The Paperless Paradigm:

Balancing Privacy, Security, Efficiency, and Convenience

in Air Travel in the Digital Transformation Age

Abstract

This article considers the use of facial recognition technology (FRT) and biometric data processing for the purpose of paperless air travel. Recent developments in artificial intelligence (AI) technology once again brought the attention to the various risks associated with its usage. On one side, the use of such technology offers efficiency, increased security, and convenience. On the other, it relies on the processing of sensitive personal data, a factor which requires stringent safeguards to ensure the protection of data and individuals' rights. While approaches towards privacy and data protection laws differ around the world, many Member States have already made significant progress in implementing biometric verification as part of their airport journey. The continuing increase in demand for travel necessitates international cooperation to ensure effective and secure passenger facilitation. The ICAO's TRIP strategy is integral in achieving this aim. This article explores the concept of seamless air travel reliant on biometrics and FRT, while analysing three examples from different jurisdictions. It evaluates the legal and regulatory frameworks in respect of privacy and data protection which apply to the use of biometrics and FRT. All of this is considered within the overarching framework of the ICAO TRIP strategy.

This paper is referenced in accordance with the OSCOLA Guide to Legal Citation.

Included figure has been created by the author using Microsoft Visio application.

Table of Contents

Figures

1. Introduction

AI has been around for over half a century and although the FLY AI Report by EUROCONTROL[1] states that the aviation industry has been slower in adopting technological and digital innovation, one could argue that the use of AI has been making significant strides in aviation in many different areas. One such area is the digitalisation of travel documents for the purpose of seamless travel experience and efficient passenger facilitation. States, airports, and airlines have been trialling and implementing paperless travel with different results. Boarding passes on mobile applications are now a common place, and the launch of machine-readable travel documents (MRTDs)[2] and their electronic version (eMRTDs, or ePassports), increased both security and efficiency in getting through the airport. The eGates enable travellers to self-serve their identity verification process allowing multiple passengers to verify their identity simultaneously, reducing wait times and impact on airports' resources. As passenger volumes continue to increase[3] and technological developments are gaining momentum, all eyes are turning to AI for solutions.

There is no global consensus currently on regulating AI. While emergence of generative AI triggered competition among governments and policy makers to put forward rules in a bid to lead the way, the EU has now set the precedent[4] with its EU AI Act.[5] The approach with the Act bears some resemblance in the way robust data protection laws have been implemented, with the EU leading the way. While the establishment of laws governing personal data goes back to 1970s, it was the General Data Protection Regulation (GDPR)[6] that rattled organisations around

---

[1] EUROCONTROL, 'The FLY AI Report. Demystifying and Accelerating AI in Aviation/ATM', (5 March 2020) https://www.eurocontrol.int/publication/fly-ai-report accessed 12 April 2023, pg.4

[2] ICAO, 'Doc 9303 Machine Readable Travel Documents' (2021) https://www.icao.int/publications/pages/publication.aspx?docnum=9303 accessed 1 June 2023

[3] With the exception of the times affected by the pandemic, the volume of travellers keeps increasing, and it is anticipated that it will surpass the pre-pandemic levels in 2024. *See*: Felix Richter, 'Tourism Recovery After Covid-19. International Tourism Approaches Pre-Pandemic Levels' (*Statista*, 18 December 2023) https://www.statista.com/chart/21793/international-tourist-arrivals-worldwide/; see also UNWTO, 'World Tourism Barometer and Statistical Annex' (*eLibrary*, January 2023) https://www.e-unwto.org/doi/abs/10.18111/wtobarometereng.2023.21.1.1 accessed 23 December 2023

[4] European Parliament, 'EU AI Act: first regulation on artificial intelligence' (19 December 2023) https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence accessed 27 December 2023

[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), OJ L 2024/1689

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L119/1

the world with its extraterritorial scope and significant fines[7] for non-compliance. In a similar fashion, the EU is pioneering with its EU AI Act.

The use of AI in aviation has been making significant headway. As part of the International Civil Aviation Organisation's (ICAO) Traveller Identification Programme (TRIP) strategy, security and facilitation of passengers plays a key role. Efficient traveller identification management heavily relies on AI technology such as facial recognition (FRT) or other biometric checks like fingerprint or iris scan. Biometrics are largely considered one of the most reliable ways of identification, but they are also considered very sensitive, as in most cases, they are inherently unchangeable. For this reason, data protection laws, such as GDPR, set higher degree of safeguards for the processing of biometric data when used for identification purposes.

In chapter 2, this article conceptualises the legal and regulatory landscape which influences achieving an objective of seamless travel experience and efficient passenger facilitation. In chapter 3, based on three examples, it analyses how the existence or lack of data protection laws and jurisdictional guidance impact the use of biometrics and FRT and how regulatory developments in AI may impact the way FRT is used at airports. The discussion in chapter 4 highlights ramifications of disjointed approach towards treatment of biometric data, and its impact on success of seamless travel experience and efficient passenger facilitation.

This article argues that while technology enhances travel efficiency, legislative requirements exist which require a balanced approach between privacy, security, efficiency, and convenience in air travel. This article suggests that ICAO should consider developing guidelines specifically addressing treatment of biometric data and use of FRT for the purposes of passenger facilitation in aviation (akin to the guidance provided for e.g. PNR), to ensure best practice and support for international cooperation.

2. Convergence of TRIP, Data Protection, and FRT

Among the strategic objectives of the ICAO is aviation security and passenger facilitation.[8] This dual objective focuses on ensuring that only legitimate travellers are able to cross borders—reducing threats like terrorism or human trafficking, while improving travel experience for passengers—making it seamless and less time-consuming. However, in order for these objectives to be fulfilled, certain elements require alignment. Figure 1 outlines the core aspects that together contribute to the achievement of ICAO's objective. Specifically, it shows the

---

[7] *Ibid*, Art. 83
[8] ICAO, 'Strategic Objectives' https://www.icao.int/about-icao/Council/Pages/Strategic-Objectives.aspx accessed 1 June 2023

convergence between the TRIP strategy, the role of FRT, and the importance of privacy and data protection, all of which play a key role in achieving the objective of seamless travel experience and efficient passenger facilitation. This section will delve into each of the elements and their intersections.
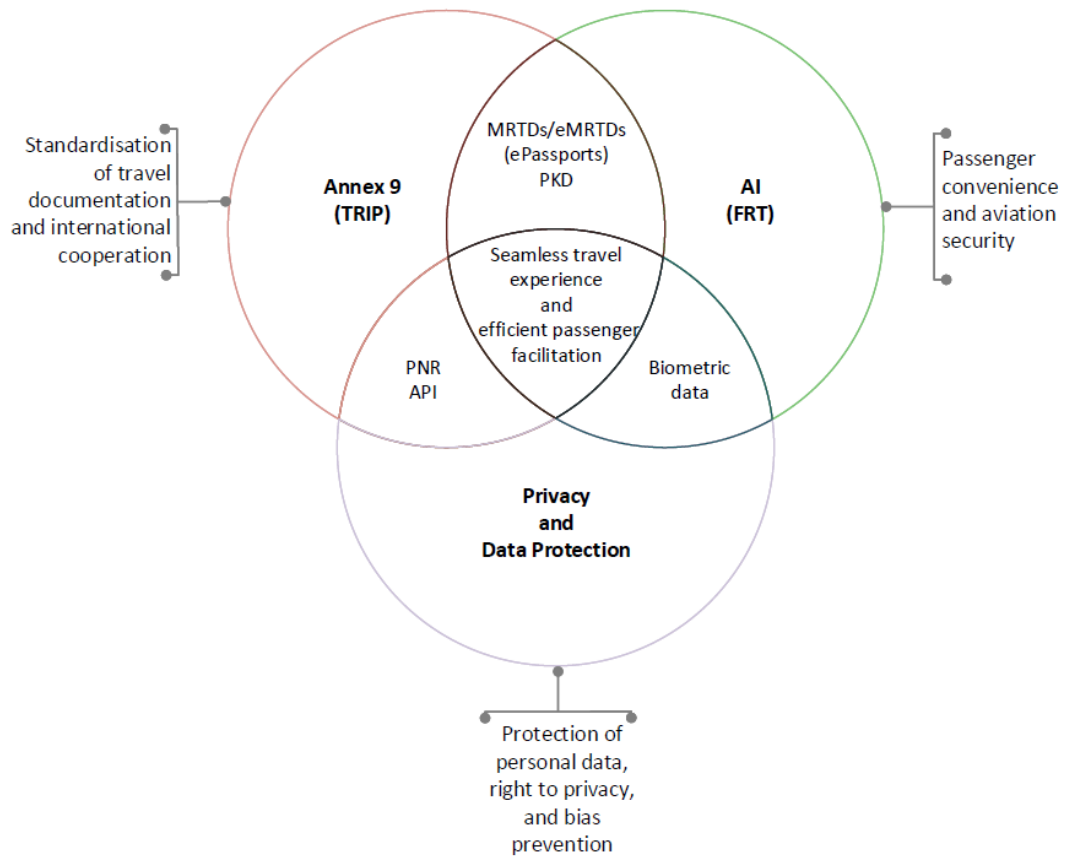

