International Journal of Information Management Data Insights 1 (2021) 100049

Contents lists available at ScienceDirect

International Journal of Information Management Data Insights

journal homepage: www.elsevier.com/locate/jjimei

The use of biometric technology at airports: The case of customs and border protection (CBP)

Nimra Khan, Marina Efthymiou*

DCU Business School, Dublin City University, Glasnevin, Dublin 9, Ireland

ARTICLE INFO

Keywords:
Biometrics
COVID-19
Technology
Entry exit
Airport security
Border control
Airports

ABSTRACT

Biometrics in an airport environment can provide a contactless way of identity verification. U.S. Department of Homeland Security (DHS) has been trialling and implementing the Biometric Entry Exit Program at U.S. Customs and Border Control (CBP). Using the Traveller Verification System (TVS), the program biometrically confirms the traveller's identity and their entry or exit, with an increased ability to detect fraudulent documents and visa overstays. This paper assesses the Biometric Exit Program to analyse the use of biometrics at airports and identify the challenges faced. An analysis is conducted on the Entry Exit Program at Dublin Airport, including facial recognition boarding gates. Pilot test results from Dublin Airport and other U.S. airports are used to identify challenges. These included a gap in stakeholder support, low biometric matching rate, infrastructure and network connectivity issues, privacy concerns amongst travellers, and heavy reliance on airlines. Recommendations and solutions for advancement are provided.

1. Introduction

Aviation, a critical component of local and national economies around the globe (Szyliowicz, 2004), accounts for 3.5 percent of the world's global GDP (IATA, 2018). Every day 120,000 flights take off with over 10 million passengers (IATA, 2018). In the past 40 years, it has been one of the fastest-growing economic sectors (IATA, 2011). By 2035, IATA (2018) predicts a doubling in demand for air travel, inevitably creating a more considerable risk of threat and need for improved security.

Airports hold importance as ports of travel, with the arrival and departure of the different profiles of people; travellers, greeters, working staff and the public (Efthymiou & Papatheodorou, 2018; Hiney, Efthymiou & Morgenroth, 2021). Holding symbolic importance, airports are perceived to be extensions of national power and prestige. Public accessibility, their high-profile nature and the mass crowding make an airport vulnerable and exposed to threats (Brooks, 2016), requiring constant security improvements. With increasing passenger numbers and, often, insufficient border human resources, "processing passengers through airport terminals and national borders in a reasonable timeframe becomes more difficult" (Bakker, 2015). According to Bakker (2015), some border control systems are virtually at breaking point. Due to such pressures, a higher probability of fraudulent behaviour and illegal crossing of international borders at airport immigration exists. Thus, presenting a need for improved airport border controls.

Passenger identification is a critical area that lacks advancement in the industry. Consider the missing of Malaysian Airlines Flight 370 in March 2014, involving two passengers with stolen passports. With a significant focus on security today, such accidents emphasize the level of security threat currently present. Hilton (2016) mentions that accurate identification is the keystone to threat identification, detection, and prevention. Potential exists for the aviation industry to improve the identification of passengers at airport border control using biometrics. Currently, the use of biometrics can be seen in several sectors (Carpenter, Maasberg, Hicks & Chen, 2016). For instance, the Chinese authorities' use of 'gait technology' is becoming widespread, enabling the identification of individuals through their body shape and way of walking. Similarly, biometrics such as fingerprints have long been used at amusement parks such as Disney World and Universal Studios for re-entry to parks. The integration of biometric use in air travel can provide faster and accurate identity verification of travellers, and it also has the potential for the integration of artificial intelligence (AI) to result in advanced detection and imaging (Verma et al., 2020).

As the aviation industry grows, security threats are of obvious concern. A vast potential exists in developing industrial processes using technological systems. At the same time, many questions are posed regarding the development and implementation of such procedures to ensure both operational efficiency and effectiveness. This era presents a challenging yet exciting period for the aviation industry, which can revolutionise how we travel.

Schultz and Soolaki (2021) argue that the pandemic has brought up the need for contactless passenger journeys through the airport. Biometrics scans can play a role in a post-pandemic scenario. Biometric

* Corresponding author.
E-mail address: marina.efthymiou@dcu.ie (M. Efthymiou).

https://doi.org/10.1016/j.jjimei.2021.100049
Received 19 June 2021; Received in revised form 6 November 2021; Accepted 13 November 2021

scans decrease the risk of disease transmission and provide a quicker throughput of passengers through a given checkpoint due to less time being taken. The importance of biometrics in a pandemic world should not be underestimated. The technology provides a touchless experience and increases the throughput of passengers through a given checkpoint due to less time being taken to process, especially for CBP who witness numerous passengers daily. Through touchless identity verification, the risk of disease transmission and long queues and crowds is minimised, proving beneficial for passengers, airports, and airlines. Some biometric controls have been implemented in the aviation industry, and these are continuously being trialled and improved globally. One such program is the Biometric Entry Exit Program by U.S. Customs and Border Protection. This paper explores the area of biometric technology at airport border control, explicitly focusing on U.S CBPs Biometric Entry-Exit Program, identifies the benefits, and analyses the challenges posed. The paper aims to address the following objectives:

1 To identify the role of biometric technology at airport border control.
2 To assess whether biometrics can provide benefits and accuracy in ID processing
3 To identify and analyse the challenges present with the biometric entry-exit program at U.S airport border controls and preclearance facilities.
4 To investigate concepts related to biometrics such as privacy impact, use of multimodal biometric, use of artificial intelligence and linkages to COVID-19 pandemics.

The paper is organised as follows. Firstly, literature referring to the existing knowledge around biometric systems and identity verification, including aspects on U.S. CBP and their operation, is reviewed. This is followed by the methodology and case of the Biometric Entry Exit Program at U.S Pre-clearance Facilities at Dublin Airport, including a discussion on e-gate boarding trials. Critical analysis and discussion on the challenges encountered across the Entry-Exit Program pilot trials are then combined with literature findings and interview data. The paper ends with the contribution to literature, practical implications, conclusions, including recommendations and opportunities for future biometric advancement.

2. Literature review

Security plays a pivotal role in the travel industry, especially air travel. The use of biometric technology is fast becoming a key instrument in developing security processes at airports (BTT, 2018). Identity establishment forms an integral part of a passenger's journey through the airport, from identification at check-in to verification at security, border control, boarding and arrivals. Automating the authentication process can bring greater security, operational efficiency and convenience through distinguishing benign travellers from imposters or recognised criminals. Existing research identifies the technologies in different areas around the airport, such as at check-in, at customs, at departures, at air traffic control and passenger assistance services (Zaharia & Pietreanu, 2018). However, not many studies specifically address technology developments at U.S. Customs and Border Control (CBP). Although Zaharia and Pietreanu (2018) study touched on border control, it did not consider the impact or use of biometric technology or facial recognition in detail.

Similarly, some studies analyse airport technology's impact on travellers and employees (Bogicevic, Bujisic, Bilgihan, Yang & Cobanoglu, 2017; Kirschenbaum, Mariani, Van Gulijk, Rapaport & Lubasz, 2012). Kirschenbaum (2017) analyses the correlation between airport employees trust in technology and their level of compliance with procedures. The research looks at how trust in technology affects the implementation of security rules and regulations. At the same time, Bogicevic et al. (2017) captures travellers' perceptions on airport technology and discusses travellers trust in technology, their satisfaction and the benefits airport technologies can bring. Negri, Borille and Falcão (2019) investigated the possibility of airport passengers using biometric technology. Halpern, Mwesiumo, Suau-Sanchez, Budd and Bråthen (2021) discuss how organisational readiness, innovation and airport size and ownership can lead to digital change at airports.

Furthermore, some studies analyse the relations and trade-offs between detection of illegal items and the average queuing times at airport security checkpoints (Hainen, Remias, Bullock & Mannering, 2013; Janssen, 2017; Knol, Sharpanskykh & Janssen, 2019). Although these studies shed light on queuing efficiencies, it is mainly in the context of passenger screening rather than border control. Artificial intelligence in biometric identity systems at airports should also be analysed, and there is a significant lack in this area. There is little research on biometrics at airport border controls. This paper aims to fill this gap and increase understanding of the challenges with biometrics through the case study presented.

Research shows that biometrics and other vital technologies positively affect passenger processing functions as processing times are significantly reduced (Haas, 2004; Kalakou, Psaraki-Kalouptsidi & Moura, 2015). Apart from Haas (2004), only a few studies investigate the implication of using biometrics at airport customs and border control. Even then, Haas (2004) does not examine in detail the pros and cons of using biometrics at airport border control or, in fact, CBP. Further airport developments linked to biometrics, such as the use of e-gates, are also not significantly discussed in the literature. Biometric e-gates are a critical development at airports, and their use is expected to grow significantly. Morosan (2016) study focuses on U.S. travellers' intentions to use such e-gates at airports. However, (Morosan, 2016) does not consider travellers' intentions towards using facial recognition technology (FRT) specifically. A gap in literature can be seen in this aspect which this paper will aim to fill.

In literature, research on technological-based security advancements at airports has been mostly restricted to focus on central passenger checkpoint screening. There is a general lack of research on the impact of biometric technologies at airport customs and border control. Although some research has been conducted on travellers' attitudes towards airport technologies, little is known from the literature about the operational efficiency biometrics can bring to airport customs or border control.

2.1. Biometric identifiers

Identification systems are vital in improving efficiency and enabling innovation according to Mir, Kar and Gupta (2020a). Biometrics is emerging and gaining ground in the aviation industry globally. The International Biometrics Identity Association (IBIA) defines it as an "automated method for verifying or identifying the identity of a living individual based on physiological or behavioural characteristics" (IBIA, 2018). The use of biometrics can enable a confirmation or identification of an individual based on "who they are" rather than "what they possess" (e.g. a Passport) or "what they remember" (e.g. answers to security questions) (Jain, Ross & Prabhakar, 2004). Furthermore, AI can also assist with 'who they are' through face detection and analysing images (Verma et al., 2020).

Biometrics is a process through which biometric identifiers, unique to an individual, are captured by a system to confirm identity. Biometric Identifiers, also known as modalities, are categorised as physiological and behavioural. Physiological characteristics include fingerprints, face, hand, odour, irises, palm prints and DNA. Whereas behavioural characteristics are related to how individuals act and include gait analysis, voice recognition, keystroke dynamics, mouse use characteristics, signature analysis and cognitive biometrics. Jain et al. (2004) argue that any human physiological and/or behavioural characteristics can be used in a biometric system if they possess certain factors, Table 1, which include:

- *Universality*: every individual has the characteristic.
- *Distinctiveness*: characteristic is unique to every individual.

Table 1
Comparison of Different Biometric Technologies (Jain et al., 2004) (*H* = High, *M* = Medium, *L* = Low).

