Balancing convenience and data privacy in the Digi Yatra app

Received (in revised form): 17th February, 2025

Vandana Gyanchandani

Lecturer, O.P. Jindal Global University, India

Vandana Gyanchandani is a Lecturer at O.P. Jindal Global University (JGU) teaching and researching international law and legal studies, with a focus on digital economy, trade, human rights, global governance and sustainable development. She has over five years' experience as a lecturer, having previously taught at the same institution. Vandana holds a Master's degree in international law and legal studies from Geneva Graduate Institute, where she gained valuable insights and skills in the global legal system and its challenges and opportunities. She has published multiple papers and articles on various topics related to her field of expertise, and has participated in several conferences and workshops to share her knowledge and passion for international law and justice. Vandana's core competencies include academic policy research, curriculum design, pedagogy, communication, collaboration and critical thinking. Her mission is to inspire and empower the next generation of legal scholars and practitioners, and to contribute to the advancement of international law and its impact on society.

O.P. Jindal Global University (JGU), Delhi, India
LinkedIn: https://www.linkedin.com/in/vandana-g-638a9123b/; Orcid: https://orcid.org/0000-0002-2969-8516;
E-mail: vgyanchandani@jgu.edu.in

Jayanti Dhingra

Student, O.P. Jindal Global University, India

Jayanti Dhingra is a third year BA LLB (HONS.) student at O.P. Jindal Global University, India.

O.P. Jindal Global University (JGU), Delhi, India
LinkedIn: https://www.linkedin.com/in/jayanti-dhingra-02741b249/; Orcid: https://orcid.org/0009-0008-5282-9837;
E-mail: 22jgls-jdhingra@jgu.edu.in

Kavya Agrawal

Student, O.P. Jindal Global University, India

Kavya Agrawal is a third year BBA LLB (Hons.) student at O.P. Jindal Global University, India.

O.P. Jindal Global University (JGU), Delhi, India
LinkedIn: www.linkedin.com/in/kavya-agrawal-0b3733206/; Orchid: https://orcid.org/0009-0001-8589-305X;
E-mail: 23kavyagrawall@gmail.com

Laasya Sarojini

Student, O.P. Jindal Global University, India

Laasya Sarojini is a second year BBA LLB (Hons.) student at O.P. Jindal University, India.

O.P. Jindal Global University (JGU), Delhi, India
LinkedIn: www.linkedin.com/in/laasya-sarojini-46000b264/; Orcid: https://orcid.org/0009-0003-6049-3839; E-mail:
23jgls-laasya@jgu.edu.in

Sanya Singh
Sanya Singh is a third year BBA LLB (Hons.) student at O.P. Jindal Global University, India.

O.P. Jindal Global University (JGU), Delhi, India

LinkedIn: www.linkedin.com/in/sanya-singh-49348225a/; Orcid: https://orcid.org/0009-0009-0306-875X; E-mail: sanyaworkemail@gmail.com

Abstract This paper introduces a pan-India facial recognition technology (FRT)-led biometric boarding system: the Digi Yatra app (DYA). It outlines the benefits and challenges of the DYA as an AI-driven FRT at airports. The paper discusses key regulatory approaches along with the applicable legal principles to govern FRT-led biometric boarding systems in the context of India and briefly compares it with the European Union (EU) standards on data privacy and artificial intelligence (AI) standards, especially as related to FRT applications for air travel. It provides practical policy recommendations by emphasising a systematic approach which covers the regulatory spectrum from broader regulatory foundations to narrower issues and context-specific applications of certain AI-driven technologies, eg FRT applications for air travel to uphold the constitutional balance between data privacy and convenience. This paper is also included in **The Business & Management Collection** which can be accessed at https://hstalks.com/business/.

KEYWORDS: Digi Yatra app, national digital travel ID, data privacy, facial recognition technologies (FRTs), GDPR, EU AI Act, biometric boarding system, Digital Personal Data Protection Act (DPDP Act), sensitive personal data, artificial intelligence

DOI: 10.69554/IPOK9437

INTRODUCTION

The Consumer News and Business Channel (CNBC) notes that the 'Smart Travel Project at Zayed International Airport in Abu Dhabi will involve biometric sensors at every airport identification checkpoint by 2025'.[1] Although some stakeholders are optimist of the changing paradigm whereby the air travel across jurisdictions becomes efficient due to artificial intelligence (AI)-led facial recognition technologies (FRTs), which work seamlessly for customers and airport operators alike,[2] other stakeholders raise concerns about the human rights violations led by FRTs that may be operated by public and private entities to profile individuals in transit at scale.[3] Specifically, the real-time untargeted FRT deployment by public and private entities may bring to life the Orwellian reality of *Nineteen Eighty-four* unless specific use cases of FRTs are regulated.[4] The aim is to balance human rights with technological innovation for convenience in order to safeguard the fundamental human rights of citizens underlined by the core values of democracy.

Given the larger dilemma of convenience versus privacy as a fundamental human right that AI technologies — specifically in our case, FRTs — present to policy makers across the world, this paper presents a brief sketch of an important case study.[5]

The paper discusses the Digi Yatra app (DYA), a pan-India biometric boarding system (DYBBS) designed mainly for seamless air travel within India. The government plans to further expand the DYA to foreign airports and passengers as well as to all kinds of travel and related activities within India, eg railways, taxi services and hotels, to enable a coherent digital ecosystem for travel.[6] In pursuance

of this ambitious national strategy to digitalise travel, the paper assesses the key benefits and challenges of FRT-enabled travel ecosystems, ie the DYA in the context of India, given the recent passage of the Digital Personal Data Protection (DPDP) Act, 2023 and relevant rules or guidelines. The paper briefly highlights the DPDP, 2023 as well as the responsible AI (RAI) recommendations by the National Institution for Transforming India (NITI) Aayog to enable DYA for responsible deployment of FRTs for air travel. It also discusses the role of the European Union (EU) General Date Protection Regulation (GDPR) and the EU Artificial Intelligence Act (AI Act) in building the foundational pieces of a regulatory framework for an effective governance of FRTs. Specifically, it highlights the relevance of a proposed Model Law on FRTs in Australia, which may provide a relevant blueprint to debate on a national FRT regulation as India aims to build a national consensus for a coherent regulatory framework relating to AI.

The paper is divided into five sections. This introduction is followed by a section that introduces the DYA alongside its key benefits and challenges. The third section discusses the main regulatory approaches to govern FRTs globally. It critically assesses the key issues presented by the DPDP, 2023, NITI Aayog's RAI Principles, the GDPR and the EU AI Act, 2024 to justify the application of FRTs via DYA in India. It outlines key principles from these regulations and guidelines which can support the DYA's compliance in India and beyond. The fourth section provides practical policy recommendations for the Indian Ministry of Civil Aviation (MoCA) overseeing the digitalisation of air travel. This is followed by a brief conclusion. The paper specifically recommends that India should consider a national regulatory consensus to govern AI technologies after the DPDP, 2023 as FRTs form a piece of the larger AI regulatory puzzle. It also recommends that beyond a general regulatory framework on AI, India should consider a more targeted national regulation to govern the development and deployment of FRTs in the Indian context to comply with the Supreme Court of India's Puttaswamy Judgment.

The use case of FRTs across sectors is increasing every day in India. Indian policy makers cannot afford to be reactionary; rather, they should adopt a cautious but proactive approach as these new technologies are being rapidly adopted across different sectors with clear implications for Indian citizens' fundamental rights. An effective regulatory oversight is required in the context of India so that the benefits of FRTs are proportionately balanced with the anticipated risks to the fundamental rights as these relate to data privacy.

DYA: INDIA'S FRT-BASED BBS

The DYA is a pan-India FRT system for air travel in India (see Figure 1), an initiative of the Ministry of Civil Aviation, Government of India.[8] An FRT is 'any computer system or device with embedded functionality that uses biometric data drawn from human faces to verify someone's identity, identify a particular individual and/or analyse characteristics about a person'.[9] An FRT system has four functionalities: (a) facial verification, ie 1:1 face matching; (b) facial identification, ie 1:n matching; (c) facial analysis, ie drawing inferences on an individual using their facial scans; and (d) facial detection, ie detect when a facial scan is in reference to an individual using their facial scans.[10] In the context of the DYA, however, we are concerned with two main functions of an FRT system: (a) 1:1 verification; and (b) 1:n identification.[11]

The DYA is a digital travel identification (ID) that is supported by a strong verifiable government-issued identity card such as Aadhaar (unique identity number), driving licence, passport etc., enabling a seamless travel experience for passengers at all airports across India.[12] The DYA is downloadable