Figure 1. Convergence of TRIP, Data Protection, and FRT for the purpose of seamless travel experience and efficient passenger facilitation

2.1. Travel Identification Programme (TRIP)

As part of meeting its strategic objectives, the ICAO established TRIP which aims to ensure a well-coordinated approach to managing the interdependent elements of traveller identification. TRIP consists of five key elements: evidence of identity, MRTDs, document issuance and control, inspection systems and tools, and interoperable applications.[9] With the development of passports containing an electronic chip with biometric information (eMRTDs, or ePassports), ICAO encourages States to join the ICAO Public Key Directory (PKD). PKD is a central

---

[9] ICAO, 'Traveller Identification Programme. ID Management Solutions for More Secure Travel Documents' https://www.icao.int/security/FAL/TRIP/Pages/default.aspx accessed 1 June 2023

repository that enables the sharing of a public key which authenticates digital signatures confirming the chip has not been tampered with.[10] In conjunction with the biometric data stored on the chip, ePassports offer robust and secure way to validate the travel document and verify the identity of the passenger.

The TRIP strategy was adopted by the Member States in 2013 and complements the implementation of one of the ICAO's standards and recommended practices (SARPs), specifically Annex 9 (Facilitation) to the Chicago Convention[11]. Annex 9 ensures that border control and security check procedures are robust and efficient. In doing so it, inter alia, encourages Member States to engage in international cooperation in collection and sharing of Advance Passenger Information (API)[12] and Passenger Name Record (PNR)[13] data, as well as sets standards for, and encourages the use of MRTDs.[14] Abeyratne pointed out that exchanges of API data in particular are important for the prevention of terrorism.[15] Moreover, Chapter 9 (Passenger Data Exchange Systems) of the Annex specifically focuses on enhancing and streamlining the processes in relation to collection, transmission, and handling of passenger data. These guidelines recognise that information about passengers constitutes personal data and requires stakeholders to process it in accordance with the relevant privacy and data protection laws.

2.2. Privacy and Data Protection

To the extent that aviation's operational processes concern individuals and their data, privacy and data protection rules will apply in jurisdictions where Member States have implemented them or where extraterritorial laws apply. Seamless international travel relies on an exchange of information about passengers, as well as verification and identification of travellers using their personal data. Despite ICAO's guidance[16] and the PNR Directive,[17] sharing of the PNR data has

---

[10] ICAO, 'ICAO PKD' https://www.icao.int/Security/FAL/PKD/Pages/default.aspx accessed 1 June 2023
[11] Convention on International Civil Aviation 1944, Annex 9—Facilitation
[12] ICAO, 'Guidelines on Advance Passenger Information (API)' (June 2022) https://www.icao.int/Security/FAL/Documents/API%20Guidelines.EN.June2022.pdf accessed 1 June 2023
[13] ICAO, 'Doc 9944 Guidelines on Passenger Name Record (PNR) Data' (2010) https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf accessed 3 June 2023
[14] *Supra* note 2
[15] Ruwantissa Abeyratne, 'Traveller Identity' (2019) *Legal Priorities in Air Transport* pg. 251
[16] *Supra* note 12
[17] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime OJ L119/132

not been a trouble-free process.[18] Divergent rules on privacy and data protection led to challenges to the existing bilateral agreements.[19]

But technological developments brought on sharing of more sensitive data, in particular—biometric data, which uniquely identifies a person[20] through their distinctive physical or behavioural characteristics. For this reason, data protection laws such as GDPR mandate additional safeguards for their processing.[21] This adoption of biometric data for passenger verification has been experiencing a notable increase. With around 1 billion of ePassports in circulation,[22] the IATA's 2023 Global Passenger Survey (GPS) revealed that travellers prioritise speed and convenience and embrace the use of biometrics and off-airport processes to take advantage of seamless travel.[23] It is worth to note that in 2017, IATA launched its own initiative—One ID.[24] This initiative, however, focuses predominantly on seamless and contactless travel using biometrics, as a means of improving passengers experience.

The most common technology used in aviation industry to verify passengers using biometric data is facial and fingerprint recognition, with the former being used currently at most airports in combination with eMRTDs. While the increase in the use of biometric data for identity verification is currently driven by efficiency, an earlier push for this type of verification was triggered by security measures following the 9/11 events. In the aftermath of the terrorist attack, the US in particular proceeded with an intelligence-led strategy resulting in collection of vast amounts of personal data[25] and an approach that the biometric identification technology may assist with terrorist attacks prevention.[26] As a result, the US moved forward with a mandatory collection of biometric data of those who arrive in the US. Similarly, in 2004 the EU implemented the Biometric Passport Regulation[27] requiring all EU citizens applying for or

---

[18] Elena Carpanelli and Nicole Lazzerini, 'PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU' (2017) *Air and Space Law* 42.4/5 pg. 382; Arianna Vedaschi, 'Privacy and data protection versus national security in transnational flights: the EU–Canada PNR agreement' (2018) *International Data Privacy Law* 8.2 pg.126; Francesca Morschbach, 'Third Country PNR Mechanisms After the CJEU's Schrems II Judgment' (2023) *Air and Space Law* 48.1 pg. 92

[19] *See* e.g. Article 29 Data Protection Working Party Opinions: 2/2004, 7/2010, 10/2011 and Opinion 1/15 of the Court (Grand Chamber)

[20] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985) ETS 108 ("Convention 108"); see also OECD, 'Biometric-based Technologies' (2004) *OECD Digital Economy Papers*, No.101, OECD Publishing, Paris, pg. 10

[21] GDPR, Art. 9

[22] ICAO, 'ePassports Basics' https://www.icao.int/Security/FAL/PKD/Pages/ePassport-Basics.aspx accessed 3 June 2023

[23] IATA, 'Global Passenger Survey 2023 Highlights' https://go.updates.iata.org/GPS-Highlights-2023; and IATA, 'Speed and Convenience Top Priority for Passengers' (25 October 2023) https://www.iata.org/en/pressroom/2023-releases/2023-10-25-01/ accessed 9 June 2023

[24] IATA, 'One ID' https://www.iata.org/en/programs/passenger/one-id/ accessed 3 June 2023

[25] Jonathan P. Aus, 'Decision-making under pressure: The negotiation of the biometric passports regulation in the Council' (2006) *ARENA,* 11 pg.10

[26] John D. Woodard Jr, 'Biometrics: Facing up to terrorism' (2001) *RAND Arroyo Center* pg. 2

[27] Regulation (EC) 2252/2004 - Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

renewing passports to undergo a compulsory biometric enrolment. This received criticism over the proportionality of data collection and the approach where all individuals are considered possible crime suspects.[28] The case of biometric passports was tested by the CJEU when a passport applicant refused biometric data collection, citing violation of the EU Charter rights under Articles 7 and 8.[29] The court ruled fingerprint storage was necessary as it prevented falsification and illegal entry, balancing it against privacy and data protection rights which are not absolute and limitations are provided by law,[30] specifically Regulation No 2252/2004,[31] Article 1(2).

2.3. Facial Recognition Technology (FRT)

In the practice of using biometric data for verification at airports, FRT is the predominant method used in conjunction with eMRTDs for the purpose of identity verification as part of passenger facilitation. It is the most widely used method due to its universality, uniqueness of human face,[32] and unlike other biometrics such as fingerprint or iris scan, it can be used at close proximity or at a distance.