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	**H**	**H**	**H**	**L**	**H**	**L**	**L**
Ear	**M**	**M**	**H**	**M**	**M**	**H**	**M**
Face	**H**	**L**	**M**	**H**	**L**	**H**	**H**
Facial thermogram	**H**	**H**	**L**	**H**	**M**	**H**	**L**
Fingerprint	**M**	**H**	**H**	**M**	**H**	**M**	**M**
Gait	**M**	**L**	**L**	**H**	**L**	**H**	**M**
Hand geometry	**M**	**M**	**M**	**H**	**M**	**M**	**M**
Hand vein	**M**	**M**	**M**	**M**	**M**	**M**	**L**
Iris	**H**	**H**	**H**	**M**	**H**	**L**	**L**
keystroke	**l**	**l**	**l**	**m**	**l**	**m**	**m**
odour	**h**	**h**	**h**	**l**	**l**	**m**	**l**
Palmprint	**M**	**H**	**H**	**M**	**H**	**M**	**M**
Retina	**H**	**H**	**M**	**L**	**H**	**L**	**L**
Signature	**L**	**L**	**L**	**H**	**L**	**H**	**H**
Voice	**M**	**L**	**L**	**M**	**L**	**H**	**H**

- *Permanence*: minimal variation in characteristics over time.
- *Collectability*: characteristic can be quantitatively measured.

2.1.1. Facial recognition

For this paper, emphasis will be placed on facial recognition. Although facial recognition technology has existed for some time, the aviation industry has begun integrating it with existing processes only recently, including integration in Artificial Intelligence programs. As facial features are different for everyone, the aim is to quickly identify imposters and illegal immigrants by matching a live facial image with a previously captured image from the database (CAPA, 2017). In comparison with fingerprints and irises, facial recognition has a higher level of collectability, acceptability and circumvention but a lower level of distinctiveness (Jain et al., 2004). The low circumvention of facial recognition is somewhat negligible in the case of airport border control. This is because the traveller will interact with the border control officer to ensure that facial recognition takes place for the traveller.

Similarly, the traveller who avoided facial recognition will be caught at the boarding gate as the non-boarded seat will be double-checked on board the aircraft. One may argue that identifiers with low circumvent should be incorporated such as iris or retina scan to compensate for the high circumvent of facial recognition. However, multi modal biometrics can increase system costs as well as acquisition times and computational times (Kosmerlj, Fladsrud, Hjelmås & Snekkenes, 2005; Labati et al., 2016). Nevertheless, due to the coronavirus pandemic where travellers are required to wear a masque, iris recognition and facial recognition may be more efficient (Kosmerlj et al., 2005).

With increased user-friendliness, it offers a more efficient and effective manner of identity verification due to a high level of acceptability and collectability. However, along with benefits, challenges also exist with what facial recognition offers, from privacy issues to accurate match rates. Further discussion to follow later in the paper.

2.1.2. Robustness and distinctiveness

Although several factors are needed to analyse a biometric identifier, the two major ones are robustness and distinctiveness. Robustness refers to the ability of a particular biometric to be repeatedly presented over time to the biometric system for successful automated measurement (Woodward, Orlans & Higgins, 2003). Changes can occur due to exposure to chemicals, ageing or injury (Woodward, Webb, Newton, Bradley & Rubenson, 2001). A highly robust biometric identifier would not be subject to significant changes over time. In comparison, an identifier with low robustness could change over time. For example, iris recognition would have higher robustness than facial recognition.

Distinctiveness refers to a person's particular biometric ability to be different from others in the user population, and the difference should be measurable (Woodward et al., 2003). An identifier with a high level of distinctiveness would be unique. A low level of distinctiveness would mean the biometric identifier is challenging to distinguish between users of a population. Generally, the purpose of the biometric system will determine the degree of robustness and distinctiveness required (Woodward et al., 2001).

2.2. Biometric systems

A biometric system is an automated process which i) uses an electronic device to capture such biometric identifiers, ii) extracts biometric data from submitted identifier, iii) compares the identifier with previously captured data, iv) matches captured identifier with a template, v) determines if provided identity is authentic (IMS, 2018). In other words, a biometric system acquires biometric data from an individual and compares it to a template to determine a person's identity. The addition of AI in biometric identity systems through face detection can be advantageous but challenging due to multiple challenges with continuous learning, decision-making, and security issues (Mir, Sharma, Kar & Gupta, 2020b).

For a biometric system to work, external documents containing biographical details, such as a passport, must be presented for 'enrolment' to the biometric system. An individual's initial interaction will permit the capturing of a biometric identifier such as a fingerprint or eye scan, which is recorded and linked to the presented external document (Mayhew, 2012). Once these are connected, the subsequent encounter of an individual with the system when biometric data is retaken will be compared to this template on file, taken during the enrolment phase.

Jain et al. (2004) argue an ideal biometric system should consider certain factors.

- *Performance*: consists of achieving acceptable accuracy and speed in capturing biometrics, need for resources, and operational and environmental factors which can affect this.
- *Acceptability*: the extent to which individuals are willing to permit the use of a specific characteristic.
- *Circumvention*: how easily the biometric system can be fooled through fraudulent methods.

Similarly, (Labati et al., 2016) suggest almost identical factors and additional factors such as:

- *Scalability:* ability to operate efficiently when traveller numbers increase.
- *Interoperability*: relation to use of same common standards, biometric device and data/results.
- *Usability*: how easily the system can be used and be learnt how to use it.
- *Privacy*: techniques to avoid theft or misuse of personal biometric data.

The consideration of the above factors can provide greater operational efficiency and security in biometric systems.

2.2.1. Verification vs identification

A biometric system can operate in two modes: Verification or Identification (Jain et al., 2004; Jain, Bolle & Pankanti, 2006; Mayhew, 2012). Verification enables a confirmation or denying of an individual's identity by matching the captured biometric data with the individual's template in the system database (1 to 1 match) (Jain et al., 2004). Jain et al. (2004) suggest that this mode is usually for positive recognition (Am I who I claim I am?), aiming to prevent multiple individuals from using the same identity. Verification systems are faster and more accurate than identification as they only require a comparison of presented biometric to stored biometric, and thus, they generate results faster (Jain et al., 2006).

On the other hand, identification enables identity confirmation by searching all users' templates in a database and then providing a match with the captured biometric data (1 to n match, where n is all templates in the database). These systems seek to identify an unknown individual (Mayhew, 2012). In today's era, identification is becoming crucial, and the problem of identifying a person accurately is becoming increasingly difficult (Jain et al., 2006). As such, biometric systems provide a convenient opportunity for faster processing of passengers at airports.

Jain et al. (2004) mention that an ideal biometric system should meet acceptable levels of recognition accuracy, speed and resource requirements. It should not pose a danger to users and be accepted by the majority of the intended population. Furthermore, it should be robust to fraudulent behaviour and cyberattacks. Moreover, AI also can both identify and verify a person's image as well as speed, accuracy, efficiency and utility (Mir, Kar & Gupta, 2021). However, for this to occur, the AI must need to learn and improve its decision-making ability in face detection (Mir et al., 2020b)

2.3. The need for a better process

According to Fergusson (2015) and Labati et al. (2016), border officers typically have 12 s to decide whether the traveller is allowed to cross the border. Such time limitations emphasise the need for automated processing to facilitate the clearance of passengers while also maintaining high-security levels (Knol et al., 2019). The majority of current airport security processes are based on biographic measures involving matching an individual's passport information. The advanced passenger information received by CBP is checked against lists including no-fly lists, active wants, terrorist screening database and others (DHS, 2017b). Although this is an efficient method of detecting travellers with high risk, it can often be lengthy and not a completely reliable system for security checks.

To further strengthen security measures, incorporating biometrics alongside biographic measures can provide an advanced level of security that is both faster and efficient (Jain et al., 2004). Biometrics involve capturing an identifier of the passenger and matching it against a database to verify identity, including many biographic elements. US DHS is utilising such a process at CBP.

At the same time, biometrics can help against the fight against global pandemics such as COVID-19 by making processes touchless, thereby reducing the risk of disease transmission and increasing passenger flow through checkpoints. The coronavirus pandemic caused economic destruction and social consequences for both developed and developing nations (Warnock-Smith, Graham, O'Connell, & Efthymiou, 2021a,b). IATA (2020) highlights that approx. 4.8 million jobs in the aviation industry have been lost or under threat because of the travel restrictions due to COVID-19. This pandemic has emphasised the need for the health and safety of not only employees but also customers. Therefore, more stringent cleanliness standards have become a key feature of airlines' operations and marketing. As airlines investigate their cleanliness standards, so should airports. Airports contain many touchpoints where passengers are required to show their travel documentation physically. This passing of documents and touching at certain checkpoints increase the risk of spreading disease during a pandemic. Biometrics provide a touchless and seamless flow of passengers through a checkpoint, being suitable in a pandemic world and suitable for CBP, who envisage numerous passengers daily (CBP, 2018).

2.4. CBP

U.S. Customs and Border Protection (U.S. CBP) is one of the world's largest law enforcement organisations, responsible for "safeguarding America's borders thereby protecting the public from dangerous people and materials". A country's borders can be conceptualised as four points of entry; airports, ports, guarded land ports, which are official and unguarded borders and shoreline, unofficial (Riley, 2006). The focus of this paper will be on CBPs border security at airports for air travel. In addition to security screening before entering the U.S., CBP Officers conduct immigration, customs and agricultural inspections on all travellers and their checked baggage. The role of customs has been referred to as a 'gatekeeper', a barrier through which international trade must pass to protect the interests of the Nation (Widdowson, 2007). On a typical day, CBP processes almost 340,000 incoming international air passengers and crew, encounters 592 inadmissible persons at U.S. ports of entry, identifies 1607 individuals with suspected national security concerns and intercepts 12 fraudulent documents (CBP 2018). It conducts operations in almost "50 countries with more than 868 CBP employees working internationally" (CBP 2018).

The Department of Homeland Security (DHS) coordinates its biometric activities through the Office of Biometric Identity Management (OBIM), which collects information on individuals travelling to the U.S. and controls their pre-entry, entry, status, and exit (EPIC, 2019). An individual's biometrics, such as fingerprints, are taken using an inkless capturing system. A digital photograph of the individual is captured upon entry to the U.S. OBIM check this and the travel documents against a database that aids CBP officers in deciding whether the individual is eligible to enter the U.S. or not. Identity verification through fingerprints or facial imaging prevents identity fraud as biometrics cannot be changed, unlike biographical data, i.e. names. OBIM includes integration and use of other systems such as:

- Arrival Departure Information System (ADIS) – stores arrival and departure information on non-US citizens travelling in and out of the US. are used to identify suspected visa overstayers.
- Advance Passenger Information System (APIS) – contains arrival and departure manifest information, typically from the airline to CBP. CBP uses to identify high-risk and inadmissible passengers.
- Interagency Border Inspection System (IBIS) – manages 'lookout' data, keeps track of information on suspects and interfaces with the Interpol and National Crime Information Centre (NCIC) databases.
- Homeland Advanced Recognition System (HART) – stores biometrics of non-US citizens and is DHS's primary biometric database.

