incriminate the defendant as the passcode was not substantive information or a clue to the crime).

[clviii] *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

[clix] *Id.*, at 40.

[clx] Haas, Eric P., *Back to the Future? The Use of Biometrics, its Impact on Airport Security, and How This Technology Should be Governed*, 84 J. Air L. & Com. 459 (reprinted in 2019).

[clxi] *United States v. Jones*, 565 U.S. 400 (2012).

[clxii] *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *see also Riley v. California*, 573 U.S. 373 (2014) (police officers could not search without a warrant defendants' cell phones under the Fourth Amendment exception for a search incident to an arrest).

[clxiii] *United States v. Walther*, 652 F.2d 788, 793 (9th Cir. 1981).

[clxiv] *People v. Owens*, 184 Cal. Rptr. 509 (Cal. Ct. App. 1982).

[clxv] *Skinner v. Railway Labor Executives' Assoc.*, 489 U.S. 602, at 615 (1989).

[clxvi] *Calderon v. Clearview AI, Inc.*, 20 civ. 1296 (CM), 20 civ. 2222 (CM), 20 civ. 3053 (CM), 20 Civ. 3104 (CM), 20 Civ. 3481 (CM), 20 Civ. 3705 (CM), 2020 WL 2792979, at *1 (S.D.N.Y. May 29, 2020); Class Action Complaint,

Mutnick v. Clearview AI, Inc., No. 1:20-cv-00512, 2020 WL 378474 (N.D. Ill. Jan. 22, 2020).

[clxvii] *Id.*

[clxviii] A review of caselaw to determine any suits filed against the FBI, CBP, or TSA regarding the use of facial recognition, the only cases located to date concerned actions filed under the Freedom of Information Act for agency records pertaining to CBP's use of facial recognition technology. *See, e.g., ACLU v. DHS*, Case 1:20-cv-02213 (S.D.N.Y, March 12, 2020); *EPIC v. CBP*, No. 19-cv-689 (D.D.C. March 12, 2019) (settled on April 24, 2020).

[clxix] 34 U.S.C. §§ 12592-93 (2017); *id.* §§ 40701-44 (2019).

[clxx] *Maryland v. King*, 569 U.S. 435, 444-45 (2013). As Judge O'Scannlain has helpfully explained:

> CODIS can be used in two different ways. First, law enforcement can match one forensic crime scene sample to another forensic crime scene sample, thereby allowing officers to connect unsolved crimes through a common perpetrator. Second, and of perhaps greater significance, CODIS enables officials to match evidence obtained at the scene of a crime to a particular offender's profile. In this latter capacity, CODIS serves as a potent tool for monitoring the criminal activity of known offenders.

United States v. Kincade, 379 F.3d 813, 819-20 (9th Cir. 2004).

[clxxi] *Id.* at 818 n.4.

[clxxii] *King*, 569 U.S. at 445.

[clxxiii] *Id.*

[clxxiv] *King*, 569 U.S. at 448. "Seemingly" because, as Justice Scalia himself notes ("the opinion does not really contain what you would call a rule of decision"), Justice Kennedy at various points relies on the search incident to arrest exception and the special needs exception to justify warrantless DNA identifications.

[clxxv] *Id.* at 465.

[clxxvi] *Id.* at 461-64. Interestingly, Justice Kennedy also noted that "[t]he special needs cases, though in full accord with the result reached here, do not have a direct bearing on the issues presented in this case, because unlike the search of a citizen who has not been suspected of a wrong, a detainee has a reduced expectation of privacy." *Id.* at 463.

[clxxvii] *Id*. at 465-66.

[clxxviii] *Id*. at 466.

[clxxix] *Id*. at 474.

[clxxx] *Id*. at 474-75.

[clxxxi] *Id*. at 468.