However, this technology is not foolproof and errors can lead to risks to national security, criminal justice, public safety, and civil rights.[33] While FRT is mostly considered as a reliable verification method, it does not cover all exceptions, such as cases of twins, siblings or doubles.[34] In 2018, a passenger gained entry via an e-Passport gate using her cousin's passport at Stansted Airport.[35] This is where fingerprint recognition fills the gap.[36] Moreover, the efficiency and security are only as good as the technology used to read ePassports and its operational implementation. Heimo et al. suggested that information systems at border control might affect security without necessarily improving it—instead, risking a reduction in aviation

---

[28] Georgios Nouskalis, 'Biometrics, e-identity, and the balance between security and privacy: case study of the passenger name record (PNR) system' (2011) *The Scientific World Journal* 11, pg.476

[29] Charter of Fundamental Rights of the European Union, 2012/C 326/02, Article 7 (Respect for private and family life) and Article 8 (Protection of personal data)

[30] Case C-291/12, Michael Schwarz v Stadt Bochum [2013] ECLI:EU:C:2013:670

[31] See *supra* note 26

[32] Paramjit Kaur, Kewal Krishan, Suresh K. Sharma, and Tanuj Kanchan, 'Facial-recognition algorithms: A literature review' (2020) *Medicine, Science and the Law* 60.2, pg.132

[33] Alice Towler, James D. Dunn, Sergio Castro Martínez, Reuben Moreton, Fredrick Eklöf, Arnout Ruifrok, Richard I. Kemp, and David White, 'Diverse types of expertise in facial recognition' (2023) *Scientific reports* 13.1, pg.1

[34] Dominik Malčík and Martin Drahanský, 'Anatomy of biometric passports' (2012) *BioMed Research International* pg.3

[35] David Bolt, 'An Inspection of Border Force Operations at Stansted Airport' (*Independent Chief Inspector of Borders and Immigration GOV.UK*, March 2018) https://assets.publishing.service.gov.uk/media/ 5abb6b9540f0b67d64e21a1c/An_Inspection_of_Border_Force_Operations_at_Stansted_Airport.pdf pg. 31, accessed 2 September 2023

[36] Ziaul H. Choudhury and M. Munir A. Rabbani, 'Biometrics passport authentication using facial Marks' (2014) *Australian Journal of Basic and Applied Science* 8.16 pg.40

and border security.[37] This is evidenced in the number of incidents investigated in the United Kingdom (UK) where eGates failed on multiple occasions,[38] where the re-inspection of eGates highlighted several shortcomings in the system,[39] and where the Home Office probed eGates after a passenger reported a fault to the border control.[40] The current guidance also acknowledges eGates and microchip errors,[41] which put their reliability into question.

Furthermore, as FRT is a subset of AI, it poses a significant risk of bias[42] due to the inherent biases in the data on which AI algorithms have been trained. Studies show that face types have strong category associations which may promote stereotype-motivated recognition errors.[43] Schuetz therefore called for an adaptive legal framework governing FRT in the US.[44] In the EU, the AI Act is said[45] to be future proof and contains provisions aimed to prevent bias in AI training.[46] But bias is not the only problem with FRT. Schouten and Jacobs argued that biometric systems, on which the FRT relies, are not often designed with security and privacy in mind.[47] Therefore, legal frameworks such as the GDPR[48] and AI Act[49] play crucial role in this regard.

---

[37] Olli I. Heimo, Antti Hakkala, and Kai K. Kimppa, 'How to abuse biometric passport systems' (2012) *Journal of Information, Communication and Ethics in Society* 10.2 pg.77

[38] See e.g. Harry Taylor and Geneva Abdul, 'Travellers faced long queues at major UK airports after electronic passport gates failed' (*The Guardian*, 27 May 2023) https://www.theguardian.com/world/2023/may/27/electronic-passport-gate-fault-causes-long-delays-at-major-uk-airports-epassport-egate; and Ben Clatworthy, 'Passport e-gates at Heathrow fail for third time in three months' (*British Aviation Group*, 10 November 2021) https://www.britishaviationgroup.co.uk/news/passport-e-gates-at-heathrow-fail-for-third-time-in-three-months/ accessed 28 May 2023

[39] David Neal, 'A re-inspection of ePassport gates' (*Independent Chief Inspector of Borders and Immigration*, May 2023) https://assets.publishing.service.gov.uk/media/65e075ed2f2b3b001c7cd769/A_re-inspection_of_ePassport_gates_May_2023.pdf accessed 9 March 2024

[40] Katie Dickson, 'Home Office investigating after woman gets through Newcastle Airport e-gates with wrong passport' (*Chronicle Live,* 15 March 2019) https://www.chroniclelive.co.uk/news/north-east-news/newcastle-airport-passport-control-gates-15980063 accessed 9 March 2024—the delayed Home Office report on airport security is not yet available.

[41] Border Force, 'Guidance— Reasons you may not get through ePassport gates (eGates)' (*GOV.UK*, 7 March 2024) https://www.gov.uk/government/publications/coming-to-the-uk/reasons-you-may-not-get-through-epassport-gates-egates accessed 9 March 2024

[42] Peter N.K. Schuetz, 'Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework' (2021) *Law & Inequality* 39.221, pg.225

[43] Heather M. Kleider, Sarah E. Cavrak, and Leslie R. Knuycky, 'Looking like a criminal: Stereotypical black facial features promote face source memory error' (2012) *Memory & cognition* 40, pg.1200

[44] *Supra* note 41, at pg.254

[45] European Commission, 'Shaping Europe's digital future. AI Act' https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai accessed 10 March 2024

[46] EU AI Act, Article 10

[47] Ben Schouten and Bart Jacobs, 'Biometrics and their use in e-passports' (2009) *Image and Vision Computing* 27.3, pg.305

[48] *See* GDPR, Art. 25, Data protection by design and default

[49] *See* EU AI Act, Chapter 2, Prohibited AI practices

3. Analysis of paperless and seamless air travel examples

ICAO's objectives to ensure seamless travel and efficient passenger facilitation can only be achieved with a successful implementation of processes and technology which comply with applicable laws. An early prototype of a paperless international travel was planned to be trialled between Canada and the Netherlands in 2020. It intended to address the increasing demand for air travel which was expected to grow to 1.8 billion passengers by 2030.[50] The initiative known as Known Traveller Digital Identity (KTDI) focused on collaboration between various stakeholder and leveraging emerging technology, such as FRT, to streamline passenger facilitation while enhancing confidence in the security measures necessary in air travel. The intention was also to link KTDI with the national systems connected to the ICAO's PKD[51] and exploit the benefits of ePassports available in over 140 Member States.[52]

The KTDI initiative has become a casualty of the Covid-19 pandemic and no plans exist to revive it.[53] However, an alternative initiative—Digital Travel Credential (DTC-1) pilot has been launched with flights resuming between Canada and the Netherlands for travellers flying from Montreal to Amsterdam on KLM airlines.[54] Although it is anticipated that it will still be several years until they are formally introduced—there is no doubt that international paperless travel is the future direction and that this development will contribute to ICAO's objectives. Consequently, this section will analyse legal and regulatory considerations in cases where FRT is already used as a substitute or alternative to the traditional passport and security checks.

---

[50] Madeleine Hillyer, 'World Economic Forum Consortium Launches Paperless Canada-Netherlands Travel Pilot' (*World Economic Forum*, 26 June 2019) https://www.weforum.org/press/2019/06/world-economic-forum-consortium-launches-paperless-canada-netherlands-travel-pilot/; see also the report: 'The Known Traveller. Unlocking the potential of digital identity for secure and seamless travel' (WEF, January 2018) https://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf; and 'Known Traveller Digital Identity Specification Guidance' (*World Economic Forum and Accenture,* March 2020) https://www3.weforum.org/docs/WEF_KTDI_Specifications_Guidance_2020.pdf accessed 1 June 2023
[51] *Ibid*, pg.14; currently 96 Member States participate in ICAO PKD; ICAO, 'ICAO PKD Participants' https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx accessed 1 June 2023
[52] *Supra* note 22
[53] Chris Burt, 'No plans to revive World Economic Forum's user-controlled airport digital ID pilot' (*Biometric Update*, 7 October 2022) https://www.biometricupdate.com/202210/no-plans-to-revive-world-economic-forums-user-controlled-airport-digital-id-pilot 4 June 2023
[54] Bianca Gonzalez, 'Digital Travel Credential trials resume with flights from Netherlands to Canada' (*Biometric Update*, 4 March 2024) https://www.biometricupdate.com/202403/digital-travel-credential-trials-resume-with-flights-from-netherlands-to-canada accessed 16 March 2024

3.1. (The Republic of) India

The launch of DigiYatra[55] in 2022 by the India's Ministry of Civil Aviation, aiming to transform passenger experience, took airports in India by storm. Available at 13 airports, with further 14 to follow in due course, DigiYatra has been dubbed the airports' "Walk in the Park" offering a "seamless, hassle-free and health-risk free air travel."[56] This means that travellers can walk through the airport without queuing for their documents to be verified. Instead, biometric identification takes place with the use of FRT and the DigiYatra application. According to India's Ministry of Civil Aviation (MoCA), by the 10 August 2023 the technology was used by 3.46 million passengers.[57] Moreover, the DigiYatra Foundation, co-owned by the Airports Authority of India and private airports intends to align it with IATA's One ID for a global interoperability.[58] The MoCA states that there is no central storage of passengers' personal information, and that the information is encrypted and stored on travellers' smartphone. It further explains that the data is purged from airports' systems within 24 hours of the traveller's flight departure.