There is a clear sense of a new territory (Hart, 2015; Hiller, 2010). At an airport, Hiller (2010) describes the boundary as symbolic. The passenger has arrived into the new territory but has not yet left, referred to as preclearance. Each traveller and their baggage undergo immigration, agriculture, and customs inspection before admission to the U.S. However, preclearance enables these inspection processes to occur on foreign soil before boarding a direct flight to the U.S., without the need for further screening or inspection on arrival (CBP 2016). As part of preclearance, security screening of passengers must be according to Transportation Security Administration (TSA) standards. Clearing passengers before they arrive in the U.S. can help reduce waiting times at U.S. airports, thus, speeding up connections and maximising aircraft utilisation (CBP 2016). Providing an improved passenger experience, passengers do not need to be screened on arrival and can reach their destination or next flight quickly (CBP 2016). Currently, preclearance occurs at 15

locations in six foreign countries globally: Canada, Ireland, the United Arab Emirates, Bermuda, Aruba and the Bahamas. In 2015, 24 percent of all commercial air traffic and 15.5 percent of all commercial air travellers arriving into the U.S. were precleared (CBP 2016). CBP plans to expand the program so that by 2024, 33 percent of all U.S. bound passengers are precleared (CBP 2016).

2.5. The biometric entry exit program

Most countries globally operate an inbound and outbound immigration process with passport and visa checking, allowing them to store information on who is entering and leaving the country, a fundamental responsibility of sovereign nations. Managing data efficiently drives businesses (Kushwaha, Kar & Dwivedi, 2021; Lootens & Efthymiou, 2021). In the U.S., the biometric entry-exit model automates this process, resulting in cost savings, enhanced accuracy and faster processing. Supported by 66 countries, the United Nations Security Council (UNSC) adopted a resolution in 2017, which encouraged member nations to increase aviation security by collecting biometric data from travellers. Before this, in 2007, the Implementing Recommendation of the 9/11 Commission Act mandated biometrics on entry and departure of all travellers.

Many airports across the U.S have now fully implemented CBPs biometric exit programs. In August 2018, Mineta San Jose International Airport was the first airport on the U.S. West Coast to identify every international traveller with facial recognition, improving security and passenger experience (Burt, 2018). It joined Orlando International Airport in Autumn 2018, which experienced an approx. 4-minute reduction in waiting times through the deployment of biometric entry and exit screening (Burt, 2018). The program is now utilised at seventeen international airports in the U.S., including Atlanta, New York City, Boston, San Jose, Chicago, and Houston. Kevin McAleenan, Acting CBP Commissioner, mentioned that by 2021, the program could reach all major U.S. airports (Rockwell, 2017). Involvement with the program is not limited to CBP only but extends to airlines and airports. Delta, JetBlue, American Airlines, British Airways and Lufthansa are all committed to the idea.

Similarly, airport authorities at Los Angeles, Orlando International, San Jose, Miami, and the Metropolitan Washington Airport Authorities are also involved (EPIC & CBP 2017). Literature suggests the involvement of stakeholders is crucial to government initiatives that involve IT-based initiatives (Pouloudi & Whitley, 1997; Ravichandran & Rai, 2000; Zhang, Dawes & Sarkis, 2005). However, agreement on goals and decision making can become complex and time-consuming as many organisations are self-interested entities (Zhang et al., 2005). Brown (2003) mentions that different stakeholders become critical to its survival during various stages of the project. Such initiatives require 'mutual and ongoing adjustment to balance various competing views' (Brown, 2003; Zhang et al., 2005).

Digital identity systems aid with identity proofing, authentication and authorisation (Nyst, Pannifer & Whitley, 2016). Due to COVID-19, digital identity systems have become more significant and have caused government stakeholders to depend on these systems (Weitzberg et al., 2021). Depending on how biometrics are used, stored and permissioned in a digital identity system, it can potentially raise privacy and security risks (Wang & De Filippi, 2020). Mir, Kar, Dwivedi, Gupta and Sharma (2020c) found that uniqueness, security and privacy are the top priority goals in an identity system and are more crucial than system scalability. Nevertheless, despite some privacy concerns, biometric technology can help in catching fraudulent individuals. Furthermore, we see that border guards performing identity checks at border control become "visually and sensorily skilled as they interact with automated technologies, data and travellers" (Grünenberg, Møhl, Olwig & Simonsen, 2020). We will examine CBP's Biometric Entry Exit System and conduct a case study at Dublin Airport to analyse biometric technology at airport border control.

Table 2
Departure Information System Process (DHS, 2018).

Obtain passengers' biographic information before flight boarding:	CBP personnel used the airline flight manifest and its Advance Passenger Information System to obtain biographic details, such as name, date of birth, passport number, and nationality for each traveller. CBP used this information to establish a list of passengers on each flight.
Create a photo gallery:	CBP used the passenger list to create a repository of digital images, referred to as a 'photo gallery'. CBP obtained passengers' images by sending electronic queries to Federal departments, such as at the U.S. Department of State, to access the individual's historical records (e.g., U.S. passport, U.S. visa and DHS encounter records). CBP also leveraged photographs on pre-screened passengers from DHS systems, such as the Automated Biometric Identification System (IDENT) to help create the gallery.
Capture traveller photos during aircraft boarding:	CBP officers instructed passengers to present their boarding passes to the boarding pass scanner as they approached the camera. Once the boarding pass was scanned, the camera captured a digital image of the traveller's face.
Match digital photos to travellers to confirm their identities:	The Departure Information System automatically compared passenger photographs captured during boarding against photo gallery records. When the Departure Information System matched a photo to an image in the gallery, the passenger was instructed to board the plane.

Using the Traveller Verification Service (TVS), CBP's cloud-based service, APIS, manifest data received from airlines and existing travellers photographs are used to confirm identity, create an exit record and biometrically ensure the exit (CBP 2019). The biometric entry-exit model operates through the use of facial recognition technology. The first CBP pilot for facial recognition at the airport began in June 2016 at Hartsfield-Jackson Atlanta International Airport, where passengers' passport photos were biometrically matched to real-time photos (DHS, 2017b). During boarding, passengers scanned their boarding passes. A camera captured their facial image, which the Departure Information System Test (DIST) utilised to automatically compare against a photo gallery with the previously captured photographs. Table 2 shows a summary of this process.

Artificial intelligence (AI) can improve biometric identity systems by analysing gait or by identifying absurd behaviours as they are designed to observe and react to their surroundings (Verma, Sharma, Deb & Maitra, 2021). Verma et al. (2021) mention that artificial intelligence applies to any machine that needs to think like a human resulting in continuous learning and problem-solving. Since artificial intelligence can do repetitive jobs, it is ideal for aiding at airport border control, where thousands of travellers are processed daily. Research is taking place in artificial intelligence and the linked Generated Adversarial Networks (GAN), which can be used for image processing and face detection (Aggarwal, Mittal & Battineni, 2021). However, challenges are also faced by the use of AI, such as continuous learning and decision-making ability (Mir et al., 2020). For instance, AI in biometric identity programs will need to learn gait normal and abnormal behaviours and will also need to know facial imaging. Another challenge is security, to manage the prevention of attacks and prevent the shared learning of confidential data (Mir et al., 2020b), as will be with CBP and their biometric systems.

2.6. Privacy

Following this initial pilot test, the DIST was developed into the TVS system. Main changes included the temporary storage of photographs in

Table 3
Qualitative Interviewee Details.

Name	Position Title	Organisation
Mike Hill	Founder and CEO	Sensi Pass
Benji Hutchinson	Vice President	NEC
Tim Meyerhoff	Director	Iris ID
CBP Officer	CBP Officer	CBP, Miami International Airport
Igor Oliviera	IT Director	VisionBox
Brett McLindin	Engineer / Facial Recognition Researcher	Independent PhD Researcher, Biometrics Institute

a secure Virtual Private Cloud (VPS) and the use of cloud-based biometric matching services to compare photos (DHS, 2017b). Several companies such as Vision-Box, SITA and NEC Corporation provide the biometric infrastructure for the pilot tests and have their own privacy policies (Burt, 2018b). However, some privacy issues about how CBP stores the data and how long it is stored are emerging (Burt, 2018b). According to a privacy report published by CBP in 2017, federals are evaluating airline compliance with protection requirements (DHS, 2017b).

Furthermore, the Electronic Privacy Information Centre (EPIC) is concerned that the biometric entry-exit program lacks the appropriate privacy safeguards and argues that the public should be informed about these systems (EPIC, 2018). However, CBP mentions that "regardless of immigration or citizenship status, CBP deletes all photos from the TVS within 12 h of the match" and purged from IT systems within 14 days (Kimery, 2018). The storage of data such as travellers' images on a system that a third party may utilise threatens customer privacy, which is an ongoing challenge. As Thommesen (2009) suggests, privacy for the customer is a means of ensuring security or protection against harm. Therefore, informing passengers of how their data is handled and securing trust can help in increasing conformance to newer technologies.

3. Methodology

This paper uses the case study of Biometrics at Dublin airport, capitalising on mixed methods. A qualitative approach involving semi-structured interviews and direct observation of pilot tests at Dublin Airport is taken. The semi-structured approach provides flexibility in conversation and enough control to stay within the study's parameters. Interviews lasted between one to one and a half hours. Additionally, interviews were recorded and transcribed, the transcripts were then confirmed by the interviewees, ensuring research validity. Bias was avoided during the interview through open-ended unbiased questions. Research validity is established using the triangular method, as findings from the interviews are incorporated with empirical studies. Studies have suggested that using the triangular method improves both credibility and validity of research by providing a detailed and balanced overview (Ashour, 2018).

Interview recordings and transcripts were also re-visited to focus on common emerging themes. The following provides an overview of the professionals interviewed. All of the mentioned professionals agreed to be named, and they have been directly involved with either the development or implementation of certain biometric programs (Table 3). They range from organisations such as NEC and VisionBox, which supply the technology for facial recognition with CBPs biometric entry-exit program and biometric boarding, to Tim Meyerhoff from Iris ID, who has worked directly with John Wagner, Deputy Executive Assistant Commissioner of CBP, and Colleen Manaher, Executive Director of CBP.