[clxxxii] *United States v. Mitchell*, 652 F.3d 387, 411 (3d Cir. 2011) (citing *Hayes v. Florida*, 470 U.S. 811, 813–18 (1985); *Davis v. Mississippi*, 394 U.S. 721, 727 (1969)), cert. denied, 565 U.S. 1275 (2012); see also *Green v. Berge*, 354 F.3d 675, 680 (7th Cir. 2004) (Easterbrook, J., concurring) ("What is 'reasonable' under the fourth amendment for a person on conditional release, or a felon, may be unreasonable for the general population. Just as parolees' homes may be searched without a warrant or probable cause, while both are required to search a free person's home, so it may be that collection of DNA samples from the general population would require person-specific cause—or at least a 'special need' . . . .").

[clxxxiii] U.S. Gov't Accountability Office, GAO-15-621, Facial Recognition Technology (2015), at 28 (referencing the Video Voyeurism Prevention Act of 2004, codified at 18 U.S.C. § 1801)); but also would include the Children's Online Privacy Protection Act in that list (15 U.S.C. §§ 6501-6506).

[clxxxiv] *Id.*

[clxxxv] 5 U.S.C. § 552a (2018).

[clxxxvi] *Id.*

[clxxxvii] Examples of systems and/or programs, specifically related to border enforcement and aviation operations, for which federal agencies collect biometric data include: IDENT, DHS Automated Biometric Identification System (formerly U.S. VISIT); E-Verify; TWIC; CBP Airport Security Program; TVS; Global Entry/Pre√; Passport.

[clxxxviii] 5 U.S.C. § 552a (e)(3).

[clxxxix] Individuals have the right to access records containing information about themselves, to amend incorrect information, and sue the agency for violations of the statute. 5 U.S.C. 552a(d) and (g).

[cxc] E-Government Act of 2002 (Pub. L. 107-347), codified at 44 U.S.C. § 3601 et seq.

[cxci] 5 U.S.C. § 552a (j) and (k).

[cxcii] *Id.* § 552a(e).

[cxciii] *Id.* § 552a(g) and (i).

[cxciv] 49 U.S.C. § 44903 (2018).

[cxcv] 49 CFR 1540.5; *see also* 19 CFR 122.181-188 (CBP Airport Security Program for unescorted access to CBP areas).

[cxcvi] 49 U.S.C. § 44703 (2018).

[cxcvii] 8 U.S.C. §§ 1181, 1185, and 1221 and 19 U.S.C. §1433 (IDENT, US-VISIT, Traveler Verification Service); Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 118 Stat. 3638); Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53; 121 Stat. 266); *see also*, Pope, Carra, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & Pol'y 769 (2018) (comprehensive discussion of DHS agencies' use of biometric data).

[cxcviii] Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53.

[cxcix] 8 U.S.C. § 1365b (2018), 49 U.S.C. §§ 114 note and 44919.

[cc] *See, e.g.*, USCIS Fact Sheet (June 2020), https://www.uscis.gov/sites/default/files/USCIS/Refugee%2C%20Asylum%2C%20and%20Int%27l%20Ops/Refugee_Screening_and_Vetting_Fact_Sheet.pdf

[cci] *See* 8 U.S.C. § 1365b (2018); Biometric Exit Frequently Asked Questions (FAQs), https://www.cbp.gov/travel/biometrics/biometric-exit-faqs (Last modified: Friday, May 15, 2020).

[ccii] DHS Office of Biometric Identification Management (OBIM) was created in March, 2013, replacing the United States Visitor and Immigration Status Indicator Technology (US-VISIT) Program, the purpose of which is to use biometrics to establish and verify the identity of foreign nationals who apply for visas and seek to enter the US. https://www.dhs.gov/obim.

[cciii] Biometric Exit Frequently Asked Questions (FAQs), https://www.cbp.gov/travel/biometrics/biometric-exit-faqs (Last modified: Friday, May 15, 2020); *see also* DHS Data Privacy and Integrity Advisory Committee (DPIAC), Report 2019-01, *Privacy Recommendations in Connection with the Use of Facial Recognition Technology* (Feb. 2019).

[cciv] GAO-20-568 at 14, Facial Recognition Technology (Sept. 2020).

[ccv] S*upra* note 120.

[ccvi] *Id.*

[ccvii] *Id.*: *see also* Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies, Cong. Rept. (Aug. 2019), https://www.tsa.gov/sites/default/files/biometricsreport.pdf

[ccviii] *Supra note* 121, at 37.