However, in a country in which no data protection legislation is yet in force,[59] questions have been raised over privacy, data security, and validity of consent in the use of DigiYatra.[60] Although, the application is said to be voluntary and data is collected with consent,[61] reports suggest that passengers are being enrolled to DigiYatra by airport security staff without consent[62] or are coerced into doing so.[63] A Member of Parliament published a response[64] from the MoCA to questions regarding involuntary enrolment, in which the MoCA insisted that the enrolment is

---

[55] Ministry of Civil Aviation, '"DigiYatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) https://www.civilaviation.gov.in/sites/default/files/2023-07/Digi%20Yatra%20Policy%20%28DIGI%20YATRA%29.pdf 18 June 2023

[56] DigiYatra Foundation, 'Re-imagining Airport Experiences, https://digiyatrafoundation.com/digi-yatra/ accessed 30 August 2023

[57] Ministry of Civil Aviation, 'DigiYatra to be launched at 6 more airports' (11 August 2023) pib.gov.in/PressReleaseIframePage.aspx accessed 30 August 2023

[58] Peden D. Bhutia, 'Future of Airports in India: DigiYatra for International Travel, Coming Soon', (*Skift*, 27 May 2024) https://skift.com/2024/05/27/future-of-airports-in-india-digiyatra-for-international-travel-coming-soon/ accessed 8 June 2024

[59] Information accurate at the time of writing—India's Digital Personal Data Protection Act 2023 was published and notified in the Official Gazette on the 11 August 2023, but it has not come into force yet.

[60] Sukriti, 'DigiYatra and the Defect in the Idea of 'Consent" (*Tech Policy*, 30 April 2024) https://www.techpolicy.press/digi-yatra-and-the-defect-in-the-idea-of-consent/ accessed 9 June 2024

[61] DigiYatra, 'DigiYatra Foundation (DYF) Privacy Policy' https://digiyatrafoundation.com/privacy-policy/ accessed 30 August 2023

[62] Jagriti Chandra, 'Centre's DigiYatra enrolment takes off as airport security staff sign up flyers without their consent' (*The Hindu*, 6 January 2024) https://www.thehindu.com/news/national/passengers-say-cisf-and-airport-staff-are-collecting-biometric-data-without-consent/article67710134.ece?ref=static.internetfreedom.in accessed 9 June 2024

[63] *Supra* note 60

[64] Saket Gokhale, 'VERY IMPORTANT: Regarding DigiYatra at airports' (*X*, 27 January 2024) https://x.com/SaketGokhale/status accessed 18 March 2024

voluntary and requires passengers' consent. Earlier, several posts on X[65] warned about structured collection of biometric data which also prompted a response on the platform from the MoCA reiterating that no data was collected centrally.[66] But sceptics argue that the lack of privacy laws and third-party access to the data remain a significant issue.[67]

Despite the reassurances, the legislative approach to protection of data and privacy in India is still an open question. While on the 11 August 2023 India published its Digital Personal Data Protection Act 2023,[68] the law has not yet come into force. Moreover, while the previous iterations of the Bill[69] alluded to special treatment of sensitive personal data such as localisation[70], undertaking a Data Protection Impact Assessment,[71] defining[72] and listing biometric data as sensitive data,[73] as well as limits on processing of certain forms of biometric data,[74] these provisions no longer exist in the finalised Act. This means that the legislation now treats all data in the same way without any special treatment or additional safeguards to data of particularly sensitive nature, such as biometrics.

While the right to privacy has been confirmed by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v Union of India*,[75] India's blanket approach to facial recognition is a controversial issue. In 2019, the National Crime Records Bureau (NCRB) issued a Request for Proposal for an Automated Facial Recognition System (AFRS).[76] Although the purpose of this system will be to identify criminals or missing people, growing concerns are being raised over mass surveillance. Similarly, India's national programme, Aadhaar, which provides individuals with a unique number linking demographic and biometric information was also alleged to be a

---

[65] Formerly Twitter platform

[66] Ankita Chakravarti, 'DigiYatra passengers' data stored on their own device not in central storage, govt says' (*India Today*, 18 March 2023) https://www.indiatoday.in/technology/news/story/digiyatra-passengers-data-stored-on-their-own-device-not-in-centralised-storage-govt-says-2348388-2023-03-18 accessed 30 August 2023

[67] Rizwan Hera, 'DigiYatra: Experts Flag Privacy Concerns Over the Facial Recognition App' (*Boom*, 21 March 2023) https://www.boomlive.in/explainers/digiyatra-air-travel-eased-face-recognition-privacy-breached-civil-aviation-jyotiraditya-scindia21396 accessed 30 August 2023

[68] Publication of the Digital Personal Data Protection Act 2023 (No.22 of 2023) in the Gazette of India https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[69] India's Digital Personal Data Protection Act has undergone a number of changes, *see* here: insideprivacy.com/wp-content/uploads/sites/51/2019/12/India-Personal-Data-Protection-Bill-2019-Redline-of-Changes-2.pdf for the redline of the previous India Personal Data Protection Bill 2019

[70] *Ibid.*, Chapter VII, S.33 and 34

[71] *Ibid.*, Chapter VI, S.27

[72] *Ibid.*, Chapter I, S.3(7)

[73] *Ibid.*, Chapter I, S.3(35)

[74] *Ibid.*, Chapter XIV, S.92

[75] *Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161*

[76] Anushka Jain, 'NCRB's National Automated Facial Recognition System' (*Panoptic Tracker*, 5 May 2024) https://panoptic.in/about accessed 8 June 2024

form of surveillance.[77] Although theoretically voluntary, the Aadhaar Act[78] brought on the reliance on it for access to benefits and services, making it mandatory.[79]

Aadhaar number is necessary for DigiYatra enrolment, as e-Passports are not yet available in India. Therefore, together with Aadhaar number, the possibility of AFRS, and a lack of data protection laws governing the use of the data, activists are cautioning travellers about the use of DigiYatra.[80] The rollout of DigiYatra has been presented at the 15th TRIP Symposium as a form of shortening passenger processing times at airports using biometric data,[81] and although it is planned to be open to international travellers,[82] the ongoing concerns over privacy and security of data[83] may have a significant impact on the continued success of its rollout.

3.2. The Unites States (US) of America

Despite privacy concerns, India's DigiYatra initiative achieved substantial enrolment to date. However, it was the US that was the forerunner in the use of FRT and biometrics in aviation. Rather than convenience of hassle-free travel, the primary driver for the implementation of FRT in the US was to enhance security in response to the 9/11 events.[84] Currently, the country boasts 238 airports that utilise Biometric Facial Comparison Technology.[85]

In the US, the FRT at airports is governed by a combination of federal laws, regulations, and guidelines, including the Aviation and Transportation Security Act[86] which established the Transportation Security Administration (TSA) instructing it to use biometric screening technologies for security checks, Customs and Border Protection operating under the Department of Homeland Security, Consolidated Appropriations Act of 2016[87] which provided

---

[77] Kalyani S. Menon, 'Aadhar: Wrong Number, or Big Brother Calling?' (2015) *Socio-Legal Review* 11.2, pg.105; see also: Pawan Singh, 'Aadhaar and data privacy: biometric identification and anxieties of recognition in India' (2021) *Information, Communication & Society*, 24.7 pg.999

[78] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

[79] Sai A Yalavarthy, 'Aadhaar: India's National Identification System and Consent-Based Privacy Rights' (2023) *Vanderbilt Journal of Transnational Law* 56, pg.624-674

[80] Disha Verma, 'Resist Surveillance Tech, Reject DigiYatra' (*Internet Freedom Foundation*, 16 January 2024) https://internetfreedom.in/reject-digiyatra/ accessed 13 June 2024

[81] ICAO, 'Presentations and Biographies' [Hareendranathan E.P, Executive Director, Indian Aviation Academy, New-Delhi] (28 June 2019) https://www.icao.int/Meetings/TRIP-Symposium-2019/Pages/Presentations.aspx accessed 13 June 2024

[82] Dev Kachari, 'DigiYatra to open up for international travel, accept passport as an ID' (*Infra/Economic Times*, 29 December 2023) https://infra.economictimes.indiatimes.com/news/aviation/digi-yatra-to-open-up-for-international-travel-accept-passport-as-an-id/106378139 accessed 7 January 2024

[83] Shaji A. George, S. Sagayarajan, T. Baskar and Digvijay Pandey, 'From Paperwork to Biometrics: Assessing the Digitization of Air Travel in India through DigiYatra' (2023) *Partners Universal International Innovation Journal* 1.4, pg.118

[84] *Supra* note 26

[85] U.S. Customs and Border Protection, 'Airports | CBP Biometrics' (30 January 2024) https://www.cbp.gov/travel/biometrics/airports accessed 23 March 2024

[86] Aviation and Transportation Security Act of 2001 (Public Law 107-71—Sept.19, 2001)

[87] Consolidated Appropriations Act of 2016 (Public Law 114-113—Dec.18, 2015), Sec.411.

funding and legislative support for the development of the biometric entry-exit system, and Intelligence Reform and Terrorism Prevention Act of 2004[88] which mandated the development of this technology to improve national security. NIST, although not mandatory, also offers digital identity guidelines which emphasize the importance of securing biometric data to protect individual privacy.[89]

The Transport Security Administration (TSA) uses FRT to enhance identity verification and security. Its proposed expanded rollout[90] triggered a letter to the Congress from 14 Senators criticising TSA's plans as a threat to privacy and civil liberties.[91] Additionally, the US also boasts a range of Trusted Traveller Programs for those who want to get through the airport quickly. These include TSA PreCheck[92] for US citizens, Global Entry[93] for international travellers, or available with some airlines—private program, Clear.[94] These programs are voluntary, paid services, which utilise biometric data for identity verification. Paradoxically, reports suggest that as many as 18m[95] passengers have enrolled for the TSA PreCheck and 17m for Clear,[96] only to find they have become so popular that the use of free security check lanes has become so rare—it became faster than the paid services.[97]

In comparison with India, the US has made some progress in respect of implementation of privacy laws, but they still resemble a patchwork approach. The country lacks a comprehensive federal privacy regime. The Privacy Act of 1974 is both outdated and limited to federal agencies, and the residual laws are either state-based[98] or sector-specific.[99] While some states have made progress introducing laws covering the processing of biometrics,[100] the approach remains fragmented.