Quantitative data is utilised to quantify the impact and highlight the successes and failures of the technology. U.S. Preclearance facilities at Dublin Airport is used as a case study. There is difficulty and complexity in collecting or obtaining data, such as match scores and decision thresholds used by the systems, on biometrics and facial recognition (Sprokkereef, 2008; Iglezakis, 2013; Labati et al., 2016). The challenges lie in evaluating accuracy as imposter attempts so far have been very few (MacLeod and McLindin, 2011; Labati et al., 2016). To substitute for the gap in quantitative research, secondary sources involving previously conducted reliable surveys and statistics are utilised. Sources of secondary data used include:

- The Passenger IT Trends Survey 2020 by SITA analyses how comfortable passengers are with utilising biometrics at airports.
- Dublin Airport Authority CBP Statistics – relating to process efficiencies in DUB.
- Other – Biometric Pilot Testing Results from U.S. airport test locations.

Direct observation has been conducted on facial recognition technology as part of the biometric entry-exit process and biometrics e-gates pilot test conducted at Dublin Airport in November of 2018. Participant observation has been successfully implemented by several scholars (Efthymiou, 2016; Efthymiou & Papathedorou, 2020).

One of the limitations is that the majority of U.S. airports, which have implemented the entry-exit program have not been analysed due to access restrictions and time limitations. The analysis is limited to results from pilot test results and issues published in news reports and articles, including the insight gained from interviews and online discussions.

4. Discussion and analysis

Many of the challenges faced with facial recognition and biometric entry-exit included inconsistent matching rates, low matching rates during pilot trials, network availability issues, bypassing facial recognition and the need for stakeholder involvement.

4.1. Inconsistent matching rate due to certain factors

The biometric entry-exit program only includes passengers between the ages of 14 to 79. Standard procedures are used for passengers outside the age range, including children, the elderly, and some with reduced mobility. The inability to match images for specific age groups was also a factor in the low biometric confirmation rate. Similarly, one interviewee also mentioned that algorithm performance is better for photos not taken long apart (timing). According to the DHS (2018), results from the pilots showed the following:

Ø Passengers under 29 and over 70 years of age had lower match rates.

Persons under the age of 29 accounted for 18 percent of passengers but 36 percent of all passengers whose photos resulted in false rejects. Similarly, passengers over 70 represented 4 percent of all passengers but 10 percent of all passengers whose photos resulted in false rejects. Many of these photos reject challenges were due to the time and age difference from when the photograph in the gallery was taken and stored and the age when the live photograph was captured on the day of travel. This time difference can be several years, during which a person's facial features may have changed (DHS 2018). One interviewee also agrees that it is a dramatic change in facial features for a photo captured as a child and a photo captured at an older age. Additionally, Spreeuwers et al. (2012) argue that 5 percent of European passports have insufficient quality photos, which can also contribute to issues in identity verification.

Table 4
Summary of Biometric Exit Tests from 2013 to 2016 (DHS, 2018).

Test	Biometric Mode	Dates	Location	Results
Air Entry-Exit *Re*-engineering Project	Test and evaluation of available technologies	2013 to 2015	Laboratory testing	Facial, iris, and fingerprints were all identified as potential biometric technologies.
Southwest Border Pedestrian Exit Field Test	Face and iris scanning	2013 to 2016	Otay Mesa land port of entry (San Diego, CA)	Travelers preferred facial recognition over iris scanning. Limited iris records were available for matching.
Biometric Exit Mobile Air Test	Mobile fingerprint reader	2014 to 2016	10 international airports	Manual process to read fingerprints was inefficient for large-scale exit processing.
1-to-1 Facial Comparison Project	Facial recognition technology	2014 to 2015	Dulles International Airport	Facial recognition technology had minimal impact on visitor entry processing and the travelling public.
Departure Information System	Facial recognition technology	2015 to 2016	Atlanta Hartsfield-Jackson International Airport	Facial recognition technology had minimal impact on the aircraft boarding process and the travelling public.

Ø Matching of certain nationalities contributed to a low biometric confirmation rate.

U.S citizens have the lowest biometric confirmation rate and are six times more likely to be rejected than foreign citizens. This was mainly because foreign visitors had to meet passport requirements, resulting in many photographs being available in the digital gallery. At the same time, U.S citizens had fewer photographs available in the digital gallery.

In conclusion, the quality of photographs in the gallery or previous encounters with U.S authorities was an important factor for accurate matching. Interviewees mentioned airport lighting and image distortion could also have effects on quality. He states that this needs to be controlled by increasing illumination to ensure travellers' faces are well lit. Similarly, Zou et al. (2007) also mentioned variation in lighting could cause dramatic changes in facial appearance. DHS (2018) reported that photos were taken at an incorrect angle. Photos from several years ago, photos in which faces were obscured with hats, glasses or scarves, and distance contributed to affecting the biometric matching rate. Such factors have also been confirmed in previous facial recognition studies (Conde et al., 2012; Sanchez del Río et al., 2015; Labati et al., 2016).

4.2. Low matching rates during pilot phase

Table 4 shows a summary of the biometric exit tests which took place from 2013 to 2016. From the table, it can be seen that all results favoured the use of biometric technology, specifically the use of facial recognition, as it did not prove to be a hindrance to either processing rate, the public or the boarding process.

However, during the initial pilot phases of the biometric entry-exit program from August to December 2017, CBP could not match biometrically approx. 15 percent of all passengers. Fig. 1 shows a comparison between technical and biometric match rates from August to December 2017. The technical match refers to TVS' algorithm's ability to match captured photos to ones in the gallery (DHS 2018). Whereas, biometric confirmation rate is the percentage of passenger's identities confirmed using facial recognition during the biometric exit pilot flights (DHS 2018). Technical problems and system disruptions explain the decline in biometric confirmation.

Similarly, Fig. 2 shows that during the pilot phase, all nine airports could not match photos for approx. 15 percent of the passengers, identifying the need for improvement. As part of this, results from CBP's pilot showed the following:

- Approx. 0.03 percent of matches were 'false positives', which referred to the passenger's photo being incorrectly matched to the image of another individual.
- Approx. 0.5 percent of matched were 'false rejects', which referred to a failure in matching a passenger's photo to another image of the same individual.

False positives can pose a higher security risk. The matching of one passengers' photo to another passenger's photo can result in incorrect identity verification. Additionally, false rejects must also be reduced to increase the efficiency of the facial recognition process. According to Labati et al., (2016), several factors can contribute to the quality deterioration of a biometric sample, shown in Table 5. Although Labati et al. (2016) discuss these with regards to e-gates, these can also be applied to the Biometric Entry Exit program in the context of Automated Border Control (ABC) involving biometrics.

Table 5
Factors contributing to Quality Deterioration of a Biometric Sample (Labati et al., 2016).

Factors	Context
User related	Physical and behavioural
User-sensor interaction	Environmental and operational
Acquisition sensor	Ease of use, maintenance, acquisition area and resolution
Processing system	Constraints on storage, exchange speed, government regulations, network communication

Labati et al. (2016) mention additional user-related and user-sensor interaction factors affecting biometric quality. From the observation of facial recognition boarding, these factors can be evident and include inexperienced travellers, stress, luggage, lack of feedback, lack of supervision by an operator. Although there is a 98 percent accuracy in matching photographs to the gallery (technical match), much improvement is yet to be seen with the confirming an increased number of passengers using facial recognition (biometric match). As such, questioning CBP's ability to expand the program to full operational capability by 2021 successfully.

4.3. Network availability issues

During the pilot phases, technical problems were encountered due to issues with network connectivity issues and sustaining links to the TVS. Additionally, frequent system disruptions slowed down the capturing of facial images and the automated data exchange between the cameras and TVS, which as a result, delayed timely matching and verification responses. According to DHS (2018), this was witnessed at all four pilot sites, and the matching service could not be resumed until the cameras were rebooted. This resulted in either boarding delays or airlines non-compliance with facial matching and continuance of utilising standard boarding procedures. Similarly, connectivity issues were also experienced during the facial recognition pilot trial at Dublin Airport. During the trial at John F Kennedy Airport (JFK) in December 2017, poor connectivity led to the inability of CBP to process almost 13 flights. Therefore, the impact can be significant.

CBP is heavily reliant on wireless networks, which is the leading cause of poor connections. Additionally, lower network strengths were witnessed during peak periods when many passengers were also connected to the wireless network. Connecting wirelessly is not the optimal solution, and CBP must utilise a wired connection for stability.

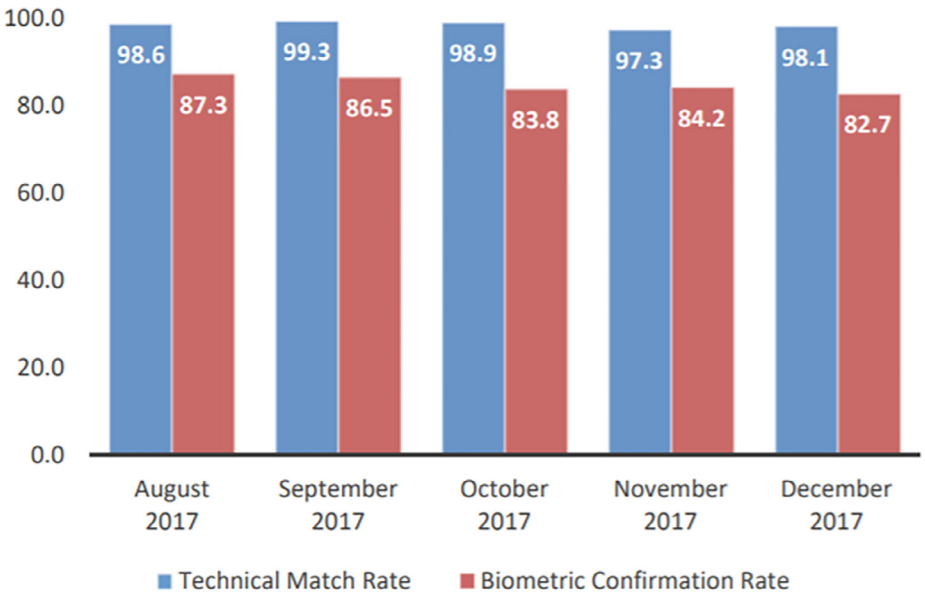

Fig. 1. Comparison of Technical and Biometric Match Rates from August to December 2017 (DHS, 2018).