[ccix] *See* 8 CFR 235.1(f) (defining "in scope travelers" as "any person who may be required by law to provide biometrics upon entry into the United States pursuant to 8 CFR 235.1(f)(ii), or upon exit from the United States pursuant to 8 CFR 215.8. "In-scope" travelers include any alien other than those specifically exempt as outlined in the CFR. Exempt aliens include: Canadian citizens under Section 101(a)(15)(B) of the Immigration and Nationality

Act who are not otherwise required to present a visa or be issued a form I-94 or Form I-95; aliens younger than 14 or older than 79 on the data of admission; aliens admitted A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (d)(1)(ii); classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or an individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply." at 4 (fn.9).

[ccx] Privacy Impact Assessment for the Traveler Verification Service DHS/CBP/PIA-056 at 21, November 14, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf; Report 2019-XX of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology As approved in Public Session, https://www.dhs.gov/sites/default/files/publications/DPIAC%20DRAFT%20Biometrics%20Recommendation%20Report%20v4_02.06.2018.pdf.

[ccxi] *Supra* note 120.

[ccxii] *Supra* note 127.

[ccxiii] *Id*.

[ccxiv] *See, e.g., ACLU v. DHS*, Case 1:20-cv-02213, (S.D.N.Y. Mar. 12, 2020); *EPIC v. CBP*, No. 19-cv-689 (D.D.C. Mar. 12, 2019) (settled on April 24, 2020).

[ccxv] Transp. Security Admin., *TSA Biometrics Roadmap: For Aviation Security & the Passenger Experience* (Sept. 2018), available at https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf

[ccxvi] *Id.*

[ccxvii] *See* Press Release, Transp. Security Admin., TSA at Boston Logan International Airport gets new credential authentication technology to improve checkpoint screening capabilities (Feb. 26, 2020), available at https://www.tsa.gov/news/press/releases/2020/02/26/tsa-boston-logan-international-airport-gets-new-credential

[ccxviii] *See, e.g., United States v. Martinez*, No. 04 CR 543, 2019 LEXIS 192708 (N.D. Ill. Nov. 6, 2019)

[ccxix] 15 U.S.C. §§ 41-58, as amended

[ccxx] Pub. L. No. 63-203, § 5 (codified at 15 U.S.C. § 45(a)).

[ccxxi] Zimmerman, Hannah, The Data of You: Regulating Private Industry's Collection of Biometric Information, 66 U. Kan. L. R. 637, 661 (2018); W. Gregory Voss and Kimberly A. Houser, Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies, 56 Am. Bus. L.J. 287, 301 (Summer 2019).

[ccxxii] Supra note 135, § 45(a)(4).

[ccxxiii] *Id.* § 45(n).

[ccxxiv] Press Release, Federal Trade Commission, FTC Gives Final Approval to Modify FTC's 2021 Privacy Order with Facebook with Provisions from 2019 Settlement (Apr. 28, 2020), available at https://www.ftc.gov/news-events/press-releases/2020/04/ftc-gives-final-approval-modify-ftcs-2012-privacy-order-facebook. For a summary of Facebook's history with FTC, see Christine S. Wilson, Commissioner, Fed. Trade Comm'n, Remarks at the Global Antitrust Institute: FTC v. Facebook (Dec. 11, 2019), available at https://www.ftc.gov/system/files/documents/public_statements/1557534/commissioner_wilson_remarks_at_global_antitrust_institute_12112019.pdf.

[ccxxv] Stewart, Lauren, Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security, 60 B.C. L. Rev. 349 (Jan. 2019); Wright, Elias, The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 650-651, 673 (Winter 2019).

[ccxxvi] In the FTC's 2012 report, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* (available at http://www.ftc.gov/os/2012/10/121022facialtechrpt.pdf.), it comments that:

> If a company uses facial recognition technologies in a manner that is unfair […], or that constitutes a deceptive act or practice, the Commission can bring an enforcement action under Section 5. In contrast, in other countries and jurisdictions, such as the European Union, in certain circumstances, consumers may need to be notified and give their consent before a company can legally use facial recognition technologies.