---

[88] Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458—Dec.17, 2004), Sec.7208

[89] National Institute of Standards and Technology, NIST Special Publication 800-63-3: Digital Identity Guidelines (*U.S. Department of Commerce*, 2017) https://pages.nist.gov/800-63-4/ accessed 31 August 2023

[90] David Pekoske, 'TSA Biometrics Strategy. For Aviation Security & the Passenger Experience' (*Transportation Security Administration*, July 2018) https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf accessed 25 August 2023

[91] Copy of the letter dated 2 May 2024, is available here: https://www.merkley.senate.gov/wp-content/uploads/2024_05_02_LTR-TSA-Freeze-to-Leadership.pdf accessed 2 June 2024

[92] TSA PreCheck, https://www.tsa.gov/precheck accessed 25 August 2023

[93] U.S. Customs and Border Protection, 'Global Entry. Trusted Traveler Program Enrollment' (25 October 2023) https://www.cbp.gov/travel/trusted-traveler-programs/global-entry accessed 26 August 2023

[94] Clear, https://www.clearme.com/ accessed 26 August 2023

[95] Nathaniel Meyersohn, 'The newest pain point in air travel is slowing down travelers who paid for convenience' (*CNN Travel*, 22 December 2023) https://edition.cnn.com/2023/12/22/travel/tsa-precheck-clear-airport-security accessed 7 January 2024

[96] Clear, 'RESERVE powered by CLEAR Hits Major Milestone of 5 Million Reservations' (*Clear*, 29 August 2023) https://ir.clearme.com/news-events/press-releases/detail/81/reserve-powered-by-clear-hits-major-milestone-of-5-million accessed 30 August 2023

[97] *Supra* note 95

[98] *See* e.g. California Consumer Privacy Act (CCPA)

[99] *See* e.g. Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191—Aug.21,1996)

[100] *See* e.g. Illinois Biometric Information Privacy Act (BIPA)

Moreover, unlike non-US citizens, the US citizens can opt-out of the biometric processing at US airports. This is pertaining to the Fourth Amendment[101] right which prohibits unreasonable searches, and following *Katz v United States*,[102] the Supreme Court confirmed that the protection included the intrusion of privacy. However, similarly to India, reports suggest that passengers are discouraged from opting out, either because it will cause delays[103] or because travellers are not informed about how to do it.[104] Issues also arise in relation to the retention of data, as the biometric data of the US citizens is deleted after 12 hours, while the non-US citizens is retained for up to 75 years.[105] This retention period also created friction in respect of PNR data exchange, discussed earlier.[106]

While there is no doubt that thorough airport checks serve greater public interest, concerns continue over growing utilisation of AI which is not always accurate, may lead to bias,[107] and facilitation of surveillance and social control.[108] Just like in India, due to a lack of specific guidance and laws ensuring transparency, there is a growing activism in the US against the use of FRT at airports.[109]

3.3. The European Union (EU)

Compared with the two examples so far, the EU's uniqueness is in its union of 27 independent European countries, most of which are party to the Schengen Agreement.[110] In a stark contrast to India and the US, the EU boasts a robust privacy and data protection framework. GDPR's success in particular can be seen in many non-European countries replicating and adopting

---

[101] US Constitution, Amendment IV

[102] Katz v. United States, 389 U.S. 347 (1967)

[103] Shira Ovide, 'You can say no to a TSA face scan. But even a senator had trouble' (*The Washington Post*, 11 June 2023) https://www.washingtonpost.com/technology/2023/07/11/tsa-airport-security-facial-recognition/ accessed 26 August 2023

[104] Allie Funk, 'I Opted Out of Facial Recognition at the Airport—It Wasn't Easy' (*Wired*, 2 July 2019) https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/ accessed 26 August 2023

[105] Congressional Research Focus, 'Biometric Entry-Exit System: Legislative History and Status' (*In Focus*, 27 August 2020) https://sgp.fas.org/crs/misc/IF11634.pdf accessed 31 August 2023

[106] See s*upra* note 18

[107] *Supra* note 41

[108] Daniel J. Solove, 'Artificial Intelligence and Privacy' (24 April 2024) *77 Florida Law Review* (forthcoming 2025), pg.50

[109] Merve Hickok and Evanna Hu, 'Don't Let Governments Buy AI Systems That Ignore Human Rights: Even in the absence of broader AI regulation, federal procurement provisions could set expectations for data quality, model performance, risk assessments, and documentation' (2024) *Issues in Science & Technology*, 40.3; *see* also: Jeramie D. Scott, 'Don't Take It at Face Value: Why TSA's Implementation of Facial Recognition is More Dangerous Than You Think' (*Epic*, 30 June 2023) https://epic.org/dont-take-it-at-face-value-why-tsas-implementation-of-facial-recognition-is-more-dangerous-than-you-think/ accessed 2 June 2024

[110] Schengen Agreement is a treaty which created Schengen Area where border controls have largely been removed enabling freedom of movement of people, goods and services between the signatory countries. Ireland and Cyprus are the only EU member states not party to the Agreement, but other European non-EU states (Iceland, Norway, Switzerland) have signed up to the Schengen Agreement.

similar, GDPR-like, data protection regimes.[111] The regulation ensures that biometric data[112]—when used to identify individuals, is considered special category of personal data, processing of which is prohibited unless conditions in Article 9 are met.[113] Just like in India and the US, activists warn against mass surveillance.[114] However, under Article 5,[115] the EU AI Act specifically prohibits or imposes requirements for certain AI practices, such as the use of 'real-time' remote biometric identification in public spaces for the purposes of law enforcement (subject to few exceptions)[116] and principally prohibits AI facial recognition for mass surveillance.[117] In the Act, publicly accessible spaces refer to any physical space that is accessible to any undetermined number of individuals, regardless of private or public ownership or the activity conducted there—this includes airports.[118]

In May 2024, the European Data Protection Board (EDPB)—an independent body which ensures consistent application of the GDPR, issued an opinion on the use of FRT at airports.[119] The EDPB addressed four specific scenarios in relation to the storage (under Articles 5(1)(f), 25 and 32 of the GDPR)[120] of biometrics obtained in the course of security checkpoints, baggage drop-off, boarding, and access to the passenger lounge—aspects of travel which make the journey more efficient and convenient, rather than necessitate the checks for the border control purposes. In that respect the EDPB concluded that for the processing to be compatible with GDPR, the biometric data should be stored on passengers' devices under their sole control or alternatively that the biometrics could be stored in a centralised storge, within the airport, but encrypted with the encryption key solely in the passenger's control. On site or cloud storage where the encryption key is in the control of the airport would not be considered compatible with the GDPR, considering that alternative options exist. This is because, storage of biometric templates carries a heightened risk as, unlike passwords, it cannot be changed if stolen or misused.

---

[111] e.g. The Personal Data Protection Act 2019 ('PDPA') in Thailand or General Personal Data Protection Law ('LGPD') in Brazil are just couple of examples.

[112] GDPR, Article 4(14) defines 'biometric data' as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

[113] GDPR, Article 9. Processing of special categories of personal data

[114] European Data Rights, 'How to fight Biometric Mass Surveillance after the AI Act: A legal and practical guide' (*EDRi*, 27 May 2024) https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/ accessed 8 June 2024

[115] EU AI Act, Article 5. Prohibited Artificial Intelligence Practices

[116] *Ibid*, Article 5.1(h), 5.2, and 5.3

[117] *Ibid,* Recital 43

[118] *Ibid,* Recital 19

[119] Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR

[120] Art.5(1)(f) – integrity and confidentiality, (f) - storage limitation; Art.25 - Data protection by design and by default; Art.32 - Security of processing

Aside from the opinion on storage, the EDPB also commented on other aspects, such as acknowledging that to use biometrics for security checkpoints, baggage drop-off, boarding, and access to the passenger lounge requires explicit consent.[121] Such consent must be freely given and must be "without any detriment (such as significantly longer delays for passengers who do not consent)."[122] The existence of robust data protection laws and specific guidance on processing data that can be called upon, is a sharp contrast between the EU and the approach in the US or India, where allegations emerged that individuals were enrolled without consent or that were unable to opt-out from the use of FRT.