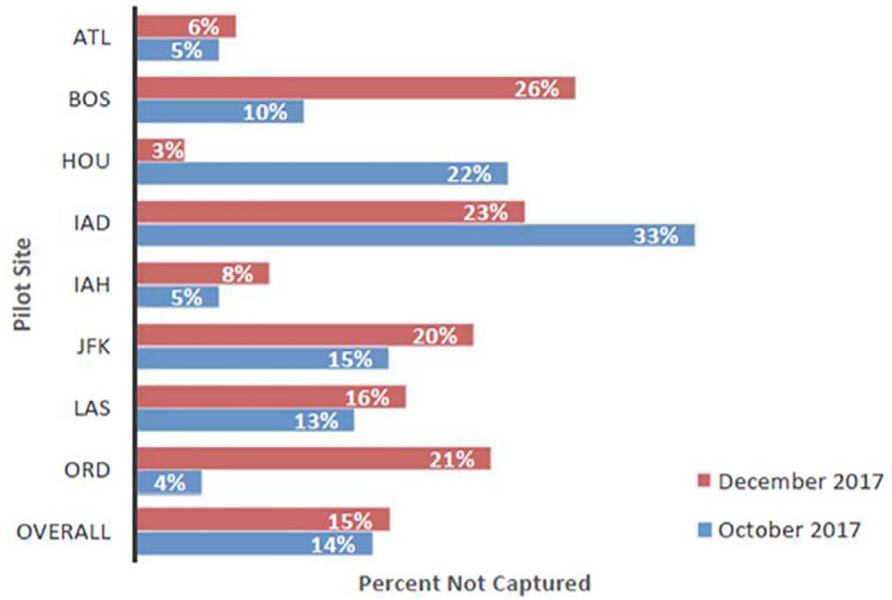

Fig. 2. Airport Rates of Failure to Capture Photos for Selected Months in 2017 (DHS, 2018).

4.4. Bypassing use of facial recognition

The occurrence of irregular operations significantly affected the biometric matching of passengers during the pilot in 2017. As the allotted time for boarding is reduced, CBP allowed many airlines to bypass the biometric processing to save time and permitted boarding with the standard procedure of scanning boarding passes, which the airlines also favoured as they aimed for on-time departures. However, this can pose a challenge as repeatedly permitting airlines to return to standard boarding procedures may become an unbreakable habit. Results from the CBPs pilot showed that in 2017, more than 220 flights departed, with fewer than 75 percent of passengers being biometrically confirmed (DHS, 2018). Therefore, if CBP plans for full operational capability by 2021, a solution to this issue must be sought.

Additionally, shortages of staff have also been a factor for airlines bypassing the facial recognition process. CBP recognised that they would not have adequate staff to support the full operational capability if airlines did not agree to provide staff (DHS, 2018). If CBP officers were to conduct biometric processing for all departing passengers at boarding gates, CBP would have no staff available for its enforcement activities. To add to this, it can be said that airline staff must be responsible for boarding their flights, even when it requires the ability to operate facial recognition technology. However, when airline agents are not trained to resolve when the technology doesn't cooperate or causes issues, would airline staff resolve to standard boarding procedures?

Moreover, it is operationally difficult to measure the time for CBP officers to go from gate to gate to conduct passenger screening. It would also be challenging to determine the impact of this due to flight delays. Furthermore, eliminating the need to wait for CBP officers to arrive at the gate can also reduce the risk of delayed flight departures.

4.5. Need for stakeholder involvement

Without airline partnership and support, CBP estimates a dramatic increase in cost and staffing levels, for instance, a rise in program budget from $1 billion to $8 billion and a similar surge in staffing requirements from 441 to 6000 (DHS, 2018). Wagner, the Deputy Executive Assistant Commissioner of CBP, mentioned that CBP initially lacked stakeholder

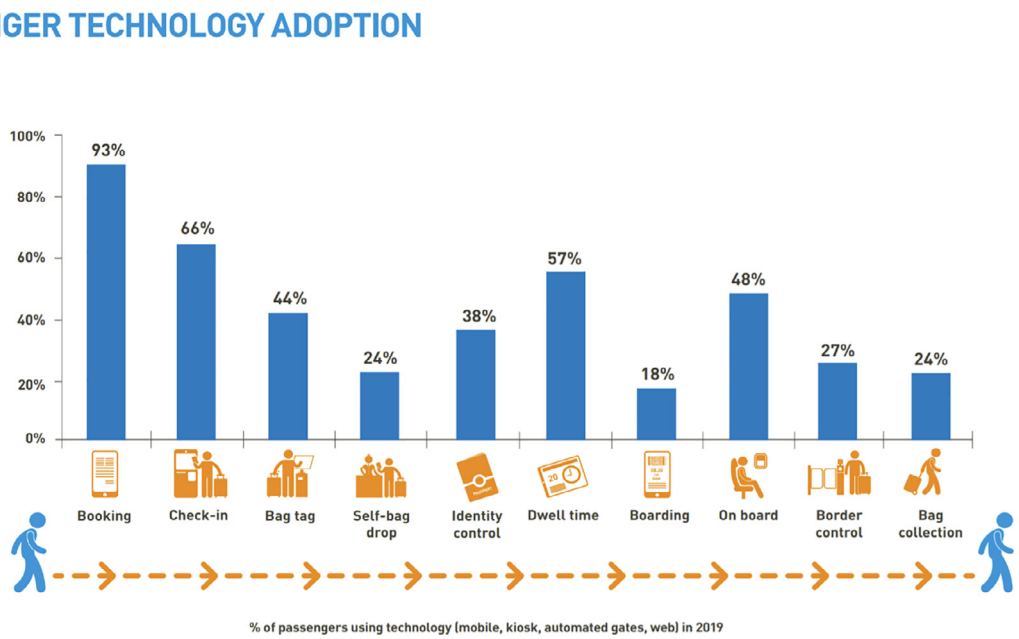

Fig. 3. Technology adoption across the airport journey (SITA, 2020).

support, "travel industry stakeholders were opposed as they thought it would cost money and slow down people". However, since after realising the benefits the technology can provide, such as an approx. 40 percent reduction in boarding times, airlines have continued to form a partnership with CBP. In 2017, JetBlue was the first airline to run its biometric technology along with CBP's facial recognition matching at Boston Logan International Airport. Soon after, Delta, American, Lufthansa and British Airways also followed (CBP, 2018a).

In addition to airline involvement and support, a collaborative approach for support from the airports is also crucial in helping overcome the challenges. A 2018 Air Transport IT Insights study by SITA, showed that over one-third of airlines currently adopt biometrics admit that integration of technology and lack of standards are significant challenges (BTT 2018). Some studies also confirm that different stakeholders become crucial to its survival during various stages of the project, requiring mutual and ongoing adjustment to balance competing views (Brown, 2003; Zhang et al., 2005).

4.6. Passengers willingness to use biometrics and the issue of privacy

According to Passenger IT Trends Survey conducted by SITA in 2020, boarding has one of the lowest levels of technology adoption, at 16 percent. Similarly, technology adoption is also one of the lowest at border control, at 27 percent, as shown in Fig. 3.

In terms of satisfaction, Fig. 4 shows that passengers who were using technology at security were far more satisfied than non-users of technology. However, a survey from the 2017 report showed that satisfaction levels are high amongst passengers using any biometric options, 8.4 on a scale of 1–10 (SITA, 2017). These results suggest that implementing biometric technology at passport control and at boarding can provide increased passenger satisfaction and operational benefits. When passengers were asked about biometrics, 57 percent said they would use biometrics instead of a passport or a boarding pass. Although this is a somewhat low score, it can be noted that as passengers learn more about how biometric technology can be beneficial for them and improve security, they will be more willing to utilise it, also the opinion of two interviewees.

In another survey by Accenture in 2014, 89 percent of respondents mentioned they were willing to share biometric details when travelling internationally (Caldwell, 2015). Results from IATA Global Passenger Survey in 2017 also suggested that passengers use one token biometric identity for all their travel transactions, from booking to security and border control and baggage collection (IATA 2017). Survey results show that out of the 58 percent of passengers who used automated border control, 90 percent were satisfied with the process (IATA 2017). In addition to this, from SITA (2020) Survey, Fig. 4 shows that passengers who used technology through security were significantly more satisfied than non-technology users. From these survey results, it can be concluded that travellers are not opposed to using biometrics but are willing to utilise them across their airport journey.

Perceived privacy is a concern amongst some travellers. SITA's 2017 Passenger IT Trends survey suggests that 33 percent of passengers have privacy concerns regarding biometric recognition at airport borders (SITA 2017). However, the privacy of the travellers is kept intact. The transferring of images is conducted through a template and not the image itself. The template consists of several binary digits such as 1's and 0's, which are securely encrypted and cannot be reverse-engineered back into an image as mentioned by an interviewee. Additionally, CBP states that after a flight departs, the images of travellers are erased from the database.

Travellers have no clue about the potential of mishappening and threats, so they get upset with a process such as their picture being captured, says an interviewee. They argue that society needs to come to terms with the fact that these technologies that offer increased security levels are critical. Research also suggests that informing passengers of data handling and ensuring trust can help increase conformance with newer technologies (Thommesen, 2009). Table 6 below provides a summary of the challenges encountered with the trials.

5. Multimodal biometrics

Multiple studies on multimodal systems have suggested that using a combination of biometric modalities can reduce some problems associated with mono-modal systems (Cimato et al., 2016; Gamassi et al., 2005; Jain et al., 2004; Labati et al., 2016). These include sensor accuracy, non-universality, noisy data and increased robustness due to limited ability for spoofing (Labati et al., 2016). The benefit is that the biometric system can obtain biometric samples from multiple modalities in one transaction. For instance, a face image and irises can be captured with the same camera. Although the system's complexity can increase

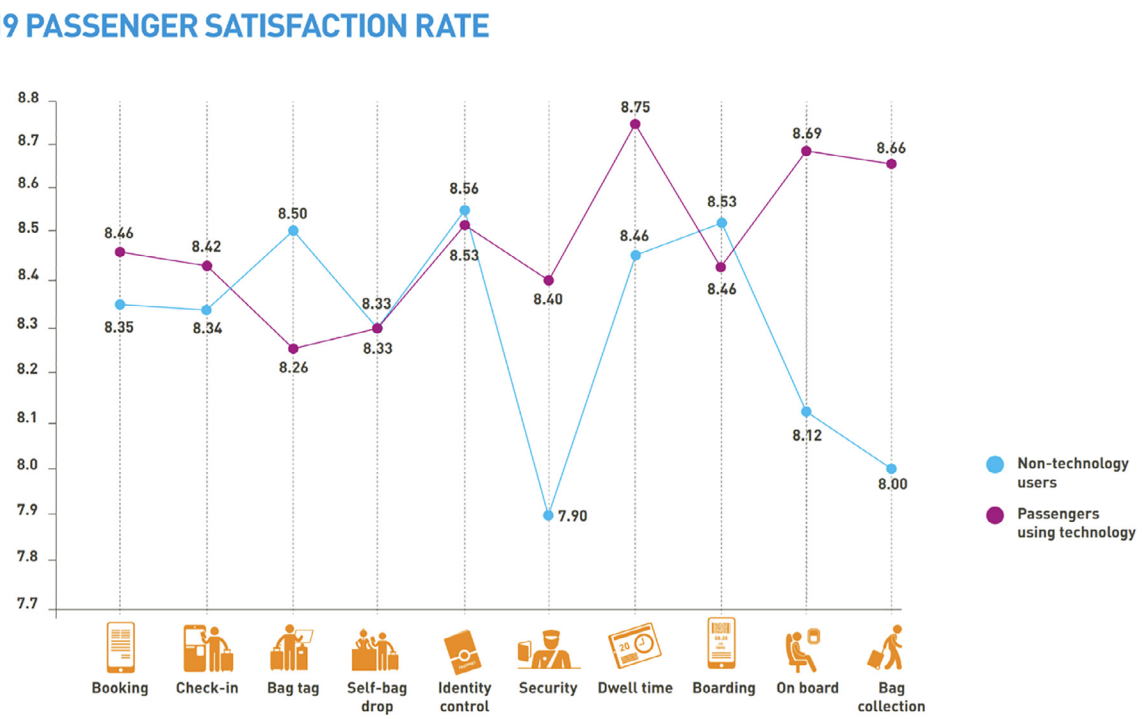

Fig. 4. Satisfaction levels across the airport journey (SITA, 2020).