Id., at 2 note 6.

[ccxxvii] Wright, *supra* note 142 at 650-651, 673. In 2014, the National Telecommunication and Information Administration (NTIA) convened a multi-stakeholder process to attempt to develop a set of voluntary guidelines regarding the commercial use--specifically use in retail--of facial recognition technology (so-called code of conduct) but during the proceedings consumer privacy advocates objected to the lack of enforcement or requirements and withdrew. The NTIA published a consensus document with input from the remaining stakeholders, but raising the question as to whether voluntary standards would ever be effective. Press Release, Consumer Federation of America, Statement on NTIA Privacy Best Practices Recommendations for Commercial Recognition Use (June 15, 2016), https://consumerfed.org/press_release/statement-ntia-privacy-best-practice-recommendations-commercial-facial-recognition-use/ [https://perma.cc/B9RX-9Q95].

[ccxxviii] 42 U.S.C. §§ 264-65. *See also* 42 U.S.C. § 268(b) (requiring Customs and Coast Guard officers to aid in the enforcement of quarantine rules and regulations).

[ccxxix] *See* 42 U.S.C. § 268 (b) (2018).

[ccxxx] 42 CFR § 71.32(a).

[ccxxxi] *See* CDC, Legal Authorities for Isolation and Quarantine, https://www.cdc.gov/quarantine/aboutlawsregulationsquarantineisolation.html (Feb. 2020).

[ccxxxii] *Id.*

[ccxxxiii] 49 U.S.C. §114(m) and §106(l)(4)

[ccxxxiv] 49 U.S.C. § 44905(b).

[ccxxxv] 14 CFR 382.21 and 382.19 (c)(1).

[ccxxxvi] The World Health Organization of which the U.S. is a member has issued binding regulations, the International Health Regulations (IHR) which require among many things that members detect, monitor and respond effectively to disease outbreaks that could spread internationally. World Health Assembly Res. 58.3, arts. 6-7, 9,13, (May 23, 2005) available at https://www.who.int/ihr/publications/9789241580496/en/.

[ccxxxvii] CDC, Health Department Checklist: Developing a Case Investigation & Contact Tracing Plan for Coronavirus Disease 2019 (COVID-19), (May 29, 2020), https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/health-department-checklist-final.pdf

[ccxxxviii] CDC, Contact Tracing Resources, https://www.cdc.gov/coronavirus/2019-ncov/php/open-america/contact-tracing-resources.html (last reviewed June 21,2020).

[ccxxxix] Health Insurance Portability and Accountability Act ("HIPAA") Pub. L. 104-191 (1996), particularly 42 U.S.C.§ 1320d–6 (penalties for wrongful disclosure); *see also* Determann, Lothar, *Healthy Data Protection*, 26 Mich. Tech, L. Rev. 229 (Spring 2020).

[ccxl] *See* www.congress.gov (last visited July 24, 2020). *See, e.g.*, Privacy Bill of Rights, S. 1214, 116th Cong. (2019); Consumer Data Privacy and Security Act, S. 3456, 116th Cong. (2020); American Data Dissemination Act, S. 142, 116th Cong. (2019); Data Care Act of 2019, S. 2961, 116th Cong. (2019); Digital Accountability and Transparency to Advance Privacy Act, S. 583, 116th Cong. (2019); H.R. 3900, 116th Cong. (2019); Privacy Score Act of 2020, H.R. 6227, 116th Cong. (2020); Office of Biometric Identity Management Authorization Act of 2019, H.R. 1729, 116th Cong. (2019).

[ccxli] https://epic.org/2020/06/senator-brown-unveils-data-acc.html (June 18, 2020).

[ccxlii] Facial Recognition Technology (Part I): Its Impact on our Civil Rights and Liberties (May 22, 2019); Facial Recognition Technology (Part II): Ensuring Transparency in Government Use (June 4, 2019); and, Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy (Jan. 15, 2020). https://www.youtube.com/watch?time_continue=7&v=2dpazLVUo_w&feature=emb_title

[ccxliii] *Id.*

[ccxliv] The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020, The National Law Review, Wednesday, January 15, 2020.