The EDPB acknowledged that the use of biometrics and FRT by airport operators and airline companies streamlines the passenger flow at airports. This means that while such processing carries risks, it may be beneficial for an efficient passenger facilitation and a seamless travel experience, but that implementation of such systems must be compatible with relevant laws to ensure both privacy and protection of passengers' personal data.

The EU also has a number of initiatives aiming to improve passenger facilitation at airports. Specifically, plans exist to replace paper documents with a Digital Identity Wallet.[123] This wallet would hold various documents including a passport, in an electronic format and would contain biometric data. The wallet would be interoperable in the EU and efforts are being made to negotiate its acceptability outside of the EU and the Schengen Area.[124] To achieve that, the EU is specifically looking towards ICAO's Digital Travel Credentials (DTC)[125] based on Document 9303[126] to ensure international interoperability of travel documents. Additionally, Croatia, Finland, and the Netherlands are already trailing the DTC system, while two airports in Italy, Milano Linate and Catania, are trailing 'FaceBoarding'[127]—a system where enrolled passengers will be able to travel without showing the physical or digital documents. In a similar fashion to the US, the new EU Entry Exit System (EES)[128] will require non-EU visitors to

---

[121] GDPR, Article 9.2(a)

[122] *Supra* note 119, pg.11

[123] EU Digital Identity Wallet, 'What is the EU Digital Identity Wallet' (*European Commission*) https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+wallet accessed 16 June 2024

[124] Jeremy Springall, 'Biometrics and the future of travel beyond the airport' [Panel discussion] (*International Airport Review*, 14 June 2024) https://www.internationalairportreview.com/video/222629/biometrics-and-the-future-of-travel-beyond-the-airport/ accessed 16 June 2024

[125] ICAO, 'Guiding Core Principles for the Development of Digital Travel Credential (DTC)' (*ICAO*, July 2023) https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/ICAO%20GUIDING%20CORE%20PRINCIPLES%20DTC_Draft%20v4.8.pdf accessed 12 August 2023

[126] See *Supra* note 2

[127] Liv Kelly, 'These European airports are trialling a new passport-free boarding process' (*TimeOut*, 16 May 2024) https://www.timeout.com/news/these-european-airports-are-trialling-a-new-passport-free-boarding-process-051624 accessed 15 June 2024

[128] European Commission, 'Entry/Exit System (EES)' https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en accessed 15 June 2024

subject themselves to collection of biometrics upon arrival. All of these initiatives rely on utilisation of biometrics and FRT. Therefore, it is reasonable to say that there is an obvious increasing momentum towards digital credentials which will enable seamless, secure, and efficient travel.

4. Discussion

Growing demand for air travel necessitates measures to enhance efficiency of passenger facilitation without compromising security. Technological advancements enable this through the use of biometrics, FRT, and digitalisation of documents. However, an ongoing concern over privacy and data protection remains. The examples of India, the US, and the EU illustrate different approaches in implementation of privacy and data protection laws, and as a result, the utilisation of biometrics and FRT. The EU boasts comprehensive laws that protect individuals' rights, while India and the US[129] have been making only incremental progress. However, the fast technological developments necessitate urgent legal frameworks. The differences in approaches to privacy have previously caused disruption (e.g. PNR) and are likely to continue with FRT and biometric data processing, over fears of mass surveillance. This may hinder ICAO's objective of seamless travel experience and efficient passenger facilitation.

The approach to sharing biometrics appears to be evolving among passengers. In 2018, the KTDI report acknowledged that individuals tend to be sceptical about sharing their personal data with authorities, but also emphasised that advance and seamless provision of biometric data will expedite security, contribute to safety, and make their journey more efficient.[130] Subsequently, the 2023 IATA's survey[131] shows that speed and convenience of getting through the airport are top priorities for passengers and that they are embracing the use of biometrics to expedite their journey. Professor Daniel J. Solove critiqued the concept of 'privacy paradox'[132]—a theory which suggests that people tend to claim they value privacy but are willing to trade it for goods and services. On the surface, IATA's survey seems to corroborate the theory suggesting that passengers are indeed willing to trade their data for speed and convenience of getting through the airport. But the 2023 SITA survey[133] offers further insight.

---

[129] On the 7 April 2024 Sen. Maria Cantwell and U.S. Rep. Cathy McMorris Rodgers proposed the American Privacy Rights Act (APRA) aiming to remedy the existing patchwork of US privacy laws. This is a second attempt as the previously proposed comprehensive privacy bill American Data Privacy Protection Act (ADPPA) introduced in previous congressional sessions did not advance to become law. *See*: draft available at: www.commerce.senate.gov/services/files/3F5EEA76-5B18-4B40-ABD9-F2F681AA965F accessed 1 June 2024

[130] *Supra* note 50, at pg.22

[131] *Supra* note 23

[132] Daniel J. Solove, 'The Myth of the Privacy Paradox' (2021) *George Washington Law Review* 89.1, pg.2

[133] SITA, '2023 Passenger IT Insights' https://www.sita.aero/globalassets/docs/surveys--reports/passenger-it-insights-2023.pdf accessed 31 May 2024, pg. 9

Specifically, passengers are increasingly more comfortable using their biometric data if it improves travel experience—but that they are more comfortable when it is used for boarding, security, and identity verification and less so for check-in, bag drop, and lounge access. This suggests that travellers are selective as to how they share their data, confirming Solove's theory that people make decisions about risk in a specific context. Privacy laws can be catalytic in enabling passengers such selective choice and in the absence of such laws, guidelines would not go amiss. This is where the role of ICAO is paramount.

ICAO considers year 2024 to be the Year of Facilitation (FAL2024).[134] With its TRIP strategy and aim to foster a comprehensive global approach to traveller identity, ICAO is best placed to develop guidelines for the processing of biometric data and the use of FRT in aviation. Such guidelines would complement the existing ones, such as PNR and API, ensure international consistency in light of fragmented privacy laws worldwide, and support the objective of efficient passenger facilitation and seamless travel experience.

5. Conclusion

This article considered the legal and regulatory landscape of paperless travel. In light of an ever-increasing number of air passengers, seamless travel experience and efficient passenger facilitation are necessary for a hassle-free and secure international travel. While the technology that enables paperless travel already exists, the implementation differs between the Member States. While India's primary focus is on efficiency, in the US the main priority is security, albeit both countries consider the other aspect a benefit. The European Schengen Area allows passport-less travel within its boundaries, but the EU's EES systems for non-EU nationals will make collection of biometric data compulsory. In addition, number of EU countries are also trailing 'FaceBoarding' possibly removing the need for documents in the future altogether.

The importance of privacy cannot be underestimated. Surveys show that privacy and data protection are essential and will remain a concern for passengers until transparent rules are applied globally and consistently. The establishment of guidelines such as PNR by ICAO triggered a development of legislations in various Member States. This shows that, while approaches to privacy differ globally, ICAO can be influential in prompting a roll out of suitable rules that will provide confidence to passengers and accelerate progress to achieving ICAO's objective of seamless travel experience and efficient passenger facilitation.

---

[134] ICAO, 'ICAO'S Traveller Identification Programme (TRIP) Strategy: A critical enabler of Global Air Transport Facilitation' https://www.icao.int/Security/FAL2024/Documents/Flyers/TRIP-and-Year-of-Facilitation.pdf accessed 20 June 2024

6. Bibliography

Primary Sources

Case Law

Case C-291/12, Michael Schwarz v Stadt Bochum [2013] ECLI:EU:C:2013:670

Katz v. United States, 389 U.S. 347 (1967)

Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161

Legislation

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016

Aviation and Transportation Security Act of 2001 (Public Law 107-71—Sept.19, 2001)

California Consumer Privacy Act (CCPA)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985) ETS 108 ("Convention 108")

Convention on International Civil Aviation 1944

Consolidated Appropriations Act of 2016 (Public Law 114-113—Dec.18, 2015)

Constitution of the United States 1789

Charter of Fundamental Rights of the European Union, 2012/C 326/02

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132

Digital Personal Data Protection (DPDP) Act (2023) of India

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191—Aug.21, 1996)

Illinois Biometric Information Privacy Act (BIPA)

Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458—Dec.17, 2004)

Lei Geral de Proteção de Dados (General Personal Data Protection Law ('LGPD') in Brazil)

Personal Data Protection Act B.E. 2562 (2019) of Thailand (PDPA)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ L119/1

Regulation (EC) 2252/2004 - Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) OJ 2024/1689