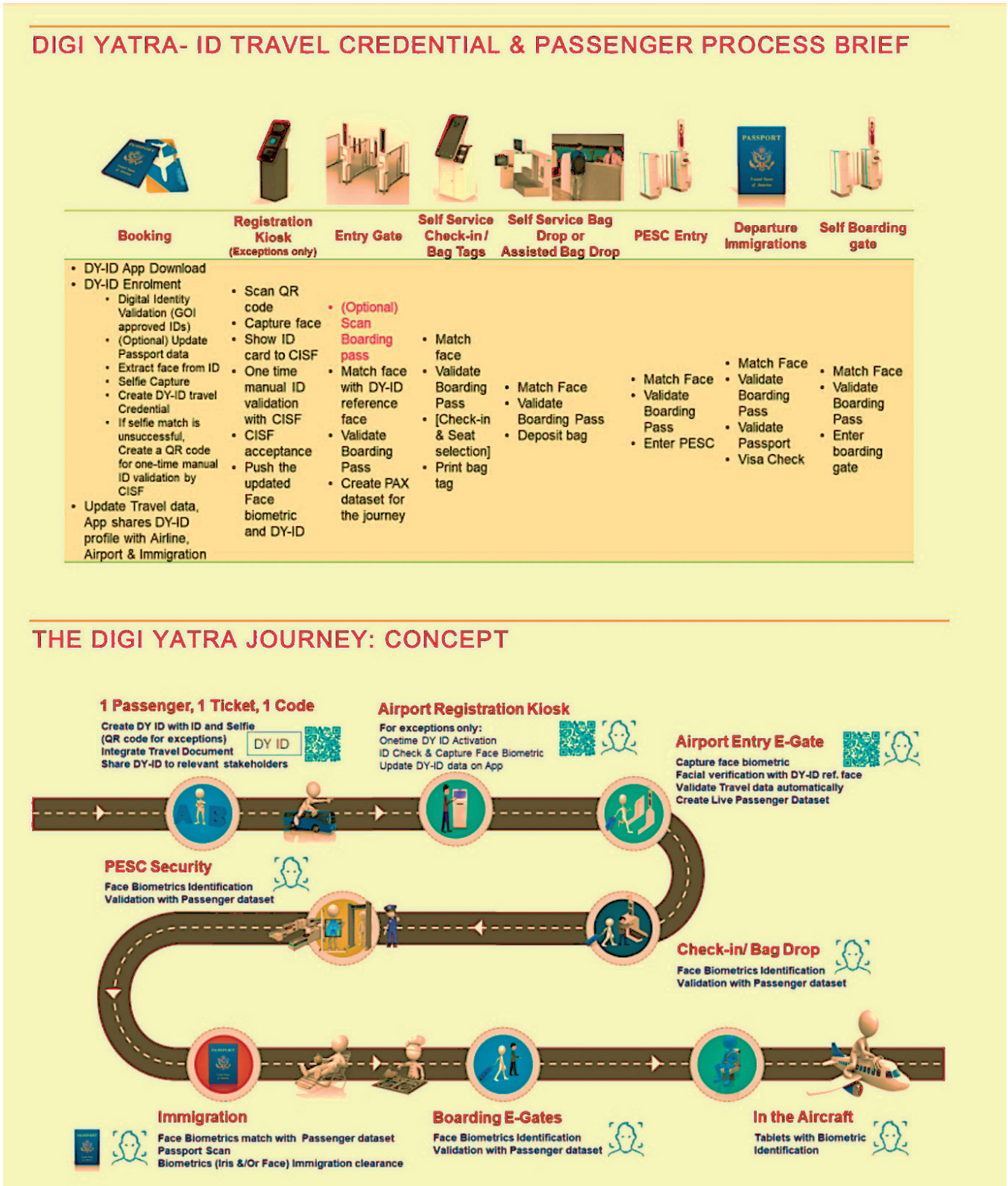

Figure 1: DYA BBS — reimagining air travel in India[7]

from PlayStore (Android) or App Store (iOS) for registration on the passenger's smartphone.[13] The passenger links their government-issued IDs using DigiLocker Wallet App or Offline Aadhaar services.[14] A digital photo of the passenger is used to match with the government-issued IDs to create an official DYA ID.[15] The facial scan as well as related personal data such as name, ID details, single token biometric face and passport data (if necessary) are secured in a digital wallet on the DYA in the passenger's smartphone.[16] The DYA is secured by public–private keypair encryption.[17] Passengers decide with whom their personal data is shared, ie airlines/online travel agencies (OTAs), airports and immigration authorities (for international travel) as well as other value-added service providers, using facial biometrics as a single token to digitally validate passenger identification and travel information.[18] The DYA official rules provide for explicit consent before sharing data with value-added service providers.[19] Passengers update their travel data by uploading the ticket/boarding pass or by scanning the electronic ticket/boarding pass barcode/mobile QR code as required.[20]

The DYA is based on W3C standards and the Digi Yatra Foundation (DYF) employs a self-sovereign identity (SSI), verifiable credentials (VC), decentralised identifiers (DIDs) and a distributed ledger to provide a decentralised layer of trust between the ecosystem's numerous participants.[21] The SSI can be understood as a digital identity which can be managed in a decentralised way without third-party interference.[22] The technology enables its users to manage their digital identities themselves.[23] Furthermore, 'verifiable credentials' can be understood as credentials that are unique to an individual and can be used to prove aspects of their identity in the same way as any physical document.[24] The DYA ID credential is like a digital passport that the owner can control.[25] Distributed ledger is a database that numerous participants can synchronise and access from distinct locations, eliminating the need for a central authority.[26]

The Ministry of Civil Aviation, Government of India provides that the application of latest technologies allows for greater individual control over their biometrics as sensitive personal data and eliminates the need for third-party involvement or control of sensitive data.[27] There is no central storage of sensitive personal data, and travel data with biometrics is purged 24 hours after the departure of the passenger's flight.[28] The legal basis of the DYA transactions can be understood as a voluntary agreement for the temporary collection, storage and use of data.[29] The Ministry emphasises that participation in DYA is entirely optional and at the discretion of the passenger.[30] Passengers are free to choose standard check-in procedures and remove their profiles to opt-out any time.[31]

Benefits

Three specific benefits of the DYA are (a) convenience and cost savings; (b) security and safety; and (c) healthcare, accessibility and sustainability.

Regarding *convenience and efficiency*, the DYA provides both benefits for individuals, airports and government at scale.[32] Use of FRTs is much more convenient and efficient than other biometrics such as fingerprints, digital devices, codes/passcodes or paper print-outs for the verification and identification of large numbers of people.[33] It has been argued that the FRT-enabled identity management ecosystem can enhance the functioning of Indian aviation, digitise manual processes at airports, improve security standards and lower the operational costs of airports quickly.[34] It can support lower congestion rates, reduce wait times and queues — frequently the result of human error.[35] Automation of identity management at airports eliminates many bottlenecks in the functioning of the airports to handle large numbers of customers.[36]

Regarding *security and safety*, it is argued that facial scans constitute a strong biometric signature as they are a unique identifier that cannot be accidentally misplaced or copied.[37] They reduce ID fraud and access of non-travellers into the terminal.[38] This adds to the security and safety of the FRT-enabled digitalisation of air travel as supported by the DYA.[39] The DYA policy indicates that it would use end-to-end, peer-to-peer encrypted communication in accordance with existing legal standards such as the DPDP and the Supreme Court's Puttaswamy verdict.[40]

Regarding *healthcare, accessibility and sustainability*, the DYA was launched on 1st December, 2022, in the midst of the COVID-19 pandemic, when physical distancing was the norm due to health concerns.[41] The DYA ensured physical distancing through contactless and paperless processing for air travel, resulting in public health benefits alongside convenience.[42] The fact that the DYA is uniformly applicable at any Indian airport enhances its value in terms of accessibility for passengers.[43] The digitalisation of airports through FRTs as proposed by the DYA not only reduces red tape but also supports sustainability goals by removing unnecessary paperwork at airports.[44] Thanks to increased efficiency in passenger processing and planning via FRT-enabled technology, it also defers costly airport infrastructure expansion.[45]

Challenges

Three challenges of the DYA are (a) errors; (b) data privacy; and (c) function creep.

Regarding *errors*, the FRT as deployed by the DYA can lead to errors and inaccuracies that may arise from the technical operation of an FRT, including as a result of issues related to training and reference data or the accuracy of an algorithm.[46] The issues include:

a. *Inaccuracy due to poor quality input data*: Independent organisations such as the U.S. National Institute of Standards and Technology (NIST) confirm that FRTs can lead to errors when low-quality facial scans are used in as input data.
b. *Algorithmic errors*: Mistakes made by algorithms in analysing facial characteristics.
c. *Demographic variation errors*: It has been noted that dark-skinned individuals and those with a disability are prone to higher rates of FRT errors.
d. *User and system errors*: Incorrect deployment without adequate controls for the accurate functioning of the system, or poor processes causing the system to exhibit errors, respectively.[47]

Various glitches and a major incident of app migration has been witnessed in the application of the DYA in India.[48] For example, Kolkata and Pune airports noted that passengers were unable to upload their boarding passes on the DYA, leaving airport officials to tackle an immediate surge of passengers, with many missing their flights due to unplanned check-in procedural requirements necessitated by the DYA malfunction.[49] The *Hindustan Times* news report noted:

> The Digi Yatra services in Pune is often non-functional because of technical glitches.[50] A heavy surge of passengers coupled with heightened security and a glitch in the Digi Yatra facility prompted complete chaos at the Pune Airport over a long weekend. Travellers were left high and dry as the break down in the Digi Yatra facility resulted in long queues for check-in procedures (with some missing their flights).[51]

In another instance, the DYF dropped Dataevolve as a technical partner in the operation of the DYA due to ongoing criminal investigations against it.[52] According to the DYF, it was not due to Dataevolve but to the expanding user base that the new app was introduced.[53] The Internet Freedom Foundation (IFF) had raised questions about

the ability of Dataevolve to access sensitive personal data of citizens before DYF dropped the technology company from the DYA's operations.[54]

Regarding *data privacy*, the issue of coercive and deceptive tactics to seek passenger consent has been a critical issue, as highlighted by various civil society organisations, especially the IFF.[55] It has been argued that despite the assurances of voluntary consent to opt for DYA, there are noted instances of coercion in many instances.[56] The DYA entry points are given priority at airports where the DYF has a stake.[57] Multiple disadvantages experienced by customers due to not opting into the DYA also function to coerce consent.[58] In some instances, passengers alleged that they were being mandatorily registered into the DYA with no explanation other than it was essential for their travel.[59] A survey on the issue suggested that many people signed up under duress or without sufficient information;[60] however, the Minister of Civil Aviation clarified that there are DigiBuddies (staff/agents at the airports) who are employed to assist passengers to opt into the DYA and explain how it functions for ease of travel.[61] Nevertheless, the situation raises questions on the viability of consent processes in place and the plausibility of subtle kinds of coercion to increase the number of passengers opting in.[62]