Table 6
Summary of Challenges.

Challenges Faced	Detail
Low Biometric Matching Rate during the pilot phase	Although the technical match rate was 98%, the low biometric match was due to age range, nationalities, illumination conditions, and obscuration factors.
Inability to match certain ages or nationalities	It is leading to a low biometric match rate. This is mainly due to photo quality or photo availability.
Connectivity issues due to Network Availability	CBP is heavily reliant on wireless networks to conduct the biometric entry-exit program. Frequent system disruptions slowed down the data exchange process.
Bypassing Use of Facial Recognition	Many airlines are reverting to standard scanning for boarding if CBP officers are unavailable or if network issues are present to avoid flight delays.
CBP officers managing new biometric duties at the gate in addition to existing responsibilities	The opinion is that airline staff should be responsible for boarding and managing the technology for their flights. However, during the trial, much of this was left to a CBP officer.
Stakeholder Support	Gaining support from airlines and airports is posing to be challenging. Without this support, costs and staffing requirements will dramatically rise.
Total reliance on airlines is a risk	If airlines fail to use the biometric program, provide funding, or staff the process adequately, it can ultimately lead to failure.
Concerns for Privacy amongst travellers	This is mainly due to some travellers not fully understanding the purpose and benefits of the technology to their journey and overall security.

through the use of multiple modalities, according to Labati et al. (2016), a higher throughput is also achievable. Similarly, (Kosmerlj et al., 2005) also argues that through the use of multimodal, an improvement in matching performance could result, which ultimately will lead to increased efficiency inflow and a better experience for the traveller.

However, the implementation of multiple modalities along with facial recognition can cause some issues for CBP's biometric entry-exit program. As seen from the above challenges, current funding is proving difficult to achieve without stakeholder cooperation. With the inclusion of multimodalities, system costs and acquisition times, and computational times can increase (Kosmerlj et al., 2005; Labati et al., 2016). Nevertheless, in the case of global pandemics where travellers can be required to wear face masks, the use of iris recognition along with facial recognition may be deemed more efficient.

6. Case study: U.S. pre-clearance and the biometric entry exit program at Dublin airport

Dublin Airport is one of the few airports globally and one of two airports in Ireland to offer pre-clearance facilities by US immigration officials (Murphy & Efthymiou, 2017). A total of 12 preclearance gates are located between upper and lower levels, covering nine aircraft stands. At its peak during summer 2018, the airport facilitated 10 airlines operating 446 weekly flights to 20 North American destinations (Conghaile, 2018). It can be said that Dublin Airport is a substantial transatlantic gateway for travel to the U.S. The Biometric Entry Exit program involving the use of facial recognition has been operational at Dublin Airport since June 2018.

Taking less than two seconds, the facial recognition verification process provides a 99 percent matching rate (Airport Business 2019). It has provided faster processing times, reducing waiting queues and, as a result improving passenger satisfaction. These results can be seen across airports that have implemented the biometric entry-exit program, including Dublin Airport. Table 7 shows a summary of trends in passenger numbers and CBP processing by month.

The table provides a comparison of 2018 vs 2019, including the total number of passengers processed by CBP per month at Dublin Airport. The percentage of passengers processed within 30 min and within 45 min is also outlined. It can be seen from the table that although months January to March 2019 experienced a rise in the number

Table 7
Summary of Trends - Passenger Numbers & Processing by Month at Dublin Airport (Source: DAA Internal Reports).

	Jan	Feb	Mar
2019 Within 30 mins	91%	97%	87%
2019 Within 45 mins	99%	100%	98%
Total Passengers	89,989	72,723	119,419
2018 Within 30 mins	70%	84%	65%
2018 Within 45 mins	89%	97%	83%
Total Passengers	75,781	63,716	110,090

of passengers (compared to 2018), the percentage of passengers processed within the timeframes has also increased. For instance, an approx. 15.8% increase in passenger numbers can be seen in January 2019 compared to January 2018. However, the percentage of passengers processed within 30 min in January 2019 was at a higher rate than in January 2018. This is also the case for the remaining months of February and March, where Dublin Airport Pre-clearance witnessed an increase in passengers but also improved processing statistics. Previously, 21 percent of passengers would be waiting above 45 min for processing in Jan 2018. In Jan 2019, this was reduced to approx. 1 percent of passengers max waiting above 45 min. Although other factors can come into play, such as staffing levels and training, part of the improvement is automated processing due to the biometric entry-exit program, which came into effect in June 2018. Passengers are now spending less and less time at the CBP booth with an officer, as identity verification is almost instant. Due to this, CBP officers are processing passengers faster, avoiding the build-up of lengthy queues.

CBP has set up one lane for standard processing without the biometric aspect to allow back-up procedures in IT failures. This aids officers in keeping familiar with traditional methods of processing passengers so operation can continue in the event of an outage. However, it can be said that additional measures should be in place to facilitate the processing of passengers in the event of system outages, as this can have a detrimental effect on flight departures and, as a result, additional pressure on airports in managing aircraft.

6.1. Facial recognition boarding: E-Gates

To further complement the biometric entry-exit program, CBP, in conjunction with American Airlines, conducted a biometric e-gate pilot trial in November of 2018. The ultimate aim is to implement biometric self-boarding over the coming years. This would involve the passenger presenting themselves at the boarding gate without a passport or a boarding pass. There are two tablet devices, as shown in Fig. 5, one with a camera facing the passenger and one with processing information facing the boarding agent. The passenger's photo will be taken as they arrive at the gate. The photo will then be compared against a small-scale photo gallery of passengers travelling on that particular flight. The photos in these galleries are compiled using the photos taken at CBP or photos stored on the passenger's travel document. Once the passengers live photo taken at the gate is matched with the photo in the gallery, a green tick shows, and the passengers are clear to board the aircraft.

However, suppose the photo does not match. In that case, a red cross will show. The passenger will proceed to the boarding agent at the gate, who will see the view in Fig. 6 and be responsible for verifying the passenger's identity before permitting them to board. There are several reasons why a match may not be made, and these will be discussed further in the next chapter. However, VeriScan, the firm implementing this technology for e-gates, has mentioned verifying will take less than two seconds. Many airlines across the U.S. have already implemented this technology and have witnessed a reduction of approx. 20 mins in boarding times (Burt, 2019). Thus, showing huge benefit potential for not only airlines but also passengers. Passengers were notified of the process through a notice posted in front of the gate. This ensured awareness and transparency. As the literature suggested, passengers are more likely to conform to procedures if aware of how their data will be used (Thommesen, 2009).

Fig. 5. Photo Capturing Tablet (Foreground) Agent View Tablet (Background).

6.2. Results from e-Gate trial and the challenges experienced

The biometric e-gate was a trial run at Dublin Airport (Table 8). It was conducted in a two-step process to ensure all passengers were scanned before boarding. The first step included the passenger presenting themselves in front of the camera, and the second step included the boarding agent scanning the boarding pass on the scanner. The trial was conducted over three days and the results were as follows:

Emerging challenges included infrastructure and equipment set-up and network issues. Initially, infrastructure issues were addressed in meetings as the plan involved a set-up of cameras built into the boarding gates. However, as the gates at Dublin Airport are cross utilised amongst many airlines and not all airlines would yet be using e-gates, installing cameras would have become very costly. VeriScan provided a solution to this by using portable equipment, which could be set up for a boarding gate and removed after the operation, as shown above in Figs. 5 and 6.

Other challenges revolved around receiving network at the boarding gates. The photo galleries to which live photos are compared to being stored on a cloud. Therefore, for biometric boarding to occur, connection to the cloud and network through WIFI signals is critical. However, during the trial, there was very weak WIFI signals present airside at the airport. The network strength was tested a day before the trial run; however, this was conducted landside and not airside. The signal variance between landside and airside was not brought to attention. The following day portable WIFI hubs were bought to strengthen the network connection. Nevertheless, this is not feasible as a permanent solution. In the future, the airport may need to scale up the network signals to allow for a smooth boarding operation.

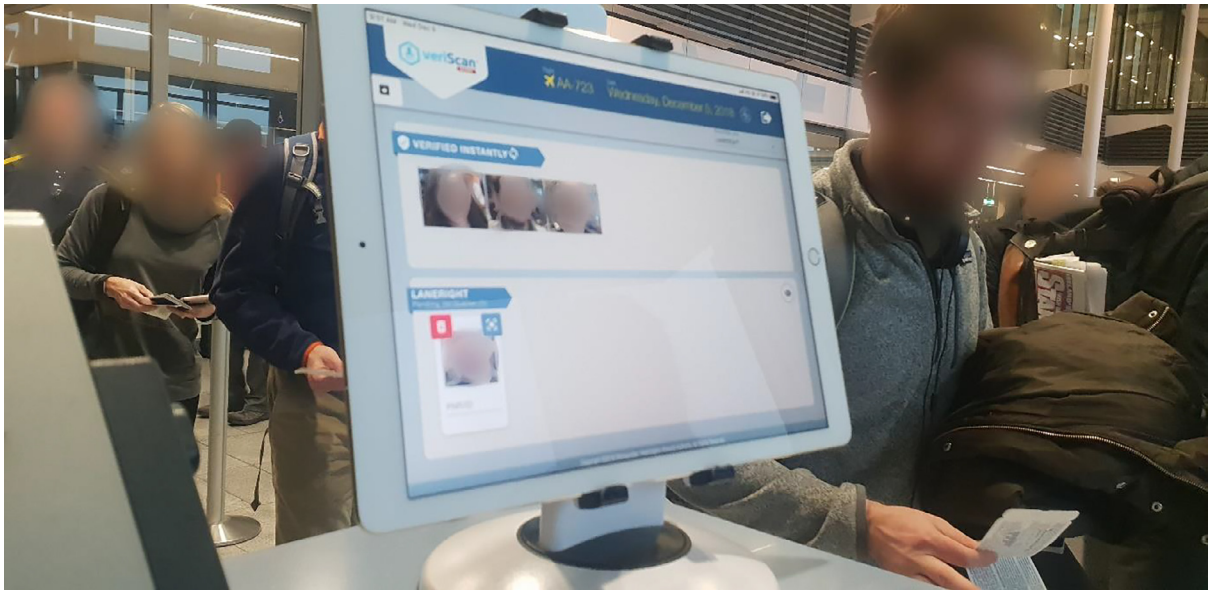

Fig. 6. Agent View Tablet showing passengers being verified (Top-row) and passengers not matched (Bottom Row).