Draft Legislation

American Privacy Rights Act (APRA), 118th Congress 2d Session; draft available online at: www.commerce.senate.gov/services/files/3F5EEA76-5B18-4B40-ABD9-F2F681AA965F accessed 1 June 2024

EU Opinions

Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)

Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries

Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR

Opinion 1/15 of the Court (Grand Chamber) pursuant to Article 218(11) TFEU — Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data from the European Union to Canada — Appropriate legal bases — Article 16(2), point (d) of the second subparagraph of Article 82(1) and Article 87(2)(a) TFEU — Compatibility with Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union

Aviation, international organisations, and country specific publications and guidelines

Border Force, 'Guidance— Reasons you may not get through ePassport gates (eGates)' (*GOV.UK*, 7 March 2024) https://www.gov.uk/government/publications/coming-to-the-uk/reasons-you-may-not-get-through-epassport-gates-egates accessed 9 March 2024

Bolt D, 'An Inspection of Border Force Operations at Stansted Airport' (*Independent Chief Inspector of Borders and Immigration GOV.UK*, March 2018) https://assets.publishing.service.gov.uk/media/5abb6b9540f0b67d64e21a1c/An_Inspection_of_Border_Force_Operations_at_Stansted_Airport.pdf accessed 2 September 2023

Clear, https://www.clearme.com/ accessed 26 August 2023

DigiYatra, 'DigiYatra Foundation (DYF) Privacy Policy' https://digiyatrafoundation.com/privacy-policy/ accessed 30 August 2023

DigiYatra Foundation, 'Re-imagining Airport Experiences, https://digiyatrafoundation.com/digi-yatra/ accessed 30 August 2023

EUROCONTROL, 'The FLY AI Report. Demystifying and Accelerating AI in Aviation/ATM' online at: https://www.eurocontrol.int/publication/fly-ai-report accessed 12 April 2023

European Commission, 'Entry/Exit System (EES)' https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en accessed 15 June 2024

European Commission, 'Shaping Europe's digital future. AI Act' https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai accessed 10 March 2024

European Parliament, 'EU AI Act: first regulation on artificial intelligence' (19 December 2023) https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence accessed 27 December 2023

EU Digital Identity Wallet, 'What is the EU Digital Identity Wallet' (*European Commission*) https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+wallet accessed 16 June 2024

Hillyer M, 'World Economic Forum Consortium Launches Paperless Canada-Netherlands Travel Pilot' (*World Economic Forum*, 26 June 2019) https://www.weforum.org/press/2019/06/world-economic-forum-consortium-launches-paperless-canada-netherlands-travel-pilot/ accessed 1 June 2023

IATA, 'Global Passenger Survey 2023 Highlights', online at: https://go.updates.iata.org/GPS-Highlights-2023 accessed 9 June 2023

IATA, 'One ID', online at: https://www.iata.org/en/programs/passenger/one-id/ accessed 3 June 2023

IATA, 'Speed and Convenience Top Priority for Passengers', online at: https://www.iata.org/en/pressroom/2023-releases/2023-10-25-01/ accessed 9 June 2023

ICAO, 'Guidelines on Advance Passenger Information (API)', online at: https://www.icao.int/Security/FAL/Documents/API%20Guidelines.EN.June2022.pdf accessed 1 June 2023

ICAO, 'Doc 9303 Machine Readable Travel Documents', online at: https://www.icao.int/publications/pages/publication.aspx?docnum=9303 accessed 1 June 2023

ICAO, 'Doc 9944 Guidelines on Passenger Name Record (PNR) Data', online at: https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf accessed 3 June 2023

ICAO, 'ePassports Basics', online at: https://www.icao.int/Security/FAL/PKD/Pages/ePassport-Basics.aspx, accessed 3 June 2023

ICAO, 'Guiding Core Principles for the Development of Digital Travel Credential (DTC)' (*ICAO*, July 2023) https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/ICAO%20GUIDING%20CORE%20PRINCIPLES%20DTC_Draft%20v4.8.pdf accessed 12 August 2023

ICAO, 'ICAO PKD', online at: https://www.icao.int/Security/FAL/PKD/Pages/default.aspx accessed 1 June 2023

ICAO, 'ICAO PKD Participants' online at: https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx accessed 1 June 2023

ICAO, 'Presentations and Biographies' [Hareendranathan E.P, Executive Director, Indian Aviation Academy, New-Delhi] (28 June 2019) https://www.icao.int/Meetings/TRIP-Symposium-2019/Pages/Presentations.aspx accessed 13 June 2024

ICAO, 'Strategic Objectives', online at: https://www.icao.int/about-icao/Council/Pages/Strategic-Objectives.aspx accessed 1 June 2023

ICAO, 'Traveller Identification Programme. ID Management Solutions for More Secure Travel Documents', online at: https://www.icao.int/security/FAL/TRIP/Pages/default.aspx accessed 1 June 2023

ICAO, 'ICAO'S Traveller Identification Programme (TRIP) Strategy: A critical enabler of Global Air Transport Facilitation' https://www.icao.int/Security/FAL2024/Documents/Flyers/TRIP-and-Year-of-Facilitation.pdf accessed 20 June 2024

Ministry of Civil Aviation, '"DigiYatra Biometric Boarding System" Reimagining Air Travel in India' (4 March 2021) https://www.civilaviation.gov.in/sites/default/files/2023-07/Digi%20Yatra%20Policy%20%28DIGI%20YATRA%29.pdf accessed 18 June 2023

Ministry of Civil Aviation, 'DigiYatra to be launched at 6 more airports' (11 August 2023) pib.gov.in/PressReleaseIframePage.aspx accessed 30 August 2023

Neal D, 'A re-inspection of ePassport gates' (*Independent Chief Inspector of Borders and Immigration*, May 2023) https://assets.publishing.service.gov.uk/media/65e075ed2f2b3b001c7cd769/A_re-inspection_of_ePassport_gates_May_2023.pdf accessed 9 March 2024

National Institute of Standards and Technology, NIST Special Publication 800-63-3: Digital Identity Guidelines (*U.S. Department of Commerce*, 2017) https://pages.nist.gov/800-63-4/ accessed 31 August 2023

No Author, 'Known Traveller Digital Identity Specification Guidance' (*World Economic Forum and Accenture,* March 2020) https://www3.weforum.org/docs/WEF_KTDI_Specifications_Guidance_2020.pdf accessed 1 June 2023

No Author, 'The Known Traveller. Unlocking the potential of digital identity for secure and seamless travel' (WEF, January 2018) https://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf accessed 1 June 2023

OECD, 'Biometric-based Technologies' (2004) *OECD Digital Economy Papers*, No.101, OECD Publishing, Paris https://www.oecd-ilibrary.org/science-and-technology/biometric-based-technologies_232075642747 accessed 12 April 2023

Pekoske D, 'TSA Biometrics Strategy. For Aviation Security & the Passenger Experience' (*Transportation Security Administration*, July 2018) https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf accessed 25 August 2023

TSA PreCheck, https://www.tsa.gov/precheck accessed 25 August 2023

UNWTO, 'World Tourism Barometer and Statistical Annex' (*eLibrary,* January 2023) https://www.e-unwto.org/doi/abs/10.18111/wtobarometereng.2023.21.1.1 accessed 23 December 2023

U.S. Customs and Border Protection, 'Airports | CBP Biometrics' (30 January 2024) https://www.cbp.gov/travel/biometrics/airports accessed 23 March 2024

U.S. Customs and Border Protection, 'Global Entry. Trusted Traveler Program Enrollment' (25 October 2023) https://www.cbp.gov/travel/trusted-traveler-programs/global-entry accessed 26 August 2023

Secondary Sources

Books

Abeyratne R, 'Traveller Identity' in *Legal Priorities in Air Transport* (Springer 2019), 251-269

Solove DJ, 'Nothing to Hide. The False Tradeoff between Privacy and Security' (Yale University Press 2011)

Journal articles

Aus JP, 'Decision-making under pressure: The negotiation of the biometric passports regulation in the Council' (2006) *Arena* 11, 1-54

Carpanelli E and Lazzerini N, 'PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU' (2017) *Air and Space Law* 42.4/5, 377-402

Choudhury ZH, 'Biometrics passport authentication using facial marks' (2014) *Australian Journal of Basic and Applied Science* 8.16, 40-47

George SA, Sagayarajan S, Baskar B, and Pandey D, 'From Paperwork to Biometrics: Assessing the Digitization of Air Travel in India through Digi Yatra' (2023) *Partners Universal International Innovation Journal* 1.4, 110-125

Heimo OI, Hakkala A, and Kimppa KK, 'How to abuse biometric passport systems' (2012) *Journal of Information, Communication and Ethics in Society* 10.2, 68-81