In addition, there is a lack of clarity on the storage and processing of sensitive personal data, ie facial scans as biometrics, by the relevant data controllers (DYF, in this case) and processors (airport operators).[63] The DYA guidelines explicitly state that according to the data privacy obligations as they relate to the processing of sensitive personal data, facial scans as biometrics are solely for the use of the airline and airport operators, without explaining the role of DYF as the nodal agency behind the implementation of the DYA.[64] The airline and airport operators can only share the data of their passengers with any third party for the purpose of ensuring the seamless passenger DYA experience.[65] Civil society organisations such as the IFF have raised concerns over the lack of transparency on such issues.[66]

The IFF argues that the DYA has a weak policy foundation in light of customers' personal data and fails to clarify the purposes for which it may be collected.[67] It says that the collected data may be used for purposes other than those related to ease of travel, such as improvement of products, contacting for surveys, processing user/customer requests and so on.[68] Further some clauses are contradictory, as the privacy policy allows for collecting, storing, processing, transferring and sharing passenger/user personal information including sensitive personal information with third parties or service providers for the purposes set out in the policy, which include marketing, events, programmes and promotions, but on the other hand states that the data collected under the DYA cannot be used by another entity since it is encrypted.[69]

Further, the Ministry of Civil Aviation in an April 2023 press statement claimed:

> that DYA passengers' data is stored in their own device and not in centralized storage[70] … In the DY process, there is no central storage of passenger's Personally Identifiable Information (PII) data.[71] All the passenger's data is encrypted and stored in the wallet of their smartphone.[72] It is shared only between the passenger and the airport of travel origin, where passenger's DY ID needs to be validated.[73] The data is purged from the airport's system within 24 hours of departure of flight.[74]

The IFF claims that this statement contradicts the DYBBS policy, which states that the airport operator will retain the travel data including the DYA ID travel credentials for a duration of 30 days from the date of departure.[75] It implies that data is stored, and that union government functionaries have access to it as required.[76] The IFF also suggests that the statement is at odds with

an interview given by Avinash Kommireddi, the founder and chief executive officer (CEO) of the company that designed the DYA ecosystem, Dataevolve, wherein he states that data authentication takes place on the Amazon Web Services (AWS) cloud platform.[77] This authentication flow has not been referenced by the Ministry of Civil Aviation of India in any of its statements about the exchange of information between a passenger's smartphone and origin airport, or mentioned in the DYBBS policy.[78] Overall, how data is stored and authenticated in the DYA ecosystem has not been made transparent, which raises concerns for whether privacy standards are being complied with.[79]

The DYA ecosystem is built and owned by the non-profit Digi Yatra Foundation, a joint venture company under section 8 of the Indian Companies Act, 2013 established by the Airport Authority of India (26 per cent) and Bangalore, Delhi, Hyderabad, Mumbai and Cochin International Airports (each accounting for 14.8 per cent, ie 74 per cent total).[80] The public–private ownership of the DYF has raised questions of accountability and transparency in the implementation of the DYA, since the DYF is exempt from right to information (RTI) file requests from the civil society on any concerns, especially those related to data privacy, as the project is governed by a non-profit body of airports.[81] Specifically, when the sensitive personal data of passengers is shared with value-added service providers within or adjacent to the relevant airports for convenience, such lack of accountability and transparency as to the regulatory role of data controllers and processors in the implementation of the DYA becomes problematic.[82] Passengers may not fully realise the extent to which access is granted to the data processed by the airports to other service providers.[83]

Biometric data, unlike passwords, cannot be changed.[84] Public and private entities can use biometric data to track movements within the airport to market different products and services without the express consent of data subjects.[85] This raises genuine concerns about the long-term security of such sensitive personal data.[86] The DYA regulatory ecosystem lacks impartial supervision since security audits are conducted on a private basis and results are withheld from the public.[87]

Regarding *function creep*, one major concern is the gradual and lateral expansion of FRT use beyond its intended purpose, which might promote surveillance activities without appropriate checks and balances.[88] The nature of FRTs being flexible makes it easier to simply expand the area and degree of coverage over time, eg the use of FRTs to monitor a crowd in a public space to search for missing persons or target criminals can also be used to evaluate the racial composition of a crowd at a given time.[89] This phenomenon is called 'function creep', as the actual function of an AI system such as FRT is laterally expanded by public and private entities.[90] Notably, FRTs are mainly developed by private entities for deployment by public entities, which raises another concern as to whether profit motives out-win technical aspects concerning regulatory control and oversight. The case of Clearview AI exemplifies the global scope of such practices, as many large technology companies such as IBM, Microsoft and Amazon have publicly halted their ambition to develop FRTs unless an adequate regulatory framework is in place to prevent malpractices.[91]

APPROACHES TO REGULATE FRT APPLICATIONS AT AIRPORTS

Broadly, there are three main approaches to regulate the data privacy concerns relating to FRTs:

a. Pre-existing data protection laws which outline protection of facial scans or biometrics as sensitive personal data,[92] eg the EU GDPR.[93]

b. Legal or voluntary (public or private) bans and moratoriums to prohibit FRTs specifically in certain contexts:[94] eg Amazon, Microsoft and IBM voluntarily ceased the sale of FRTs until a proper regulation was enacted,[95] and San Francisco became the first US city to ban the use of FRTs in 2019.[96]
c. A coherent FRT regulatory framework alongside a general data protection law:[97] eg Washington DC, Virginia and Massachusetts have introduced legislation to regulate FRTs while key Federal Bills have been proposed in pursuance of same.[98] The concerns relating to real-time FRTs have been a source of major concern for privacy activists for their potential to enable indiscriminate mass surveillance.[99]

India recently enacted its National Data Protection Framework, titled the DPDP Act, 11th August 2023.[100] Although it lacks a national AI regulatory framework or a specific FRT regulation at a national or state level, there are certain features of the DPDP, 2023 which can be useful to govern the application of FRTs at airports.[101] The DPDP emphasises the need both to balance the rights of individuals and to process such data for convenience and for lawful purposes only.[102] 'Lawful purpose' means 'any purpose which is not expressly forbidden by law'.[103] Critically, it must be highlighted that unlike the EU GDPR, which will be discussed subsequently, the DPDP does not have a higher level of protection of 'sensitive personal data' which includes 'biometric data' as compared to general 'personal data'.[104] The DPDP covers core data protection principles such as purpose limitation, lawful purpose, accuracy, erasure (right to be forgotten), storage limitation, integrity, confidentiality and accountability.[105] It emphasises that the 'consent' by data subjects/principals must be 'free, specific, informed, unconditional and unambiguous with a clear affirmative action'.[106] The DPDP provides for the need of 'verifiable' parental/guardian consent for children/differently abled individuals.[107] It specifically prohibits 'tracking or behavioural monitoring of child or targeted advertising directed at children'.[108]

The DPDP states that the central government may classify any data fiduciary or class of data fiduciaries as a 'significant data fiduciary' on the assessment of select factors, including the volume and sensitivity of personal data collected and risks to data principal, in addition to issues relevant for public order and security.[109] All significant data fiduciaries must appoint data protection officers who will select independent data auditors to carry out personal data audits to ensure compliance with the DPDP, 2023.[110] Specifically, the independent data auditors need to undertake periodic data impact assessments.[111]

In order for personal data to be transferred to third countries, the DPDP provides for a blacklist approach whereby the specific third country must not be explicitly restricted to process personal data originating from India.[112] Specific notifications by relevant government agencies will further specify how third-country transfers of personal data will take place in future, although there is a specific exception relating to contractual relationship.[113] The DPDP rules provide that the 'transfer to any country/entity outside India in pursuance of offering goods or services to data principals within India is subject to requirements which may be specified by the central government'.[114]

The NITI Aayog, a key public policy think-tank of the Government of India, released the National Strategy on AI (NSAI) and subsequently a White Paper titled 'Responsible AI for All – Adopting the Framework – A Use Case Approach for Facial Recognition Technology' in June 2023.[115] The White Paper sets out the NITI Aayog's RAI principles for a better regulatory approach to the application of FRTs by public and private entities.[116] Specifically, these RAI principles are:

a. *Principle of safety and reliability*: FRTs should be deployed reliably as intended with sufficient safeguards in place to ensure the safety of stakeholders.
b. *Principle of equality*: FRTs should treat individuals under the same circumstances equally.
c. *Principle of inclusivity and non-discrimination*: FRTs should not deny opportunity to qualified persons on the basis of identity such as religion, race, caste, sex, descent, place of birth or residence in matters of education, employment, access to public spaces, etc.
d. *Principle of transparency*: The design and functioning of FRTs should be recorded for external scrutiny and audit to prove that their deployment is fair, honest, impartial and guarantees accountability.
e. *Principle of accountability*: The design, development and deployment of the AI system must be responsible and the relevant stakeholders must be accountable.
f. *Principle of protection and reinforcement of human values*: FRTs should support positive human values without disturbing the social harmony in community.