[ccxlv] *Rosenbach v. Six Flags Entm't Corp*., 129 N.E.3d 1197 (Ill. 2019).

[ccxlvi] *Id.* at 6-9.

[ccxlvii] *Patel v. Facebook,* Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020).

[ccxlviii] *Rivera v. Google, Inc*., 238 F. Supp. 3d 1088, 1091 (N.D. Ill. 2017).

[ccxlix] *Id.*, at 1095.

[ccl] Rivera v. Google, Inc., 366 F. Supp. 3d 998,1006 (N.D. Ill. 2018).

[ccli] *Id.*

[cclii] *Id.*, at 1276; *see also*, Jackson, Michelle, Opting Out: Biometric Information Privacy and Standing, 18 Duke L. & Tech. Rev. 293 (Apr. 2020)

[ccliii] *Patel*, 932 F.3d at 25. *But see Rivera v. Google*, 366 F.Supp.3d 998 (N.D. Ill. 2018) (A showing of a concrete injury required to establish standing for a violation of BIPA).

[ccliv] BIPA May Apply to Clearview AI's Creation of Biometric Data, Law360 Expert Analysis (February 18, 2020

[cclv] 740 ILCS 10 ("Biometric identifiers do not include…photographs…"); See, e.g., *Mutnick v. Clearview AI, Inc. et al*, No. 1:20-cv-00512 (N.D. Ill. January 22, 2020); *Vance v. IBM Corp*., No. 1:20-cv-00577 (N.D. Ill. January 24, 2020).

[cclvi] *Miller v. Southwest Airlines Co*., 926 F.3d 898 (7th Cir. 2019)

[cclvii] No. 19-cv-2149, 2020 WL 2404878, at *1 (N.D. Ill., May 12, 2020).

[cclviii] The Railway Labor Act, 45 U.S.C. § 151 et seq.

[cclix] *Supra* notes 189-190; *Crooms*, 2020 WL 2404878.

[cclx] *See*, *Bryant v. Compass Grp. USA, Inc*., 958 F. 3d 617 (7th Cir. May 5, 2020) for a discussion of standing requirements and decisions (Standing found in case where plaintiff alleged violation of BIPA for the failure to comply with statutory requirements associated with an account to biometrically access a vending machine).

[cclxi] Facebook Closes in on $650 Million Settlement of a Lawsuit Claiming it Illegally Gathered Biometric Data, https://www.businessinsider.com/facebook-wins-preliminary-approval-to-settle-facial-recognition-lawsuit-2020-8 (August, 20, 2020).

[cclxii] Facebook Federal Litigation Filings, https://companyprofiles.justia.com/company/facebook/dockets/case (last visited Aug. 4, 2020).

[cclxiii] Tex. Bus. & Com. Code Ann. § 503

[cclxiv] *Id.*

[cclxv] *Id.*

[cclxvi] Wash. Rev. Code § 19.375 (excludes physical or digital photographs, as well as video or audio recordings from the definition of "biometric identifier); Wash. H.B. 1493 (2017).

[cclxvii] Wash. H.B. 1493 (2017).

[cclxviii] *Id.* § 3(4).

[cclxix] *Id.* § 4

[cclxx] *Id.* § 5.

[cclxxi] Wash. S.B. 6280 (2020).

[cclxxii] *See, e.g., Washington State Announces 2 New Consumer Privacy Bills*, CookiePro Blog (Jan. 24, 2020), https://www.cookiepro.com/blog/washington-state-consumer-privacy-bills/; Hofer, Jonathan, *Washington Passes Deficient Facial Recognition Bill*, Catalyst (May 8, 2020), https://catalyst.independent.org/2020/05/08/facial-recognition-washington-passes-deficient-bill-state/

[cclxxiii] Cal. Civ. Code § 1798.100 et seq.

[cclxxiv] *Id.*; For detailed summary, see Zaller, Anthony, *Employee Biometric Data Issues Under California Law*, California Employment Law Report (Feb 7. 2020), https://www.californiaemploymentlawreport.com/2020/02/employee-biometric-data-issues-under-california-law/.