Table 8
E-Gate Boarding Trial Results Dublin Airport.

Pilot Trial Day	Number of passengers boarded	Time taken to board
Day 1	116	17 min(Two-stage process including scanning of boarding passes)
Day 2	160	14 min(Two-stage process including scanning of boarding passes)
Day 3	110	7 min(No boarding passes were scanned on this day, only facial recognition)

7. Contributions and implications

7.1. Contributions to literature

There has been a significant gap in the research are of biometrics in an airport environment. Not many studies have investigated the effects of using facial identification or AI at airport border controls. Studies have been conducted on solely border control (Zaharia & Pietreanu, 2018), on technology at airport departures, air traffic control (Zaharia & Pietreanu, 2018), on technology impact on employees/travellers (Bogicevic et al., 2017; Kirschenbaum et al., 2012), but no study had addressed technological developments at U.S CBP or biometrics at airport border controls. This paper provides a detailed analysis of the use of facial recognition at airport border controls, its advantages, and the challenges (DHS, 2018), which can be faced by considering previously conducted trials and current case studies. This paper shows the time-saving opportunities available through biometrics and highlights passengers' attitudes towards technology at airports (SITA, 2020). Through interviews with biometric professionals and trial results, it has been confirmed that although technical match rates are high, biometric confirmation rates muse see some improvement. Further studies should look at the use of multimodal technology such as using both facial and iris recognition to provide a better process, especially in the age of pandemics where travellers are required to wear a face masque.

7.2. Practical implications

This paper provides practical challenges and implications which implementers of biometric technology at airports should consider. There is significant analysis on the matching rates, avoiding poor quality results and how the biometric system may be bypassed. Through a practical case study, the paper also demonstrates the added benefits of biometric technology, such as fast processing and boarding. It also shows how much stakeholder support is essential and that travellers should be educated on the benefits of the technology for their journey as many privacy concerns result from a lack of understanding. For additional trials or implementation of biometrics technology at boarding gates, the results of this paper can be beneficial due to the data on matching rates, analysis on why match rates can be low and the discussion on practical challenges which can be alleviated through stakeholder support and improved connectivity networks.

8. Conclusion and recommendations

An overview of biometric modalities and the factors crucial for a successful biometric system was discussed in the literature review, followed by the concept and need for biometrics at airport borders. Excessive waiting times at U.S ports of entry proved that a gap in operational efficiencies was present. In addition to the legal requirements for biometric implementation, it was clear that a biometric system was necessary. The excessive wait times indicate lengthy queues and crowded areas, which are not ideal in a pandemic world. Thus, we understand the importance of biometrics at border control and at airport security checkpoints, as they are touchless and reduce processing times, avoiding long queues and crowds. The entry-exit program at U.S preclearance facilities at Dublin Airport was observed and analysed, along with the facial recognition boarding trial to identify challenges and assess accuracy. Results showed that even with an increase in the number of passengers, the throughout rate remained high. Results from the biometric e-gate trial conducted in conjunction with American Airlines showed a dramatic decrease in time taken to board passengers onto the aircraft through facial recognition boarding. Some of the challenges faced included network connectivity issues and infrastructure issues. However, these were also encountered during pilot tests at other U.S. airports.

By interviewing industry professionals responsible for biometric programs, including CBPs entry exit program, further insight was received on the challenges and issues encountered. It was determined that although the technical match rate is high with facial recognition, the bio-

metric confirmation rate is yet to see some improvement. Upon exploration, several factors contributed to this low match rate, both user-related and system-related, which can be addressed through further process improvements. Additional challenges revolved around network availability issues and the need for stakeholder involvement and collaboration regarding operations, staffing and funding of the program. Furthermore, pressurising flight schedules also impacted the airlines' willingness to utilise the technology. From pilot tests at U.S airports, it was seen that shortages of CBP officers and reduction in allotted boarding time resulted in airline officials reverting to standard boarding procedures to achieve timely flight departures.

Following on from the challenges, recommendations to address the challenges faced by CBP, at both Dublin Airport and other U.S Airport locations are highlighted below (DHS 2018).

- CBP must collaborate with airline and airport stakeholders to overcome network connectivity, infrastructure issues, funding and staffing issues.
  A solid network connection must be established to ensure operational demands are met, including timely processing of passengers, timely departure performance of aircraft, and avoiding inefficiencies due to system disruptions. Similarly, stakeholder input is needed to provide for funding and staffing for the program.
- Continuous improvement of algorithms to increase match rates that consider both age factors and quality, is needed.
  This can improve the process and remove bottlenecks in passenger flow, ensuring both operational efficiency and improved user experience. Improving match rates can also reduce operational complexities for CBP officials who supervise the process or airline agents, enabling them to focus on more critical tasks. An interviewee suggests that improving the facial recognition template is the best way to improve the matching accuracy. If the algorithms are not up to speed, you might not receive an accurate match and may need to revert to standard processing methods.
- CBP must develop back-up procedures or enforcement mechanisms to avert airlines from bypassing the biometric process after flight boarding.
  Bypassing the process defeats the purpose of the biometric entry-exit program, which is to verify identity with higher accuracy and with a larger aim of identifying imposters and visa overstays. This is often due to system disruptions, unavailability of officers or restricted boarding times. The development of an enforcement mechanism will ensure the biometric process is carried out in every scenario with consistency.
- Development of a plan for funding and staffing of the program is needed if airlines fail to collaborate with CBP in executing the program.
  Cooperation from stakeholders, especially airlines, is key to the success of the biometric entry-exit program. Due to its staff shortages and funding issues, CBP is currently reliant upon airlines to provide for the operation of the exit program at boarding gates in the U.S. Similarly, CBP is reliant upon airlines for funding of the program. Last, if airlines do not agree to cooperate, CBP must develop a back-up plan to ensure the success of its program.
- Inform the travelling public about biometric technology through a transparent and straightforward educational campaign and the benefit it provides to them and improve the overall level of security in air travel.
  As established through the thesis, many travellers have concerns regarding their privacy mainly due to a lack of awareness. Once they become more aware of the associated benefits, they will be more willing to cooperate. As interviewees stated, privacy is kept intact with the biometric systems. For instance, images are not transferred as the image itself but are transferred as templates, a series of encrypted binary digits that cannot be reverse-engineered back to the image, providing security. Similarly, an interviewee mentioned Vision Box's technology is built on privacy by design, a concept that ensures building privacy to design the system's operation and solution.

References

Aggarwal, A., Mittal, M., & Battineni, G. (2021). Generative adversarial network: An overview of theory and applications. *International Journal of Information Management Data Insights, 1*(1).

Airport Business. (2019). *Miami International Airport Launches Biometric Exit Technology [online] available from.* http://www.airport-business.com/2019/02/miami-international-airport-launches-biometric-exit-technology/. [15 May 2021].

Ashour, M. (2018). Triangulation as a Powerful Methodological Research Technique in Technology-Based Services. *Business & Management Studies: An International Journal, 6*.

Bakker, D. (2015). *The Strong Case for Automated Controls at the Border [online] available from.* https://www.internationalairportreview.com/article/76336/automated-border-controls/. [6 December 2020].

Bogicevic, V., Bujisic, M., Bilgihan, A., Yang, W., & Cobanoglu, C. (2017). The Impact of Traveler-Focused Airport Technology on Traveler Satisfaction. *Technological Forecasting and Social Change, 123*(C), 351–361.

Brooks, N. (2016). *Reducing the Risks - Airport World Magazine [online] available from.* https://www.airport-world.com/features/safety-security/5876-reducing-the-risks.html. [15 May 2021].

Brown, M. M. (2003). Technology Diffusion and the "Knowledge Barrier. *Public Performance & Management Review, 26*(4), 345–359.

BTT. (2018). Airports Face Biometric Integration Challenge. *Biometric Technology Today, 2018*(9), 12.

Burt, C. (2018). *San Jose to Become First All-Biometric Airport on U.S. West Coast for International Travel [online] available from.* https://www.biometricupdate.com/201808/san-jose-to-become-first-all-biometric-airport-on-u-s-west-coast-for-international-travel. [15 May 2021].

Burt, C. (2019). *Emirates Airlines Biometric Boarding with VeriScan at Dulles Reaches Full Operation [online] available from.* https://www.biometricupdate.com/201906/emirates-airlines-biometric-boarding-with-veriscan-at-dulles-reaches-full-operation. [15 May 2021].

Caldwell, T. (2015). Market Report: Border Biometrics. *Biometric Technology Today, 2015*(5), 5–11.

CAPA. (2017). *Airport Technology – What Passengers Want: Greater Personal Control of the Airport Process CAPA [online] available from.* https://centreforaviation.com/analysis/reports/airport-technology-what-passengers-want-greater-personal-control-of-the-airport-process-380131. [15 May 2021].

Carpenter, D., Maasberg, M., Hicks, C., & Chen, X. (2016). A multicultural study of biometric privacy concerns in a fire ground accountability crisis response system. *International Journal of Information Management, 36*(5), 735–747.

CBP. (2016). *Preclearance Guidance FY-2016-Final U.S. Customs and Border Protection [online] available from.* https://www.cbp.gov/document/guidance/preclearance-guidance-fy-2016-final. [22 February 2021].

CBP. (2018). *CBP Snapshot of Operations*.

CBP. (2019). *Biometrics U.S. Customs and Border Protection [online] available from.* https://www.cbp.gov/travel/biometrics#How-it-works. [15 May 2021].

Cimato, S., Gamassi, M., Piuri, V., Sana, D., Sassi, R., & Scotti, F. (2016). Personal Identification and Verification Using Multimodal Biometric Data. *2006 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety* [online] available from https://www.academia.edu/14333370/Personal_identification_and_verification_using_multimodal_biometric_data [17 May 2021].

Conghaile, P. (2018). *Irish Airports First in Europe with Facial Recognition for US Preclearance [online] available from.* https://www.independent.ie/life/travel/travel-news/irish-airports-first-in-europe-with-facial-recognition-for-us-preclearance-37412082.html. [15 May 2021].

DHS. (2018). *Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide [online] OIG-18-80*. available from https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf . [12 May 2021].