Likewise, Daniel J. Solove in a recent article titled 'AI and Privacy' provides for a broad regulatory oversight of the applications of AI technologies, specifically highlighting five core regulatory principles:

> '(a) transparency about the data that organizations collect and use; (b) due process as guarantees of meaningful notice and opportunity to be heard; (c) stakeholder involvement as development of AI in an exclusive manner often lacks the involvement of all relevant stakeholders; (d) mix of internal and external accountability – Regulation should balance a tightrope between overly trusting organizations to manage themselves along with avoiding micromanaging and requiring permission for everything an organization might do. Ultimately, there must be a mix of internal and external accountability mechanisms and (e) enforcement and remedies to balance the investment push to develop AI technologies.[117]

The NITI Aayog clarifies that:

> The RAI principles have been developed by first identifying systemic considerations prevalent AI systems across the world, the identifying principles that may be used to mitigate the identified considerations. The principles are based on current understanding and AI landscape and must evolve with innovation and technology advances and with a greater understanding of the impact of AI.[118]

Critically, the NITI Aayog highlights specific concerns and relevant recommendations to mitigate the data protection risks from the application of FRTs at airports via the DYA.[119] It outlines special procedures for the handling of personal and sensitive data, which needs to be specifically identified in the operation of the DYA.[120] Although the DYA is required to delete the biometric data 24 hours after the flight, the privacy guidelines state that the DYA shall have the right to change the data purge settings based on security requirements on a need basis.[121] The NITI Aayog specifies a set of defined timelines and purposes for the retention of different types of data within the DYA ecosystem.[122] Any security-based exceptions should be clearly highlighted by the proposed ethics committee and outlined in an official standard operating procedure (SOP).[123] It further specifies that this is a continuous process which needs to be updated and a dedicated ethics committee should regularly review such processes.[124]

The NITI Aayog stresses that the use of facial recognition data and other relevant subject data for providing value-added services should only be activated through an opt-in rather than an opt-out method of consent, with an ability to revoke consent at any time.[125] A provision for opting in provides users with an active choice with less transactional risks to protect their personal data.[126] An explicit consent must be required

to create individual profiles and processing of sensitive personal data.[127] Transparency in the collection of personal data and its processing at all stages of the DYA's life cycle must be provided in a clear and concise format.[128] A continuous monitoring of the performance of the entire DYA ecosystem is necessary.[129]

Additional value-added service providers require an explicit consent, which may be set out in a licensing agreement between the DYF and the third-party vendors prior to sharing individuals' sensitive personal data.[130] Further, the SOP should provide clear protocols for the sharing of individuals' personal data with any security agency, central or state government agency based on current protocols existing at the time.[131] Any sharing of personal data with such public or private agencies should be in conformity with the DPDP, 2023, and the Puttaswamy Judgment by the Supreme Court.[132] Ideally, an ethics committee should draft these inter-agency data-sharing protocols.[133] An agency should be established to publish specific standards to be followed by the DYA programme on the explainability, bias and errors in the use of FRTs at airports specifically for the Indian context by obtaining relevant feedback from the stakeholders.[134]

The EU GDPR, in contrast to India's DPDP, 2023, provides for deeper commitments on the data protection principles of lawfulness, transparency, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, accountability, right to access information relating to personal data processing, and right to erasure (right to be forgotten), which are specifically tailored for the protection of biometric data as sensitive personal data.[135] As noted above, India's DPDP neither has a definition of 'sensitive personal data' or 'biometric data', nor specifically distinguishes between them in order to provide higher standards of data protection for sensitive personal data.[136] The GDPR explicitly prohibits the processing of sensitive personal data, which includes facial scans as biometrics, unless the data principal has given an explicit consent for a specific purpose.[137] The GDPR, like the DPDP, provides that the consent should be freely given, specific, informed and unambiguous indication of the data subject's wishes as a clear affirmative action.[138] It provides for a parental/guardian consent to process personal data of children or differently abled individuals.[139] An explicit consent is mandatory to process sensitive personal data.[140] Unlike the DPDP, the GDPR includes a more coherent set of transparency and accountability obligations for data controllers and processors.[141]

Both the GDPR and the DPDP confirm that the data subjects/principals shall have the right to not be subject to a decision based solely on automated processing, including profiling which produces legal effects relating to the subject.[142] Similarly, the GDPR, like the DPDP, provides for data protection impact assessments in the case of data processing which is significant in scope and is likely to result in high risks to the rights and freedoms of natural persons.[143] It states that such data protection impact assessments shall contain at least 'a systematic description of the processing operations', 'purposes of the processing', 'legitimate interests pursued by controller', 'an assessment of necessity' and 'proportionality of the processing operations in relation to the purposes given the rights of the data subjects'.[144]

On third-country transfers of personal data, the GDPR offers a principled and transparent approach compared to the DPDP.[145] The GDPR provides for a general adequacy decision mechanism for the transfer of personal data to select third countries.[146] The mechanism requires the select countries to provide evidence to the EU Commission (EC) that their regulatory environment, specifically in relation to data protection issues, is compatible with or at least 'essentially equivalent' to the EU's regulatory requirements.[147] If the EC approves an adequacy decision for a country, then

personal data from the EU can flow freely to the select third countries without any further substantive procedures.[148]

In the absence of a general adequacy arrangement, however, the GDPR gives reasonable alternatives for specific entities/institutions in third countries to process personal data from the EU, eg binding corporate rules,[149] standard data protection clauses,[150] approved codes of conduct,[151] certification mechanisms,[152] etc.[153] Critically, Article 49(1) of the GDPR provides for a derogation from obligations relating to third-country transfers if the data subject (individual/s) has explicitly consented to the proposed transfer after having been informed of the possible risks, given the lack of adequate or alternative safeguards.[154] It is, however, a high-threshold obligation which needs to be met, as consent will be express, explicit, freely given, specific, informed and revocable without detriment.[155]

On 23rd May, 2024, the European Data Protection Board (EDPB) released a statement on the use of facial recognition to streamline passenger flow and its compatibility with specific provisions of the GDPR (specifically, Articles 5(1)(e) and (f), 25, and 32) at the request of the French Supervisory Authority.[156] The EDPB highlighted three scenarios where FRTs are deployed at airports.

The first scenario stores the biometrics of individuals in their personal devices under their control to authenticate (via 1:1 comparison).[157] In this case the measure meets the necessity principle if the controller can demonstrate that there are no less intrusive alternative solutions that could achieve the same objective effectively.[158] The intrusiveness of the processing of biometrics needs to be counterbalanced with the active involvement of the passengers to control their own data.[159] Sensitive personal data should be deleted from the systems once the purpose is met.[160] Additionally, specific safeguards need to be in place, such as a proper data processing impact assessment to be compliant with the GDPR.[161]

The second scenario provides for centralised storage and management of biometrics within airports in an encrypted form with an individual key solely in the hands of passengers.[162] This enables passenger authentication (via 1:1 comparison) as they proceed through the airport checkpoints.[163] The enrolment data is valid for a certain period, which could be one year after last flight or passport expiry date.[164] This data processing meets the necessity principle if there are no alternative solutions which are less intrusive that could achieve the same objective.[165] The intrusiveness of the data processing needs to be counterbalanced by the active involvement of passengers, since they should solely control the key to the encrypted biometric data.[166] If the data controller implements appropriate safeguards, the data security risks using a centralised database would be mitigated and the impact on the data subjects' rights be considered proportional to the benefits of convenience.[167] The controllers should provide for the shortest possible central storage of personal data and explain the options available to the data subjects, given their preferred storage period.[168]

In the third scenario, the biometrics are stored centrally in an encrypted form under the airport operator's control.[169] The storage period is 48 hours and the data is deleted once the plane takes off.[170] The EDPB emphasises that there are evidently less intrusive means to simplify air travel.[171] The central storage of biometrics in a single database could risk confidentiality and security at scale if the database is compromised.[172] Therefore, this scenario does not meet the necessity and proportionality principles in the GDPR.[173]

The fourth scenario involves the centralised storage of an enrolled biometric template in an encrypted form in the cloud under the control of the airline company or its cloud service provider.[174] This enables 1:n passenger identification.[175] The storage period in this scenario can be as long as the individual has

an account with the airline company.[176] The ID and biometric data is stored in a central database in the cloud. Multiple entities could have access to such sensitive personal data in a cloud, including outside actors.[177] The sensitive personal data is decrypted when in use and the keys are under the control of the airline company or its processors.[178] The centralised storage architecture also leads to the passenger losing control of their data to a greater extent compared to the previous scenarios.[179] The data could also be stored for a significant period of time, exposing it to higher risks. It is beyond strictly necessary and proportionate for the purposes unless strong measures are taken to mitigate the risks.[180] Similar results can be achieved in a less intrusive manner. The impact on the data subjects seems to outweigh any anticipated benefits.[181] Therefore, this scenario does not meet the necessity and proportionality principles in the GDPR.[182]

The EU AI Act covers explicit prohibitions on the deployment of FRTs, especially real-time, untargeted biometric surveillance via scraping of facial images from the Internet or CCTV footage.[183] It states that FRTs that perform profiling of natural persons needs to be considered as a high-risk system.[184] Critically, it advocates for a risk management system for high-risk AI technologies such as FRTs which is a continuous iterative process planned and run throughout the entire life cycle of a high-risk AI system, requiring regular systematic review and updating.[185] It needs to evaluate relative risks of the system period to adopt appropriate and targeted risk management measures.[186] The EU AI Act necessitates a fundamental rights impact assessment for high-risk AI systems on the impact on fundamental rights that the use of such a system may produce, which takes into account the process, timeline, categories of persons affected, specific risks of harm, implementation of human oversight and countermeasures in case of materialisation of risks.[187]

The Council of Europe's Guidelines on FRTs refer to the relevant principles in Convention 108+ (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).[188] These guidelines provide key principles for FRT developers, manufacturers, service providers and public or private entities. Some of the general principles include lawfulness, strict limitations of uses, defined legal basis per context, certification mechanisms, enabling education and awareness, data protection impact assessments, ethical frameworks for AI systems, protection of data subjects' rights, etc. Specifically, the guidelines stipulate that 'consent' cannot be a legal ground for facial recognition deployment by public authorities, given the imbalance of power between data subjects and such authorities. The law should clearly provide for specific purposes of FRT deployment by public authorities, and to ban private entities from deploying FRTs in uncontrolled environments such as shopping centres, etc. The use of FRTs by private entities requires an explicit, specific, free and informed consent of data subjects. Given the need for such consent, FRTs can only be deployed in a controlled environment by the private entities for verification, authentication and categorisation purposes.