[cclxxv] Cal. Civ. Code § 1798.140(c).

[cclxxvi] Shank, T. Bruce, The Data Privacy Revolution: How the Era of the General Data Protection Regulation Impacts Tennessee Businesses, 21 Transactions 139 (Fall 2019).

[cclxxvii] *Id.* at § 1798.150: (a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

See also Attorney General website at California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa (last visited Aug. 4, 2020).

[cclxxviii] CCPA § 1798.150 (a)-(b).

[cclxxix] Tex. Bus. & Com. Code Ann. § 503; Wash. Rev. Code § 19.375. (excludes physical or digital photographs, as well as video or audio recordings, from the definition of "biometric identifier); Cal. Civ. Code § 1798.100 et seq.

[cclxxx] *Id.;* Wash. Rev. Code § 19.375.

[cclxxxi] S.5575A, 2019-2020 Leg. Sess. (N.Y. 2019), available at https://legislation.nysenate.gov/pdf/bills/2019/S5575A.

[cclxxxii] N.Y. Lab. Law §201-a (McKinney 2019).

[cclxxxiii] *New York SHIELD Act FAQs*, The National Law Review (Mar. 11, 2020), https://www.natlawreview.com/article/new-york-shield-act-faqs.

[cclxxxiv] S.B. 220, 2019 Leg., 80th Sess. (Nev. 2019), available at https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Text.

[cclxxxv] Kohne, Natasha G., et al, , *New Nevada Privacy Law Takes Effect in October - Comparison of Nevada Law to CCPA*, AG Data Dive (Sept. 10, 2019), https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/new-nevada-privacy-law-takes-effect-in-october-comparison-of.html.

[cclxxxvi] H.R. 2478, 50th Leg., Second Reg. Sess. (Ariz. 2012); H.R. 1153, 2019 Sess. (Fla. 2019); S. 120, 191st General Court (Mass. 2019).

[cclxxxvii] *See, e.g., 2019 Consumer Data Privacy Legislation*, National Conference of State Legislatures (Jan. 3, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

[cclxxxviii] Hudgins, Victoria, *Why 4 Local Governments Banned Facial Recognition Tech*, Law.com (Nov. 25, 2019 11:45 AM), https://www.law.com/legaltechnews/2019/11/25/why-4-local-governments-banned-facial-recognition-tech/?.

[140] Read, Max, *Why We Should Ban Facial Technology*, N.Y. Mag., (Feb. 3, 2020), https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html; Johnston, Karen, *A Comparison of Two Smart Cities: Singapore and Atlanta*, 3 J. Comp. Urb. L. & Pol'y 191 (2019); Jarmanning, Ally, *Boston Bans Use of Facial Recognition Technology. It's the Second Largest City to Do So*, WBUR News (June 24, 2020), https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban.

[ccxc] *See, e.g.*, Gandhi, Amisha, *California County Oversight of Use Policies For Surveillance Technology*, 108 Calif. L. Rev. 1011 (Jun. 1, 2020); Ringrose, Katelyn, *Law Enforcement's Pairing of Facial Recognition Technology With Body-Worn Cameras Escalates Privacy Concerns* (Feb. 2019) , https://www.virginialawreview.org/sites/virginialawreview.org/files/04.%20Final%20Ringrose.pdf.

[ccxci] *See, e.g.*, ICAO Public Key Directory, https://www.icao.int/Security/FAL/PKD/BVRT/Pages/default.aspx (last visited Aug. 4, 2020).

[ccxcii] ICAO Doc 9303 is currently in its 7th edition: https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf

[ccxciii] MRTDs History, Implementation and Interoperability (Int'l Civil Aviation Organization: New Tech. Working Group, Working Paper No. 17, 2007), https://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-17/TagMrtd17_WP016.pdf#search=MRTDs%20History%2C%20Implementation%20and%20Interoperability

[ccxciv] Sec. 3.2, Doc. 9303 (2015).