Merve Hickok and Evanna Hu, 'Don't Let Governments Buy AI Systems That Ignore Human Rights: Even in the absence of broader AI regulation, federal procurement provisions could set expectations for data quality, model performance, risk assessments, and documentation' (2024) *Issues in Science & Technology*, 40.3, 37-41

Kaur P, Krishan K, Sharma SK, and Kanchan T, 'Facial-recognition algorithms: A literature review' (2020) *Medicine, Science and the Law* 60.2, 131-139

Kleider HM, Cavrak SE, and Knuycky LR, 'Looking like a criminal: Stereotypical black facial features promote face source memory error' (2012) *Memory & cognition* 40, 1200-1213

Dominik Malčík and Martin Drahanský, 'Anatomy of biometric passports' (2012) *BioMed Research International*, 1-8

Menon KS, 'Aadhar: Wrong Number, or Big Brother Calling?' (2015) *Socio-Legal Review* 11.2, 85-108

Morschbach F, 'Third Country PNR Mechanisms After the CJEU's Schrems II Judgment' (2023) *Air and Space Law* 48.1, 91-112

Nouskalis G, 'Biometrics, e-identity, and the balance between security and privacy: case study of the passenger name record (PNR) system' (2011) *The Scientific World Journal* 11, 474-477

Jeramie D. Scott, 'Don't Take It at Face Value: Why TSA's Implementation of Facial Recognition is More Dangerous Than You Think' (*Epic*, 30 June 2023) https://epic.org/dont-take-it-at-face-value-why-tsas-implementation-of-facial-recognition-is-more-dangerous-than-you-think/ accessed 2 June 2024

Schouten B and Jacobs B, 'Biometrics and their use in e-passports' (2009) *Image and Vision Computing* 27.3, pg. 305-312

Schuetz PNK, 'Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework' (2021) *Law & Inequality* 39.221, 221-254

Singh P, 'Aadhaar and data privacy: biometric identification and anxieties of recognition in India' (2021) *Information, Communication & Society*, 24.7, 978-993

Solove DJ, 'Artificial Intelligence and Privacy' (24 April 2024) *77 Florida Law Review* (forthcoming 2025)

Solove DJ, 'The myth of the privacy paradox' (2021) *George Washington Law Review*, 89.1, 1-52

Towler A, Dunn JD, Martínez SC, Moreton R, Eklöf F, Ruifrok A, Kemp RI, and White D, 'Diverse types of expertise in facial recognition' (2023) *Scientific reports* 13.1, 11396

Vedaschi A, 'Privacy and data protection versus national security in transnational flights: the EU–Canada PNR agreement' (2018) *International Data Privacy Law*, 8.2, 124-139

Woodard Jr, JD, 'Biometrics: Facing up to terrorism' (2001) *Rand Arroyo Center*, 1-3

Yalavarthy SA, 'Aadhaar: India's National Identification System and Consent-Based Privacy Rights' (2023) *Vanderbilt Journal of Transnational Law* 56, pg.624-674

Online sources

Bhutia PD, 'Future of Airports in India: DigiYatra for International Travel, Coming Soon', (*Skift*, 27 May 2024) https://skift.com/2024/05/27/future-of-airports-in-india-digiyatra-for-international-travel-coming-soon/ accessed 8 June 2024

Burt C, 'No plans to revive World Economic Forum's user-controlled airport digital ID pilot' (*Biometric Update*, 7 October 2022) https://www.biometricupdate.com/202210/no-plans-to-revive-world-economic-forums-user-controlled-airport-digital-id-pilot accessed 4 June 2023

Chakravarti A, 'DigiYatra passengers' data stored on their own device not in central storage, govt says' (*India Today*, 18 March 2023) https://www.indiatoday.in/technology/news/story/digiyatra-passengers-data-stored-on-their-own-device-not-in-centralised-storage-govt-says-2348388-2023-03-18 accessed 30 August 2023

Chandra J, 'Centre's DigiYatra enrolment takes off as airport security staff sign up flyers without their consent' (*The Hindu*, 6 January 2024) https://www.thehindu.com/news/national/passengers-say-cisf-and-airport-staff-are-collecting-biometric-data-without-consent/article67710134.ece?ref=static.internetfreedom.in accessed 9 June 2024

Clatworthy B, 'Passport e-gates at Heathrow fail for third time in three months' (*British Aviation Group*, 10 November 2021) https://www.britishaviationgroup.co.uk/news/passport-e-gates-at-heathrow-fail-for-third-time-in-three-months/ accessed 28 May 2023

Clear, 'RESERVE powered by CLEAR Hits Major Milestone of 5 Million Reservations' (*Clear*, 29 August 2023) https://ir.clearme.com/news-events/press-releases/detail/81/reserve-powered-by-clear-hits-major-milestone-of-5-million accessed 30 August 2023

Congressional Research Focus, 'Biometric Entry-Exit System: Legislative History and Status' (*In Focus*, 27 August 2020) https://sgp.fas.org/crs/misc/IF11634.pdf accessed 31 August 2023

Dickson K, 'Home Office investigating after woman gets through Newcastle Airport e-gates with wrong passport' (*Chronicle Live,* 15 March 2019) https://www.chroniclelive.co.uk/news/north-east-news/newcastle-airport-passport-control-gates-15980063 accessed 9 March 2024—the delayed Home Office report on airport security is not yet available

European Data Rights, 'How to fight Biometric Mass Surveillance after the AI Act: A legal and practical guide' (*EDRi*, 27 May 2024) https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/ accessed 8 June 2024

Funk A, 'I Opted Out of Facial Recognition at the Airport—It Wasn't Easy' (*Wired*, 2 July 2019) https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/ accessed 26 August 2023

Gokhale S, 'VERY IMPORTANT: Regarding DigiYatra at airports' (*X,* 27 January 2024) https://x.com/SaketGokhale/status accessed 18 March 2024

Gonzalez B, 'Digital Travel Credential trials resume with flights from Netherlands to Canada' (*Biometric Update*, 4 March 2024) https://www.biometricupdate.com/202403/digital-travel-credential-trials-resume-with-flights-from-netherlands-to-canada accessed 16 March 2024

Hera R, 'DigiYatra: Experts Flag Privacy Concerns Over the Facial Recognition App' (*Boom*, 21 March 2023) https://www.boomlive.in/explainers/digiyatra-air-travel-eased-face-recognition-privacy-breached-civil-aviation-jyotiraditya-scindia21396 accessed 30 August 2023

Jain A, 'NCRB's National Automated Facial Recognition System' (*Panoptic Tracker,* 5 May 2024), https://panoptic.in/about accessed 8 June 2024

Kachari D, 'Digi Yatra to open up for international travel, accept passport as an ID' (*Infra/Economic Times*, 29 December 2023)

https://infra.economictimes.indiatimes.com/news/aviation/digi-yatra-to-open-up-for-international-travel-accept-passport-as-an-id/106378139 accessed 7 January 2024

Kelly L, 'These European airports are trialling a new passport-free boarding process' (*TimeOut*, 16 May 2024) https://www.timeout.com/news/these-european-airports-are-trialling-a-new-passport-free-boarding-process-051624 accessed 15 June 2024

Meyersohn N, 'The newest pain point in air travel is slowing down travelers who paid for convenience' (*CNN Travel*, 22 December 2023) https://edition.cnn.com/2023/12/22/travel/tsa-precheck-clear-airport-security accessed 7 January 2024

Ovide S, 'You can say no to a TSA face scan. But even a senator had trouble' (*The Washington Post*, 11 June 2023) https://www.washingtonpost.com/technology/2023/07/11/tsa-airport-security-facial-recognition/ accessed 26 August 2023

Richter F, 'Tourism Recovery After Covid-19. International Tourism Approaches Pre-Pandemic Levels' (*Statista*, 18 December 2023) https://www.statista.com/chart/21793/international-tourist-arrivals-worldwide/ accessed 23 December 2023

Springall J, 'Biometrics and the future of travel beyond the airport' [Panel discussion] (*International Airport Review*, 14 June 2024) https://www.internationalairportreview.com/video/222629/biometrics-and-the-future-of-travel-beyond-the-airport/ accessed 16 June 2024

Sukriti, 'Digi Yatra and the Defect in the Idea of 'Consent'', (*Tech Policy*, 30 April 2024) https://www.techpolicy.press/digi-yatra-and-the-defect-in-the-idea-of-consent/ accessed 9 June 2024

Taylor H and Abdul G, 'Travellers faced long queues at major UK airports after electronic passport gates failed' (*The Guardian*, 27 May 2023) https://www.theguardian.com/world/2023/may/27/electronic-passport-gate-fault-causes-long-delays-at-major-uk-airports-epassport-egate accessed 28 May 2023

Verma D, 'Resist Surveillance Tech, Reject DigiYatra' (*Internet Freedom Foundation*, 16 January 2024) https://internetfreedom.in/reject-digiyatra/ accessed 13 June 2024