In terms of making the DYA available to international passengers at international airports across jurisdictions, it is relevant to note specific initiatives by the International Civil Aviation Organization (ICAO) to enable global interoperability of biometric boarding systems by providing for common principles on data protection, data security and system design. Specifically, the ICAO's Doc 9303 titled 'Machine Readable Travel Documents (MRTDs)' recommends 'facial recognition' as the primary biometric identifier due to its non-intrusive nature and ease of connectivity with existing systems. This paper includes an appendix for policy makers and relevant stakeholders which lists relevant international organisations and jurisdictions that have endorsed specific AI guidelines, principles and regulations for further deliberations (see Appendix A).

POLICY RECOMMENDATIONS

The NITI Aayog rightly provides that FRT systems are inherently data-intensive technologies (mostly algorithmic in design).[189] In light of the scale of biometric data captured by such systems, which are given a higher degree of data protection in the context of the EU GDPR as setting the global benchmark for personal data protection, there is a legal imperative to develop coherent guardrails around the use of FRTs in India across sectors. A national regulatory framework is supported by the NITI Aayog as well as other experts instead of piecemeal statutes emerging in siloes and in conflict with one another.[190]

Apart from the DYA where FRTs are extensively used, there are also various other applications for FRT in different sectors. The Panoptic Tracker, an initiative by the IFF, provides central and state-level FRT deployments in India across sectors.[191] Currently, India has around 170 FRT systems, of which 20 are already in operation and the rest are in initial stages of testing.[192] In 2018, the Unique Identification Authority of India (UIDAI), which governs the Aadhaar, biometric digital identity of India, issued a circular to use facial scans for authentication.[193] There was an additional authentication to be used from fingerprint and iris scans.[194] In 2021, the Department of Pensions and Pensioners Welfare (DoP&PW) implemented FRTs for pensioners to develop a Digital Life Certificate (DLC).[195] The certificate is linked with Aadhaar and thus removes the need for citizens to submit physical certificates for obtaining their pensions.[196] FRTs are also used to record attendance at workplaces.[197] In fact, during the COVID-19 pandemic, to maintain social distancing, FRTs were deployed in private and government schools and colleges for recording and maintaining attendance records.[198]

In 2019, the National Crimes Records Bureau (NCRB) under the Ministry of Home Affairs invited bids for the implementation of a centralised system called Automated Facial Recognition System (AFRS).[199] Its purpose was to create a repository of all criminals or suspended criminals in a database for easy identification or verification and access was given to police stations.[200] The AFRS's main objective is modernising the police force, information gathering, criminal identification, verification and its dissemination among various policy organisations and units across the country.[201] The request for protocol (RFP) was replaced by a new RFP in 2020, which states that the AFRS technology will not be integrated with CCTV cameras.[202] Concerns were raised about the discriminatory policing against minority communities in India.[203] The use of AFRS can give unchecked power to law enforcement agencies to track any person without addressing any security or privacy concerns.[204] Nevertheless, it is being used by law enforcement agencies in various states including New Delhi, Punjab, Andhra Pradesh, Uttar Pradesh, etc.[205] In fact, the instalment of CCTV cameras also shows the constant surveillance and monitoring being carried out on people.[206]

These examples are just a few among many instances in which FRTs are being deployed.[207] The ubiquity of FRT has also raised various privacy concerns before the courts in India.[208] It is used in almost every application, ranging from complex usages by law enforcement agencies to maintain public order, to everyday consumer devices such as phones and tablets, where facial recognition and other forms of biometric recognition are becoming increasingly common.[209]

According to Mohanty and Sahu's piece in *Carnegie India* titled 'India's Advance on AI Regulation', India inclines towards a pro-innovation approach to enable the potential of AI technology while understanding its real risks.[210] This is mentioned in the G20 Ministerial Declaration during the Indian Presidency and an official Statement in Parliament in April 2023 that the 'Indian government is not considering bringing a law or regulating the growth of AI in the country'.[211] Simultaneously, the Ministry

of Electronics and Information Technology (MeitY) issued a government advisory for government's permission before deploying AI models in India and to prevent algorithmic discrimination and deepfakes.[212] The advisory was replaced with a fresh one which remains in force.[213] The Government clearly has a fragmented approach, as there are differing views within the system.[214] Currently, the Government is building consensus while adopting caution.[215] The authors recommend the Government to follow the global regulatory landscape on AI while taking an issue-focused, systematic approach to regulate specific concerns regarding AI technologies before developing a broader national regulatory framework for AI in India.[216]

The DYF, especially the Ministry of Civil Aviation, Government of India, needs to ensure compatibility of the DYA with the basic GDPR standards before expanding the applicability to international passengers and airports in future. As noted earlier, facial scans are biometrics which are protected as sensitive personal data in the GDPR. Non-compliance with necessary data protection standards as applicable to international passengers and jurisdictions can lead to financial penalties or fines as well as reputational harm.

By way of a relevant case study, a coordinated investigation and penalties/fines have been imposed on Clearview AI in Europe for multiple GDPR violations (see Table 1), specifically violation of Article 9 of the GDPR which relates to the processing of a special category of personal data (biometrics) of EU citizens. The article provides for an explicit consent, given the specific cycle of data collection and legitimate purpose with adequate safeguards, especially as related to third-party service providers seeking access to biometric data, creates specific compliance issues for DYA in light of the challenges discussed earlier. Specifically, the Dutch DPA noted that:

> Clearview is a commercial business that offers facial recognition services to intelligence and investigative services.[217] Customers of Clearview can provide camera images to find out the identity of people shown in the images. For this purpose, Clearview has a database with more than 30 billion photos of people. Clearview scrapes these photos automatically from the Internet. And then converts them into a unique biometric code per face. Without these people knowing this and without them having given consent for this. … Clearview should never have built the database with photos, the unique biometric codes and other information linked to them. This especially applies for the codes. Like fingerprints, these are biometric data. Collecting and using them is prohibited. There are some statutory exceptions to this prohibition, but Clearview cannot rely on them.

The University of Sydney (UTS) proposed an architecture for a future FRT regulation by policy makers in Australia.[219] It is interesting to note its key features in the Indian context to regulate FRTs.[220] The Model Law provides a risk-based regulation with specific obligations on developers and deployers of FRTs.[221] It suggests that due to the use of facial scans, FRTs will generally limit human rights; however, it is important to understand the context wherein such limitations may be justified.[222] In pursuance, it is necessary to conduct human rights risk assessment inclusive of specific factors such as:

Table 1: Clearview fines and penalties

Data protection authorities	Fines/penalties on the Clearview AI	Date
France DPA	€20m	December 2022
Italy DPA	€20m	March 2022
Greece DPA	€20m	December 2022
UK DPA	£7.5m	May 2022
Dutch DPA	€30.5m	May 2024

Source: European Data Protection Agency (EDPB)[218]

- The *spatial context*, ie the place or environment (public places or controlled spaces of work or law enforcement) where the FRT application is used.
- The *functionality* of FRTs employed, ie verification, identification, analysis or detection.
- The *performance* of FRTs, ie the relative accuracy that can produce reliable results.
- Whether the FRT produces *output* that leads to a decision which has a legal or similar impact for an individual or a group, and whether such decisions are partially or fully automated.
- Whether affected individuals can provide free and informed *consent*, or withhold such consent, prior to the use of FRTs.[223]

The UTS Model Law states that it is the cumulative assessment of such factors which can help policy makers decide the risk level (moderate, significant or extreme) of FRTs to the human rights of citizens involved in a specific context.[224] The Model Law proposes a harmonised application of regulatory standards across all sectors to ensure reasonable regulatory oversight on FRTs' development and deployment.[225]

To regulate the use of FRTs across different sectors in India, it is important to establish a core regulatory framework for FRT development and deployment in the Indian context. It will be necessary, however, to have an overarching national regulatory consensus on data privacy and AI that strikes an acceptable legal balance between data privacy and convenience to effectively guide sectoral applications of FRTs. The Puttaswamy Judgment by the Supreme Court of India emphasised that there is a need to strike a constitutional balance between right to data privacy and economic convenience as two conflicting human rights; however, such a balance is struck differently within every jurisdiction, given the distinct subjective realities and expectations of citizens.

A sectoral regulatory approach to govern FRT applications would ultimately warrant a national consensus on regulatory concerns about data privacy and AI, as FRT regulations are part of the larger debate on data privacy versus convenience. Although the aim is to achieve the highest net societal benefit that is greater than the sum of these two conflicting values at a given time, the exercise is a socio-political and economic calibration rather than a mathematical one.

India should adopt the EU's general regulatory approach which introduced a comprehensive data protection regulation, the GDPR, followed by the AI Act. These overarching legal texts set the national approach to balance economic development and innovation with the protection of fundamental human rights in the EU's context. These foundational regulations make it more feasible for the EU to ensure an effective regulatory approach on the application of FRTs by public and private sectors, as the larger policy consensus is clear in terms of data protection and regulation of AI, which needs to interact and inform the governance of FRTs across sectors.

India has a national data protection framework which is yet to become fully operational, as clarity on various provisions, specifically on third-country transfer of personal data, will be notified by the central government. India, however, lacks consensus on a national regulatory approach for AI. India will be in a better position to regulate sectoral application of FRTs when the larger regulatory dilemmas are clarified through a national consensus on data protection and AI governance. The legal vacuum due to the lack of a national AI regulation in India will make sectoral governance of FRT applications ineffective in the long run.

CONCLUSION

This paper has assessed the key benefits and challenges of FRT-enabled national biometric boarding systems in India, ie the DYA. It has explained the regulatory approaches of India versus the EU to navigate the challenges of AI-led FRT systems for air travel.