[ccxcv] Cole, Louise, Digital Travel Credentials, https://www.icao.int/Meetings/TRIP-Symposium-2019/PublishingImages/Pages/Presentations/Digital%20Travel%20Credentials.pdf (last visited Aug. 4, 2020).

[ccxcvi] ICAO-TR Digital Travel Credentials (October 2020).

[ccxcvii] UNHCR Strategy on Digital Identity and Inclusion, https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf (last visited Aug. 4, 2020).

[ccxcviii] ACI Smart Security, https://aci.aero/about-aci/priorities/security/smart-security/ (last visited Aug. 4, 2020).

[ccxcix] Smiths Detection, *An Update on the IATA/ACI Smart Security initiative – 60 Seconds with Sébastien Colmant* (May 2, 2018), https://www.smithsdetection.com/insight/aviation/60-seconds-with-sebastien-colmant/.

[ccc] ACI, *SPT: Ideal Process Flow V2.0* (Dec. 2006), available at https://aci.aero/Media/f79bbcd5-eea4-4ff8-9e57-d61468d080c8/V86X2w/About%20ACI/Priorities/IT%20-%20New/Documentation/Simplifying-Passenger-Travel-Interest-Group-(SPTIG)-Ideal-Process-Flow-(IPF).pdf.

[ccci] *One ID and Standardization of Identity Management Solutions* (Int'l Civ. Aviation Org. A40-WP/301, 2019) available at https://www.iata.org/contentassets/e45e5219cc8c4277a0e80562590793da/one-id-standarization-identity-management-solutions.pdf.

[cccii] *Id.*

[ccciii] Secure and Simplify Travel with Digital Travel Credentials, ttps://www.id4africa.com/2019/almanac/ENTRUST-DATACARD.pdf (last visited Aug. 4, 2020).

[ccciv] IATA, *One ID Concept Paper* (2018), available at https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/oneid-concept-paper.pdf

[cccv] IATA, *One ID End State and Key Principles* (2018), available at https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/oneid-endstate-key-principles.pdf

[cccvi] Appleton, Patrick, *NEXTT Generation of Travel*, Airlines. IATA (Oct. 30, 2019), https://www.airlines.iata.org/analysis/nextt-generation-of-travel.

[cccvii] *Id.*

[cccviii] One ID Fact Sheet, https://www.iata.org/en/iata-repository/pressroom/fact-sheets/fact-sheet---one-id/ (last visited Aug. 4, 2020).

[cccix] *See* World Economic Forum, *Known Traveller Digital Identity Specifications Guidance* (Mar. 26, 2020), https://www.weforum.org/whitepapers/known-traveller-digital-identity-specifications-guidance

[cccx] World Economic Forum, *A Framework for Responsible Limits on Facial Recognition Use Case: Flow Management* (Mar. 2, 2020), https://www.weforum.org/whitepapers/a-framework-for-responsible-limits-on-facial-recognition-use-case-flow-management.

[cccxi] *Id*.

[cccxii] *Id.*

[cccxiii] Fair Information Practice Principles, https://iapp.org/resources/article/fair-information-practices/ (last visited Aug. 4, 2020).

[cccxiv] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid change: Recommendations for Businesses and Policymakers* (Washington D.C.: March 2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; *see also Facing Facts*, *supra* note 135.

[cccxv] *Id.*

[cccxvi] Data protection by design and default, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (last visited Aug. 4, 2020).

[cccxvii]For examples of other checklists, *see, e.g.*, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, The National Law Review (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020; Data protection by design and default, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (last visited Aug. 4, 2020).

[cccxviii] European Data Protection Board, Guidelines 04/2019 on Article 25: Data Protection by Design and by Default (2019), available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf; *see also* European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (2020) (providing guidance on consent under GDPR), available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. For a comprehensive summary of the elements of Data Protection by Design and by Default, see www.twobirds.com/en/news/articles/2019/global/edpb-publishes-guidelines-on-data-protection-by-design-and-by-default .

[cccxix] Guidelines 05/2020, *supra* note 168.

[cccxx] European Data Protection Board, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies (2020), available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202002_art46guidelines_internationaltransfers publicbodies_v1.pdf.