Efthymiou, M., & Papatheodorou, A. (2018). Evolving Business Models. In A. Graham, & N. Harper (Eds.), *(2018) the routledge companion to air transport management*. Routledge.

Efthymiou, M. (2016). *Challenges in aviation governance: Implementation of single european sky and eu emissions trading scheme*. Doctoral dissertation, University of West London.

Efthymiou, M., & Papatheodorou, A. (2020). Environmental Policies in European Aviation: A Stakeholder Management Perspective. *Walker, bergantino, sprung-much and loiacono (2020) sustainable aviation*. Cham: Palgrave Macmillan.

EPIC and CBP. (2017). *CBP Concept of Operations [online] available from.* https://epic.org/foia/dhs/cbp/biometric-entry-exit/Concept-of-Operations.pdf. [5 May 2021].

Gamassi, M., Lazzaroni, M., Misino, M., Piuri, V., Sana, D., & Scotti, F. (2005). Quality Assessment of Biometric Systems: A Comprehensive Perspective Based on Accuracy and Performance Measurement. *IEEE Transactions on Instrumentation and Measurement, 54*(4), 1489–1496.

Grünenberg, K., Møhl, P., Olwig, K., & Simonsen, A. (2020). Issue Introduction: IDentities and Identity: Biometric Technologies, Borders and Migration. *Ethnos*, 1–12.

Haas, E. P. (2004). *Back to the Future - The Use of Biometrics, Its Impact of Airport Security, and How This Technology Should Be Governed, 35*.

Hainen, A. M., Remias, S. M., Bullock, D. M., & Mannering, F. L. (2013). A Hazard-Based Analysis of Airport Security Transit Times. *Journal of Air Transport Management, 32*, 32–38.

Halpern, N., Mwesiumo, D., Suau-Sanchez, P., Budd, T., & Bråthen, S. (2021). The effect of organisational readiness, innovation, airport size and ownership on digital change at airports. *Journal of Air Transport Management, 90*, Article 101949.

Hart, M. (2015). Threshold to the Kingdom: The Airport Is a Border and the Border Is a Volume'. *Criticism, 57*(2), 173–189.

Hiller, H. H. (2010). Airports as Borderlands: American Preclearance and Transitional Spaces in Canada. *Journal of Borderlands Studies, 25*(3–4), 19–30.

Hilton, C. (2016). Fingerprints: A New Means of Identification in Airport Security Screening. *Journal of Air Law and Commerce, 81*(3), 32.

Hiney, N., Efthymiou, M., Morgenroth, E. L., et al. (2021). Regional airport business models: The Shannon Group as a case study. In A. Graham, et al. (Eds.), *Air transport and regional development case studies*. Abingdon, UK: Routledge (Taylor & Francis).

IATA. (2011). *Vision 2050 [online] available from.* https://www.iata.org/pressroom/facts_figures/Documents/vision-2050.pdf. [6 December 2020].

IATA. (2017). *IATA Global Passenger Survey 2017 [online] available from.* https://www.iata.org/publications/store/Pages/global-passenger-survey.aspx?_prclt=6UpFhfK7. [1 July 2020].

IATA. (2018). *IATA - Value of Aviation [online] available from.* https://www.iata.org/policy/promoting-aviation/Pages/index.aspx. [6 December 2018].

IBIA. (2018). *Glossary: Biometrics [online] available from.* https://www.ibia.org/biometrics/glossary. [29 December 2020].

IMS. (2018). *Migrant and Refugee Identification.*

Jain, A. K., Bolle, R., & Pankanti, S. (2006). *Biometrics: Personal identification in networked society*. Springer Science & Business Media.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20.

Janssen, S. (2017). 'Agent-Based Security and Efficiency Estimation in Airport Terminals'. In *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems [online] held 2017 at* (pp. 1840–1841). Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems. available from. http://dl.acm.org/citation.cfm?id=3091282.3091462 .

Kalakou, S., Psaraki-Kalouptsidi, V., & Moura, F. (2015). Future Airport Terminals: New Technologies Promise Capacity Gains. *Journal of Air Transport Management, 42*(C), 203–212.

Kirschenbaum, A., Mariani, M., Van Gulijk, C., Rapaport, C., & Lubasz, S. (2012). Trusting Technology: Security Decision Making at Airports'. *Journal of Air Transport Management, 25*, 57–60.

Knol, A., Sharpanskykh, A., & Janssen, S. (2019). Analyzing Airport Security Checkpoint Performance Using Cognitive Agent Models. *Journal of Air Transport Management, 75*, 39–50.

Kosmerlj, M., Fladsrud, T., Hjelmås, E., & Snekkenes, E. (2005). 'Face Recognition Issues in a Border Control Environment'. in Advances in biometrics [online] ed. by Zhang, D. and Jain, A.K. vol. 3832. Berlin, Heidelberg: Springer Berlin Heidelberg, 33–39. available from http://link.springer.com/10.1007/11608288_5 [27 June 2020]

Kushwaha, A. K., Kar, A. K., & Dwivedi, Y. K. (2021). Applications of big data in emerging management disciplines: A literature review using text mining. *International Journal of Information Management Data Insights, 1*(2), Article 100017.

Labati, R. D., Genovese, A., Muñoz, E., Piuri, V., Scotti, F., & Sforza, G. (2016). Biometric Recognition in Automated Border Control: A Survey. *ACM Computing Surveys, 49*(2), 1–39.

Lootens, K. J. B., & Efthymiou, M. (2021). The adoption of network-centric data sharing in Air Traffic Management. In *Research anthology on reliability and safety in aviation systems, spacecraft, and air transport* (pp. 127–151). IGI Global.

Mayhew, S. (2012). *Explainer: What Is Biometric Identification? [online] available from.* https://www.biometricupdate.com/201212/explainer-what-is-biometric-identification. [30 December 2020].

Mir, U. B., Kar, A. K., & Gupta, M. P. (2020a). Digital Identity Evaluation Framework for Social Welfare. In *International Working Conference on Transfer and Diffusion of IT* (pp. 401–414). Cham: Springer.

Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020c). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. *Government Information Quarterly, 37*(2), Article 101442.

Mir, U., Kar, A. K. K., & Gupta, M. P. (2021). AI-enabled digital identity-inputs for stakeholders and policymakers. *Journal of Science and Technology Policy Management*. 10.1108/JSTPM-09-2020-0134.

Mir, U., Sharma, S., Kar, A., & Gupta, M. (2020b). Critical success factors for integrating artificial intelligence and robotics. *Digital Policy, Regulation and Governance,, 22*(4), 307–331.

Morosan, C. (2016). An Empirical Examination of U.S. Travelers' Intentions to Use Biometric e-Gates in Airports. *Journal of Air Transport Management, 55*, 120–128.

Murphy, G., & Efthymiou, M. (2017). Aviation safety regulation in the multi-stakeholder environment of an airport. *Journal of Air Transport Studies, 8*(2), 1–26.

Negri, N. A. R., Borille, G. M. R., & Falcão, V. A. (2019). Acceptance of biometric technology in airport check-in. *Journal of Air Transport Management, 81*, Article 101720.

Nyst, C., Pannifer, S., & Whitley, E. A. (2016). Digital Identity: Issue Analysis. *Monograph, 8 June. Guildford: Consult Hyperion – Omidyar Network*. Available at: Http://www.chyp.com/ .

Pouloudi, A., & Whitley, E. A. (1997). Stakeholder Identification in Inter-Organizational Systems: Gaining Insights for Drug Use Management Systems. *European Journal of Information Systems, 6*(1), 1–14.

Ravichandran, T., & Rai, A. (2000). Quality Management in Systems Development: An Organizational System Perspective. *MIS Quarterly, 24*, 381–415.

Rockwell, M. (2017). *U.S. Biometric Exit Could Be Ready inside of Four Years - [online] available from.* https://fcw.com/articles/2017/11/28/cbp-biometric-exit-rockwell.aspx. [15 May 2021].

Schultz, M., & Soolaki, M. (2021). Analytical approach to solve the problem of aircraft passenger boarding during the coronavirus pandemic. *Transportation Research Part C: Emerging Technologies, 124*, Article 102931.

SITA. (2017). *Passenger IT Trends Survey 2017 SITA [online] available from.* https://www.sita.aero/resources/type/surveys-reports/passenger-it-trends-survey-2017. [22 June 2020].

SITA. (2020). *Passenger IT Trends Survey 2020 SITA [online].*

Spreeuwers, Hendrikse, & Gerritsen (2012). Evaluation of Automatic Face Recognition for Automatic Border Control on Actual Data Recorded of Travellers at Schiphol Airport. In *2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG), '2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)'* (pp. 1–6). held 6 September 2012.

Szyliowicz, J. S. (2004). Aviation Security: Promise or Reality? *Studies in Conflict & Terrorism, 27*(1), 47–63.

Thommesen, J. (2009). Privacy Implications of Surveillance Systems. 16

Verma, S., Sharma, R., Deb, S., & Maitra, D. (2021). Artificial intelligence in marketing: Systematic review and future research direction. *International Journal of Information Management Data Insights, 1*(1).

Wang, F., & De Filippi, P. (2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain, 2*.

Warnock-Smith, D., Graham, A., O'Connell, J. F., & Efthymiou, M. (2021a). Impact of COVID-19 on air transport passenger markets: Examining evidence from the Chinese market. *Journal of air transport management, 94*, Article 102085.

Warnock-Smith, D., Graham, A., O'Connell, J. F., & Efthymiou, M. (2021b). A disaggregated analysis of airlines and airports serving the Chinese market before and since the Covid-19 pandemic. *RGS-IBG Annual International Conference, 31 August - 3 September 2021, Online*.

Weitzberg, K., et al. (2021). Between surveillance and recognition: Rethinking digital identity in aid. *Big Data & Society*. 10.1177/20539517211006744.

Widdowson, D. (2007). The Changing Role of Customs: Evolution or Revolution? *World Customs Journal, 1*(1), 31–37.

Woodward, J. D., Orlans, N. M., & Higgins, P. T. (2003). *Biometrics: Identity assurance in the information age*. New York: McGraw-Hill/Osborne.

Woodward, J. D., Webb, K. W., Newton, E. M., Bradley, M., & Rubenson, D. (2001). *Army Biometrics Applications [online] available from.* https://apps.dtic.mil/dtic/tr/fulltext/u2/a393724.pdf. [17 May 2021].

Zaharia, S. E., & Pietreanu, C. V. (2018). Challenges in Airport Digital Transformation. *Transportation Research Procedia, 35*, 90–99.

Zhang, J., Dawes, S. S., & Sarkis, J. (2005). Exploring Stakeholders' Expectations of the Benefits and Barriers of E-government Knowledge Sharing. *Journal of Enterprise Information Management, 18*(5), 548–567.