Critically, it suggests that India should have a coherent approach to assess and regulate data protection concerns posed by AI-led and FRT-enabled BBSs in India, taking necessary guidance from the EU standards on AI and FRT regulatory approaches. At present, India's data protection regulatory framework is too soft and opaque, especially as it relates to obligations of the state and its agencies to encapsulate the numerous regulatory challenges posed by widespread application of AI technologies — specifically, in the context of this paper, FRT-enabled national air travel. Table 2 provides the key benefits, challenges and policy recommendations for the DYA to the relevant policy makers and stakeholders.

Table 2: Benefits and challenges of DYA

Benefits	Challenges	Policy recommendations
Convenience and efficiency	Errors	Upgrade the FRT-enabled biometric boarding systems at airports within India at a regular interval to ensure technical errors and glitches are resolved in time and systems have the latest technological advancements for a better experience of air travel within India and beyond.
Security and safety	Data privacy	Resolve concerns relating to coercive consent wherein some passengers have complained that they were coerced into using the DYA by airport personnel. Promote transparency via the DYA platform and guidelines on the storage and processing of biometrics in the life cycle of the DYA programme — especially, the role of the DYF alongside airports, airlines and third-party service providers in the storage, processing and sharing of biometrics and related personal data of passengers.
Healthcare, accessibility and sustainability	Function creep	Conduct a comprehensive Data Protection Impact Assessment (DPIA) via an expert agency to calibrate compliance with DPDP and GDPR standards to deliberate present and future compliance of the DYA. The DYA will expand to include international passengers, foreign airports and other means of travel within India. A DPIA in coordination with the relevant state and judicial agencies will ensure pre-empting the regulatory challenges confronted by the DYA, especially as it relates to the issue of 'function creep'.

APPENDIX A: SPECIFIC INSTITUTIONS/COUNTRIES WITH AI AND FRT GUIDELINES/LAWS

Specific constitutions/countries with AI and FRT guidelines/laws

International organisations

1. AI Safety Summit 2023 — The Bletchley Declaration[226]
2. G-20 (Group of Nations) — G20 AI Principles[227]
3. G-7 (Group of Nations) — Hiroshima Process — International Guiding Principles for Organizations Developing Advanced AI Systems[228]
4. Global Privacy Assembly (GPA) — Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology; Adopted Resolution on Facial Recognition Technology; Adopted Resolution on Accountability in the Development and Use of Artificial Intelligence[229]
5. International Civil Aviation Organization (ICAO) — ICAO Doc-9303 – Machine Readable Travel Documents (MRTD)[230]
6. International Telecommunication Union (ITU) — ITU AI Standards[231]
7. OECD — OECD AI Principles[232]
8. Paris AI Summit 2025 — Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet[233]
9. United Nations (UN) Inter-Agency Working Group on Artificial Intelligence — Principles for the Ethical Use of Artificial Intelligence in the United Nations System[234]
10. United Nations Educational, Scientific and Cultural Organization (UNESCO) — Ethics of Artificial Intelligence; Policy Framework for Responsible Limits on Facial Recognition – Use Case: Law Enforcement Investigations[235]
11. World Economic Forum (WEF) — AI Value Alignment: Guiding Artificial Intelligence Towards Shared Human Goals[236]

Countries

1. African Union — Continental Artificial Intelligence Strategy; Artificial Intelligence in Economic Policymaking[237]
2. Asia-Pacific Economic Cooperation (APEC) — Artificial Intelligence in APEC[238]
3. Association of Southeast Asian Nations (ASEAN) — ASEAN Guide on AI Governance and Ethics[239]
4. Canada — AI Governance in Canada[240]
5. Japan — Governance Guideline for Implementation of AI Principles[241]
6. Singapore — Singapore's Approach to AI Governance[242]
7. UK — Implementing the UK's AI Regulatory Principles – Initial Guidance for Regulator; A pro-innovation approach to AI regulation[243]

References

1. Consumer News And Business Channel (CNBC) (2024), 'The World's First Airport to require Biometric Boarding is set to arrive in 2025', available at https://www.cnbc.com/2024/08/22/worlds-first-airport-to-require-biometric-boarding-to-arrive-in-2025.html (accessed 30th January, 2025).
2. *Ibid*.
3. *Ibid*.
4. Sinmaz, E. (April 2025), 'Live Facial Recognition labelled "Orwellian" as Met Policy Push Ahead with Use', *Guardian*, available at https://www.theguardian.com/technology/2023/apr/05/live-facial-recognition-criticised-metropolitan-police (accessed 30th January, 2025).
5. DigiYatra Foundation, 'Frequently Asked Questions', available at https://digiyatrafoundation.com/ (accessed 30th January, 2025).
6. Chandra, J. (June 2024), 'DigiYatra could be expanded to hotels, rail travel and public places: CEO', *The Hindu*, available from: https://www.thehindu.com/news/national/digi-yatra-could-be-expanded-to-hotels-rail-travel-and-public-places-ceo/article68300903.ece (accessed 30th January, 2025).
7. Ministry of Aviation, '"Digi Yatra Biometric Boarding System", Reimagining Air Travel in India', available at https://www.civilaviation.gov.in/sites/default/files/2023-07/Digi%20Yatra%20Policy%20%28DIGI%20YATRA%29.pdf (accessed 30th January, 2025).
8. *Ibid*.
9. Davis, N., Perry, L. and Santow, E. (September 2022), 'Facial Recognition Technology – Towards a Model Law', University of Technology Sydney, available at https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf (accessed 30th January, 2025).
10. *Ibid*.
11. *Ibid*.
12. Ministry of Aviation, ref. 8 above.
13. *Ibid*.
14. *Ibid*.
15. *Ibid*.
16. *Ibid*.
17. *Ibid*.
18. *Ibid*.
19. *Ibid*.
20. *Ibid*.
21. DigiYatra Foundation, ref. 5 above.
22. Bosch, 'Digital identity – enabling secure collaboration with blockchain technology', available at https://www.bosch.com/stories/self-sovereign-identities/ (accessed 30th January, 2025).
23. *Ibid*.
24. One Identity, 'What Are Verifiable Credentials and How Do They Work?', available at https://www.oneidentity.com/learn/what-are-verifiable-credentials-in-cybersecurity.aspx#:~:text=Verifiable%20Credentials%20(VCs)%20are%20digital,several%20bodies%2C%20including%20the%20W3C (accessed 15th July, 2024).
25. Truvera (February 2025), 'Decentralized Identifiers (DIDs): The Ultimate Beginner's Guide 2023', available at https://www.dock.io/post/decentralized-identifiers#:~:text=of%20these%20problems.-,What%20Are%20Decentralized%20Identifiers%20(DIDs)%3F,to%20you%20by%20someone%20else (accessed 19th February, 2025).
26. Majaski, C. (June 2023), 'Distributed Ledgers: Definition, How They're Used, and Potential', Investopedia, available at https://www.investopedia.com/terms/d/distributed-ledgers.asp#:~:text=A%20distributed%20ledger%20is%20a%20database%20that%20is%20synchronized%20and,use%20of%20a%20distributed%20ledger (accessed 15th July 2024).
27. DigiYatra Guidelines, ref. 8 above; Ministry of Civil Aviation, Government of India (March 2023), 'Under Digi Yatra, passengers' data is stored in their own device and not in centralized storage', available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1907479#:~:text=Under%20Digi%20Yatra%2C%20passengers%E2%80%99%20data%20is%20stored%20in,and%20stored%20in%20the%20wallet%20of%20their%20smartphone (accessed 30th January, 2025).
28. *Ibid*.
29. *Ibid*.
30. *Ibid*.
31. *Ibid*.
32. Amazon Web Services (AWS), 'DigiYatra Foundation Transforms Passenger Processes at Airports Across India with DigiYatra Mobile App on AWS', available at https://aws.amazon.com/solutions/case-studies/digi-yatra-foundation/; Ministry of Civil Aviation, 'Union Minister for Civil Aviation Shri Jyotiraditya Scindia Launched DigiYatra for Three Airports in the Country', Government of India, available at https://pib.gov.in/PressReleasePage.aspx?PRID=1880272; Business Standard (February 2023), 'Over 160,000 air travellers have taken benefit of DigiYatra: Official', available at https://www.business-standard.com/article/current-affairs/over-160-000-air-travellers-have-taken- benefit-of-digi-yatra-official-123022301125_1.html; Sinha, S. (May 2024), 'DigiYatra to transform international travel with e-passports, hotel check-ins and more; details here', Good Returns, available at https://www.goodreturns.in/personal-finance/digi-yatra-to-transform-international-travel-with-e-passports-hotel-check-ins-more-details-here-1344979.html (all accessed 30th January, 2025).
33. *Ibid*.
34. *Ibid*.
35. *Ibid*.
36. *Ibid*.
37. Ministry of Aviation, ref. 8 above, pp. 11–12; Amazon Web Services (AWS), 'The Facts on Facial Recognition with Artificial Intelligence', available at https://aws.amazon.com/rekognition/

the-facts-on-facial-recognition-with-artificial-intelligence/ (accessed 30th January, 2025).
38. *Ibid*.
39. *Ibid*.
40. *Ibid*.
41. DD News (September 2024), 'Union Minister Ram Mohan Naidu inaugurates DigiYatra Facility at nine more airports', available at https://ddnews.gov.in/en/union-minister-ram-mohan-naidu-inaugurates-digi-yatra-facility-at-nine-more-airports/ (accessed 30th January, 2025).
42. *Ibid*.
43. *Ibid*.
44. *Ibid*.
45. *Ibid*.
46. Davis *et al*., ref. 9 above, pp. 28–29.
47. *Ibid*.
48. First Post (April 2024), 'Is Digi Yatra storing passenger data? The controversy explained', available at https://www.firstpost.com/explainers/digiyatra-storing-passenger-data-controversy-13760590.html (accessed 30th January, 2025).
49. Shriyan, S. (August 2023), 'DigiYatra Systems Crash at Kolkata Airport; Passengers Left Stranded for up to 11 Hours', Curly Tales, available at https://curlytales.com/digiyatra-systems-crash-at-kolkata-airport-passengers-left-stranded-for-up-to-11-hours/; Bengrut D. (April 2023), 'Digi Yatra facility at Pune airport faces tech glitches', *Hundustan Times*, available at https://www.hindustantimes.com/cities/pune-news/pune-airport-s-digiyatra-service-faces-technical-glitches-passengers-complain-about-non-functional-facial-biometrics-check-in-and-boarding-digiyatra-puneairport-facialrecognition-technicalglitches-101680628738087.html (both accessed 30th January, 2025).
50. *Ibid*.
51. *Ibid*.
52. Verma, D. (April 2024), 'Dear Digi Yatris it's time to deboard', Internet Freedom Foundation (IFF), available at https://internetfreedom.in/dear-digi-yatris-its-time-to-deboard/; Shaikh, T. (April 2024), 'DigiYatra App Data Compromised; App Maker Dropped After the Data Breach. Is Your Data Safe?', Curly Tales, available at https://curlytales.com/digiyatra-app-data-compromised-app-maker-dropped-after-the-breach-is-your-data-safe/#google_vignette (both accessed 30th January, 2025).
53. *Ibid*.
54. *Ibid*.
55. Internet Freedom Foundation (IFF), 'Hey DigiYatra Foundation, Open Up the Doors…', available at https://internetfreedom.in/digi-yatra-foundation-open-up-the-doors/#:~:text=Of%20late%2C%20passengers%20across%20India,been%20registered%20for%20the%20service; *The Hindu* (January 2024), 'Airports to ensure DigiYatra registration is voluntary and consensual: Scindia', available at https://www.thehindu.com/news/national/airports-to-ensure-digi-yatra-registration-is-voluntary-and-consensual-scindia/article67782525.ece; Verma, D. (February 2024), 'DigiYatra: Service or Surveillance', The India Forum, available at https://www.theindiaforum.in/technology/digi-yatra-service-or-surveillance; Mavad A. (June 2024), 'Are non-DigiYatra fliers also being photographed?', *The Deccan Herald*, available at https://www.deccanherald.com/lifestyle/travel/are-non-digiyatra-fliers-also-being-photographed-3066081; Bharti, D. (January 2024), 'Govt. pushes people to register for DigiYatra, collects facial data at airport to enrol them without consent', IndiaToday, available at https://www.indiatoday.in/technology/news/story/govt-pushes-people-to-register-for-digi-yatra-collects-facial-data-at-airport-to-enrol-them-without-consent-2485919-2024-01-08; Sukriti (April 2024), 'DigiYatra and the Defect in the Idea of Consent', TechPolicy.Press, available at https://www.techpolicy.press/digi-yatra-and-the-defect-in-the-idea-of-consent/; Verma, D. (January 2024), 'Resist Surveillance Tech, Reject DigiYatra', Internet Freedom Foundation (IFF), available at https://internetfreedom.in/reject-digiyatra/; BW Business World (January 2024), 'Data Collection for DigiYatra Requires Passenger Consent: Jyotiraditya Scindia', available at https://www.businessworld.in/article/data-collection-for-digi-yatra-requires-passenger-consent-jyotiraditya-scindia-507884 (all accessed 30th January, 2025).
56. *Ibid*.
57. *Ibid*.
58. *Ibid*.
59. *Ibid*.
60. *Ibid*.
61. *Ibid*.
62. *Ibid*.
63. *Ibid*.
64. *Ibid*.
65. *Ibid*.
66. *Ibid*.
67. *Ibid*.
68. *Ibid*.
69. *Ibid*.
70. *Ibid*.
71. *Ibid*.
72. *Ibid*.
73. *Ibid*.
74. *Ibid*.
75. *Ibid*.
76. *Ibid*.
77. *Ibid*.
78. *Ibid*.
79. *Ibid*.
80. *Ibid*.
81. *Ibid*.
82. *Ibid*.
83. *Ibid*.
84. *Ibid*.
85. *Ibid*.
86. *Ibid*.
87. *Ibid*.

88. Bajpai, R. C. and Yadav, S. (January 2021), 'Use of Facial Recognition Technology in India: A Function Creep Breaching Privacy', Oxford Huan Rights Lab, available at https://ohrh.law.ox.ac.uk/use-of-facial-recognition-technology-in-india-a-function-creep-breaching-privacy/; Houwing, L. (2020), 'Opinions – Stop the Creep of Biometric Surveillance Technology', *European Data Protection Law Review*, Vol. 6, No. 2, available at https://edpl.lexxion.eu/article/edpl/2020/2/5; Korweitz, A. (August 2021), 'A New AI Lexicon: Function Creep', AI Now Institute, available at https://ainowinstitute.org/publication/a-new-ai-lexicon-function-creep (all accessed 30th January, 2025).
89. *Ibid*.
90. *Ibid*.
91. Hao, K. (June 2020), 'The two-year fight to stop Amazon from selling face recognition to the police', MIT Technology Review, available at https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/ (accessed 30th January, 2025).
92. University of Technology Sydney (UTS) (September 2022), 'New report offers blueprint for regulation of facial recognition technology', available at https://www.uts.edu.au/sites/default/files/2022-09/27.09.22%20New%20report%20offers%20blueprint%20for%20regulation%20of%20facial%20recognition%20technology.pdf (accessed 30th January, 2025).
93. EUR-Lex (April 2016), '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)', available at https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (accessed 30th January 2025).
94. University of Technology Sydney (UTS), ref. 92 above.
95. Hao, ref. 91 above.
96. Lee, D. (May 2019), 'San Francisco is first US city to ban facial recognition', BBC, available at https://www.bbc.com/news/technology-48276660 (accessed 30th January 2025). American Civil Liberties stated that 'with this vote, San Francisco has declared that FRTs are incompatible with a healthy democracy and that residents deserve a voice in decisions about high-tech surveillance'.
97. University of Technology Sydney (UTS), ref. 92 above.
98. World Economic Forum (WEF) (November 2022), 'A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations', available at https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf (accessed 30th January, 2025).
99. Selinger, E. and Hartzog, W. (2019), 'The Inconsentability of Facial Surveillance', *Loyola Law Review*, Vol. 6, No. 101, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557508 (accessed 30th January, 2025).
100. Ministry of Electronics & Information Technology (MeitY), Government of India, 'Digital Personal Data Protection Act, 2023', available at https://www.meity.gov.in/content/digital-personal-data-protection-act-2023 (accessed 30th January, 2025).
101. *Ibid*.
102. *Ibid*.
103. *Ibid*.
104. *Ibid*.
105. *Ibid*.
106. *Ibid*.
107. *Ibid*.
108. *Ibid*.
109. *Ibid*.
110. *Ibid*.
111. *Ibid*.
112. *Ibid*.
113. *Ibid*.
114. *Ibid*.
115. NITI Aayog (June 2018), 'National Strategy for Artificial Intelligence #AIforAll', available at https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf (accessed 30th January, 2025).
116. *Ibid*.
117. Solove, D. (February 2024), 'Artificial Intelligence and Privacy', *Florida Law Review*, Vol. 77, SSRN available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4713111 (accessed 30th January, 2025).
118. *Ibid*.
119. *Ibid*.
120. *Ibid*.
121. *Ibid*.
122. *Ibid*.
123. *Ibid*.
124. *Ibid*.
125. *Ibid*.
126. *Ibid*.
127. *Ibid*.
128. *Ibid*.
129. *Ibid*.
130. *Ibid*.
131. *Ibid*.
132. *Ibid*.
133. *Ibid*.
134. *Ibid*.
135. EUR-Lex, ref. 93 above.
136. *Ibid*.
137. *Ibid*.
138. *Ibid*.
139. *Ibid*.
140. *Ibid*.
141. *Ibid*.
142. *Ibid*.
143. *Ibid*.
144. *Ibid*.
145. *Ibid*.
146. *Ibid*.
147. *Ibid*.

148. *Ibid.*
149. European Commission (EC), 'Binding Corporate Rules (BCR)', available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#:~:text=What%20are%20binding%20corporate%20rules,group%20of%20undertakings%20or%20enterprises (accessed 30th January, 2025). BCRs are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding and enforced by every member concerned of the group.
150. European Commission (EC), 'EU Standard Contractual Clauses', available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed 30th January, 2025). Standard contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries. This includes model contract clauses – so-called SCCs – that have been preapproved by the EC.
151. Data Protection Commission of Dublin, 'Codes of Conduct', available at https://www.dataprotection.ie/en/organisations/codes-conduct (accessed 30th January, 2025). Codes of Conduct, under the GDPR, are voluntary set of rules that assist members of that Code with data protection compliance and accountability in specific sectors or relating to particular processing operations.
152. Data Protection Commission of Dublin, 'GDPR Certification', available at https://www.dataprotection.ie/en/organisations/gdpr-certification (accessed 30th January, 2025). Certification schemes in GDPR specify the mechanisms in place for the processing of personal data and how appropriate controls and measures are implemented. These may then be assessed by an accredited certification body.
153. *Ibid.*
154. *Ibid.*
155. *Ibid.*
156. European Data Protection Board (EDPB) (2024), '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)', available at https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112024-use-facial-recognition-streamline_en (accessed 30th January, 2025).
157. *Ibid.*
158. *Ibid.*
159. *Ibid.*
160. *Ibid.*
161. *Ibid.*
162. *Ibid.*
163. *Ibid.*
164. *Ibid.*
165. *Ibid.*
166. *Ibid.*
167. *Ibid.*
168. *Ibid.*
169. *Ibid.*
170. *Ibid.*
171. *Ibid.*
172. *Ibid.*
173. *Ibid.*
174. *Ibid.*
175. *Ibid.*
176. *Ibid.*
177. *Ibid.*
178. *Ibid.*
179. *Ibid.*
180. *Ibid.*
181. *Ibid.*
182. *Ibid.*
183. EUR-Lex (2024), '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)', available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (accessed 30th January, 2025).
184. *Ibid.*
185. *Ibid.*
186. *Ibid.*
187. *Ibid.*
188. European Data Protection Board (EDPB) (2023), 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement', Version 2.0, available at https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (accessed 30th January, 2025).
189. NITI Aayog, ref. 115 above.
190. *Ibid.*
191. Digi Yatra Foundation (DYF), 'The Panoptic Tracker', available at https://panoptic.in/ (accessed 30th January, 2025).
192. Pankaj, J. (June 2024), 'Widespread Use of Facial Recognition Tech across India', BusinessLine, available at https://www.thehindubusinessline.com/data-stories/amid-growing-need-for-security-over-1513-crore-invested-in-deploying-facial-recognition-technology-across-country/article68288599.ece (accessed 10th July, 2024).
193. Unique Identification Authority of India, Government of India, 'What Is Face Recognition?', available at https://uidai.gov.in/en/17-english-uk/resident/12722-what-is-face-recognition.html (accessed 30th January, 2025).
194. *Ibid.*
195. Ministry of Personnel, Public Grievances &

Pensions, 'Department of Pension & Pensioners Welfare Is Possibly One of the First Departments in the Govt Sector to Have Started Using the Latest "Face Recognition Technology" for Establishing the Aadhar Based Identification of Elderly Pensioners to Generate "Digital Life Certificate", Says Dr Jitendra Singh', available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1985134 (accessed 10th July, 2024).

196. *Ibid*.
197. *Ibid*.
198. Bhatnagar, G. (February 2021), "'Pandora's Box of Privacy Issues": Experts on Delhi Govt Schools' Use of Facial Recognition Tech', The Wire, available at https://thewire.in/education/delhi-government-schools-facial-recognition-cctv-cameras (accessed on 10th July 2024).
199. National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India (2019), 'Request For Proposal to procure Automated Facial Recognition System (AFRS)', available at https://eprocure.gov.in/eprocure/app?component=%24DirectLink&page=FrontEndViewTender&service=direct&sp=S%2B6yRhk%2BPBLNDUmlDZkD8DQ%3D%3D (accessed 30th January, 2025).
200. *Ibid*.
201. *Ibid*.
202. *Ibid*.
203. *Ibid*.
204. *Ibid*.
205. *Ibid*.
206. *Ibid*.
207. *Ibid*.
208. *Ibid*.
209. *Ibid*.
210. Mohanty, A. and Sahu, S. (November 2024), 'India's Advance on AI Regulation', Carnegie India, available at https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en&center=india (accessed 30th January, 2025).
211. *Ibid*.
212. *Ibid*.
213. *Ibid*.
214. *Ibid*.
215. *Ibid*.
216. *Ibid*.
217. Autoriteit Persoonsgegevens (2024), 'Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition', available at https://autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition (accessed 30th January, 2025).
218. European Data Protection Board (EDPB) (May 2023), 'Facial Recognition: The French SA imposes a penalty payment on Clearview AI', available at https://www.edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en; European Data Protection Board (EDPB) (September 2024), 'Dutch Supervisory Authority imposes a fine on Clearview because of illegal data collection for facial recognition', available at https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en; European Data Protection Board (EDPB) (May 2022), 'Facial Recognition: Italian SA fines Clearview AI EUR 20 million', available at https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en; Covington (June 2022), 'Facial Recognition Update: UK ICO Fines Clearview AI Pound 7.5m & EDPB Adopts Draft Guidelines on Use of FRT by Law Enforcement', available at https://www.insideglobaltech.com/2022/06/02/facial-recognition-update-uk-ico-fines-clearview-ai-7-5m-edpb-adopts-draft-guidelines-on-use-of-frt-by-law-enforcement/; European Data Protection Board (EDPB) (July 2022), 'Hellenic DPA fines Clearview AI 20 million euros', available at https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en (all accessed 30th January, 2025).
219. Davis *et al.*, ref. 9 above, pp. 28–29.
220. *Ibid*.
221. *Ibid*.
222. *Ibid*.
223. *Ibid*.
224. *Ibid*.
225. *Ibid*.
226. Prime Minister's Office 10 Downing Street/Foreign Commonwealth & Development Office/Department for Science, Innovation & Technology (February 2025 [updated]), 'The Bletchley Declaration by Countries Attending the AI Safety Summit, 1–2 November 2023', Gov.UK, available at https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023? (accessed 19th February, 2024)
227. Organisation for Economic Co-operation and Development (OECD) (June 2019), 'G20 AI Principles', available at https://oecd.ai/en/wonk/documents/g20-ai-principles (accessed 30th January, 2025).
228. Ministry of Foreign Affairs Japan (MOFA), 'Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems', available at https://www.mofa.go.jp/files/100573471.pdf (accessed 30th January, 2025).
229. Global Privacy Assembly (October 2022), 'Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology', available at https://globalprivacyassembly.org/wp-content/uploads/2022/11/15.1.c.Resolution-on-Principles-and-Expectations-for-the-Appropriate-Use-of-Personal-Information-in-Facial-Recognition-Technolog.pdf; Global Privacy Assembly (October 2020), 'Adopted Resolution on Facial Recognition Technology', available at https://globalprivacyassembly.

org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Facial-Recognition-Technology-EN.pdf; Global Privacy Assembly (October 2020), 'Adopted Resolution on Accountability in the Development and Use of Artificial Intelligence', available at https://globalprivacyassembly.org/wp-content/uploads/2020/11/GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN.pdf (all accessed 30th January 2025).

230. International Civil Aviation Organization (ICAO), 'Machine Readable Travel Documents (MRTD)', Doc-9303, available at https://www.icao.int/publications/pages/publication.aspx?docnum=9303 (accessed 30th January, 2025).
231. International Telecommunication Union (ITU), 'IYU-T Recommendations', available at https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx (accessed 30th January, 2025).
232. Organisation for Economic Co-operation and Development (OECD), 'OECD AI Principles overview', available at https://oecd.ai/en/ai-principles (accessed 30th January, 2025).
233. Élysée (February 2025), 'Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet', available at https://www.elysee.fr/en/emmanuel-macron/2025/02/11/statement-on-inclusive-and-sustainable-artificial-intelligence-for-people-and-the-planet (accessed 19th February, 2025).
234. United Nations (UN) (September 2022), 'Principles for the Ethical Use of Artificial Intelligence in the United Nations System', available at https://unsceb.org/sites/default/files/2022-09/Principles%20for%20the%20Ethical%20Use%20of%20AI%20in%20the%20UN%20System_1.pdf (accessed 30th January, 2025).
235. United Nations Educational, Scientific and Cultural Organization (UNESCO), 'Ethics of Artificial Intelligence', available at https://www.unesco.org/en/artificial-intelligence/recommendation-ethics; UN Interregional Crime and Justice Research Institute (November 2022), 'Policy Framework for Responsible Limits on Facial Recognition – Use Case: Law Enforcement Investigations', available at https://unicri.org/A-Policy-Framework%20-for-Responsible-Limits-on-Facial-Recognition (both accessed 30th January, 2025).
236. World Economic Forum (WEF) (October 2024), 'AI Value Alignment: Intelligence Towards Shared Human Goals', available at https://www3.weforum.org/docs/WEF_AI_Value_Alignment_2024.pdf (accessed 30th January, 2025).
237. African Union (August 2024), 'Continental Artificial Intelligence Strategy', available at https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy (accessed 30th January, 2025).
238. Asia-Pacific Economic Cooperation (APEC) Business Advisory Council, 'Artificial Intelligence in APEC – Overview of the state of AI in APEC economies and the enabling initiatives that will further drive adoption', available at https://ncapec.org/wp-content/uploads/2020/11/ABAC-AI-Report.pdf; Asia-Pacific Economic Cooperation (APEC) (November 2022), 'Artificial Intelligence in Economic Policymaking', Brief No. 52, available at https://www.apec.org/docs/default-source/publications/2022/11/artificial-intelligence-in-economic-policymaking/222_psu_artificial-intelligence-in-economic-policymaking.pdf (both accessed 30th January, 2025).
239. Association of Southeast Asian Nations (ASEAN) (2024), 'ASEAN Guide on AI Governance and Ethics', available at https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf (accessed 30th January, 2025).
240. AIGS Canada, 'Governing AI: A Plan for Canada', available at https://aigs.ca/white-paper.pdf (accessed 30th January, 2025).
241. Ministry of Economy, Trade and Industry (METI) (January 2022), 'Governance Guidelines for Implementation of AI Principles', Ver. 1.1, available at https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_2.pdf (accessed 30th January, 2025).
242. Personal Data Protection Commission (PDPC) Singapore, 'Singapore's Approach to AI Governance', available at https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework (accessed 30th January, 2025).
243. Department for Science, Innovation & Technology (February 2024), 'Implementing the UK's AI Regulatory Principles – Initial Guidance for Regulators', Gov.UK, available at https://assets.publishing.service.gov.uk/media/65c0b6bd63a23d0013c821a0/implementing_the_uk_ai_regulatory_principles_guidance_for_regulators.pdf; Department for Science, Innovation & Technology/Office for Artificial Intelligence (August 2023 [updated]), 'A pro-innovation approach to AI regulation', Gov.UK, available at https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper (both accessed 30th January, 2025).